T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI TİCARET VE LOJİSTİK ANABİLİM DALI

Yüksek Lisans Tezi

GENÇ TÜKETİCİLERİN SOSYAL MÜHENDİSLİK İLE SİBER GÜVENLİK FARKINDALIKLARININ ONLİNE ALIŞVERİŞ NİYETLERİ ÜZERİNDEKİ ETKİSİNİN ÖLÇÜLMESİ

Gülcihan AYDANER
165016034

Tez Danışmanı:
Dr. Öğretim Üyesi Özer YILMAZ

BANDIRMA 2019

T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI TİCARET VE LOJİSTİK ANABİLİM DALI

Yüksek Lisans Tezi

GENÇ TÜKETİCİLERİN SOSYAL MÜHENDİSLİK İLE SİBER GÜVENLİK FARKINDALIKLARININ ONLİNE ALIŞVERİŞ NİYETLERİ ÜZERİNDEKİ ETKİSİNİN ÖLÇÜLMESİ

Gülcihan AYDANER
165016034

Tez Danışmanı:
Dr. Öğretim Üyesi Özer YILMAZ
Dr. Öğretim Üyesi Ufuk ÇELİK (Eş Danışman)

BANDIRMA 2019

YÜKSEK LİSANS TEZİ ONAYI

Bandırma Onyedi Eylül Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası Ticaret ve Lojistik Anabilim Dalı, Uluslararası Ticaret ve İşletmecilik Tezli Yüksek Lisans Programında Yüksek Lisans Öğrencisi Gülcihan AYDANER tarafından Dr. Öğr. Üyesi Özer YILMAZ ve Dr. Öğr. Üyesi Ufuk ÇELİK (Eş Danışman) danışmanlığında hazırlanan "Genç Tüketicilerin Sosyal Mühendislik ve Siber Güvenlik Farkındalıklarının Online Alışveriş Niyetleri Üzerindeki Etkisinin Ölçülmesi" başlıklı tezi aşağıdaki jüri üyeleri tarafından 17/05/2019 tarihinde yapılan Tez Savunma Sınavında oyçokluğu/oybirliği ile başarılı bulunmuş ve Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Başkanı
Dr. Öğr. Üyesi Oğuz DİKER

Jüri-Danışman
Dr. Öğr. Üyesi Özer YILMAZ

Jüri Üyesi
Doç. Dr. Hatice AYDIN

ETİK BEYAN

TÜRKİYE CUMHURİYETİ
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile bu tezdeki bütün bilgilerin akademik kurallara ve etik ilkelere uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi ayrıca beyan ederim. (...../...../20...)

Gülcihan AYDANER

.

ÖZET

GENÇ TÜKETİCİLERİN SOSYAL MÜHENDİSLİK İLE SİBER GÜVENLİK FARKINDALIKLARININ ONLİNE ALIŞVERİŞ NİYETLERİ ÜZERİNDEKİ ETKİSİNİN ÖLÇÜLMESİ

Gülcihan AYDANER

İnternet ve bilişim suçları; işlenmesi kolay, saldırı maliyeti çok düşük, toplumsal ve ticari maliyeti çok yüksek suçlar arasında yer almaktadır. Bu nedenle dijital dönüşümün getirdiği yeniliklerle birlikte ülke ekonomilerinin geleceği olan online ticaret üzerinde özenle durulması gereken bir noktaya ulaşmıştır. Bu çalışmanın amacı; online ortamlarda alışveriş yapan genç tüketicilerin, sosyal mühendislik ile siber güvenlik farkındalıklarını ölçmektir. Çalışma online alışverişlerde güvenli internet kullanım farkındalığının sağlanması ile güvenli toplumların ve güvenli online ticari hayatın oluşturulmasına katkı sağlayacaktır. Bu amaçla yapılan çalışmada online tüketicilere ve online ticari faaliyetlerde bulunan işletmelere, sosyal mühendislik ile siber güvenlik risklerini doğru yönetebilmeleri için gerekli taktikler ve tedbir amaçlı bilgiler aktarılmıştır. Ayrıca Bandırma Onyedi Eylül Üniversitesi Merkez Kampüsünde 693 öğrencinin katılımıyla gerçekleşen bir anket çalışması yapılmış verilerin analizinde SPSS Versiyon 24 ve Amos 22 paket programları kullanılarak Yapısal Eşitlik Modellemesinden (YEM) faydalanılmıştır. Bu araştırma ile "Online Alışveriş Güvenlik Modeli" (OAGM) oluşturularak alanında özgün bir çalışma tamamlanmıştır. Bu model dışında tüketicilerin online alışveriş niyetleri ile sosyal mühendislik ve siber güvenlik farkındalıklarını bir arada inceleyen ve aralarındaki ilişkisel bağları tespit ederek ortaya çıkaran herhangi bir çalışmaya ulaşılamamıştır. Bu nedenle ortaya konulan model orijinal olma niteliği taşımaktadır. Anket çalışmasının ikinci bölümünde ise konuya ilişkin genel değerlendirme anketi uygulanmış tanımlayıcı istatistikler aracılığıyla yapılan analizler sonucunda değerlendirmelerde bulunulmuştur.

Araştırmada genç tüketicilerin sosyal mühendislik farkındalıklarında meydana gelen değişimde, çok güçlü bir oran olan %65 lik bir kısmının genç tüketicilerin siber güvenlik farkındalıklarında meydana gelen değişim tarafından açıklandığı tespit edilmiştir. Aktarılan tüm bilgilerle birlikte yükseköğretim öğrencilerinin bilgi güvenliği ve güvenli internet kullanımı konularında eğitimlere ihtiyaç duydukları belirlenmiştir.

Anahtar Kelimeler: Siber Güvenlik, Sosyal Mühendislik, Online Alışveriş, Sosyal Ağlar, Dijital Vatandaşlık.

ABSTRACT

MEASUREMENT OF THE IMPACT OF SOCIAL ENGINEERING AND CYBER SECURITY AWARENESS OF YOUNG CONSUMERS ON ONLINE SHOPPING INTENTIONS

Gülcihan AYDANER

Internet and cyber crimes; easy to process, very low cost of attack, social and commercial costs are among the very high crimes. Therefore, with the innovations brought about by digital transformation, the future of the country's economies, online trade, has reached a point that needs to be carefully considered. The aim of this study is; to measure social engineering and cyber security awareness of young consumers shopping in online environments. The study will contribute to the creation of safe communities and safe online commercial life by ensuring the awareness of safe internet usage in online shopping. In this study; the necessary tactics and precautionary information were given to the online consumers and the businesses that are engaged in online commercial activities in order to manage social engineering and cyber security risks correctly. In addition, a survey was conducted with the participation of 693 students at the Central Campus of Bandırma Onyedi Eylül University. SPSS Version 24 and Amos 22 package programs were used for data analysis. Structural Equation Modeling (SEM) was used in the analyzes. With the analysis, özgün Online Shopping Security Model (OSSM) was created and a unique study in the field was completed. In addition to this model, there is no study that explores the intersections of consumers' online shopping intentions, social engineering and cyber security awareness and identifying the relational links between them. Therefore, the model is original. In the second part of the survey, general evaluation questionnaire was applied and the general evaluations were made as a result of the analyzes made by using descriptive statistics.

In the study, it was found that 65% of the very strong rate in the change of social engineering awareness of young consumers was explained by the change in cyber

security awareness of young consumers. It has been determined that higher education students need training on information security and safe internet use with all the information transferred.

Keywords: Cyber Security, Social Engineering, Online Shopping, Social Networks, Digital Citizenship .

ÖNSÖZ

Bu çalışmada siber güvenlik, sosyal mühendislik ve online alışveriş konularında; online tüketicileri ve online ticari faaliyetlerde bulunan işletmeleri aydınlatacak tedbir amaçlı gerekli bilgi ve taktiklere yer verilmiştir. Ayrıca Yapısal Eşitlik Modellemesi (YEM) analizi ile Online Alışveriş Güvenlik Modeli (OAGM) oluşturularak alanında özgün bir çalışma tamamlanmıştır. Çalışmanın tüketicilere, ticari işletmelere ve bu alanlarda yapılacak tüm çalışmalara faydalı olması beklenmektedir.

Öncelikle bu çalışmanın ortaya çıkma ve yürütülme aşamasında; ilgileri, alâkaları ve bilgi birikimleriyle her zaman yanımda olan ve çalışma süresince tam desteklerini aldığım danışman hocalarım; Dr. Öğr. Üyesi Sayın Özer YILMAZ' a ve Dr. Öğr. Üyesi Sayın Ufuk ÇELİK' e

Her fırsatta zaman ayırarak bilgi birikimiyle beni aydınlatan Dr. Öğr. Üyesi Sayın Senem NART hocama, veri toplama aşamasında destek olan tüm hocalarıma, anket çalışmasına katılarak çalışmayı tamamlamamızda büyük katkıları olan Bandırma Onyedi Eylül Üniversitesinde öğrenim gören tüm öğrencilere, katılmamı önerdiği bir siber güvenlik konferansı ile tez konumun zihnimde netleşmesine vesile olan arkadaşım Nihal KALAYCI OFLAZ' a desteklerini kelimelerle anlatmanın mümkün olmadığı ve bu tezi ithaf ettiğim canım aileme,

Teşekkür ederim. Hayatınızda her şey istediğiniz gibi olsun…

İÇİNDEKİLER

Sayfa

TEZ ONAY SAYFASI ..... **ii**
ETİK BEYAN SAYFASI ..... **iii**
ÖZET ..... **iv**
ABSTRACT ..... **vi**
ÖNSÖZ ..... **viii**
İÇİNDEKİLER ..... **ix**
TABLOLAR ..... **xiv**
ŞEKİLLER ..... **xv**
GRAFİKLER ..... **xvi**
DENKLEMLER ..... **xvii**
KISALTMALAR ..... **xviii**
TANIMLAR ..... **xix**
GİRİŞ **1**

BİRİNCİ BÖLÜM
SOSYAL MÜHENDİSLİK İLE İLGİLİ TEMEL KAVRAMLAR

1. SOSYAL MÜHENDİSLİK KAVRAMI 3
1.1. Sosyal Mühendislik Atak Döngüsü 4
1.2. Sosyal Mühendislik Saldırı Tipleri 5
1.2.1.Tersine Sosyal Mühendislik 5
1.2.2. Sırtında Gezdirmek (Piggyback Rides) 6
1.2.3. Teknik Yetkili Gibi Konuşmak (Kimliğe Bürünme, Techie Talk) 6
1.2.4. Kimlik Avı (Yemleme, Oltalama, Sazan Avlama, Phishing) 7
1.2.5. Balina Avı (Whaling) 8
1.2.6. Telefon Oltalaması (Vishing) 9
1.2.7. Kimlik Hırsızlığı 9
1.2.8. Sosyal Medya Ağı (Social Medya Networking) 9
1.2.9. Zihin Dili Programlaması (Mind Language Programming-MLP) 10
1.2.10. Cinsiyet Cazibesini Kullanmak 11

1.2.11. Dostça Yapılan Toplantılar ve Konuşmalar 11
1.2.12. Omuz Sörfü- Omuz Gezintisi (Shoulder Surfing) 11
1.2.13. Çöp Dalışı (Dumpster Diving) 11
2. SOSYAL MÜHENDİSLERİN ÖZELLİKLERİ 11
2.1. Sosyal Mühendislerin Bilgi Toplama Kaynakları ve Düşünme Biçimleri 12
2.2. Sosyal Mühendislik Saldırısında Örnek Senaryo 14
3. SOSYAL MÜHENDİSLİK SALDIRILARINA KARŞI ALINACAK TEMEL BİREYSEL GÜVENLİK ÖNLEMLERİ……16
4. SOSYAL MÜHENDİSLİKTE KURUMSAL RİSK BİLİNCİ VE SİSTEM DEĞERLENDİRMELERİ 20
4.1. Sistem Değerlendirmeleri (Sistem A - Sistem B - Sistem C) 20
4.2. Sosyal Mühendislik Koruma Modeli 22
4.3. Kurumlarda Bilgi Güvenliği Bilincinin Yayılması 24
4.4. Sosyal Mühendislik Saldırılarına Karşı Alınacak Temel Kurumsal Güvenlik Önlemleri……...25
5. SOSYAL MÜHENDİSLİK FAALİYETLERİ VE YASALARDA SOSYAL MÜHENDİSLİK……...27

İKİNCİ BÖLÜM

SİBER GÜVENLİK İLE İLGİLİ TEMEL KAVRAMLAR

1. SİBER GÜVENLİK VE TEMEL KAVRAMLAR 30
1.1. Siber Saldırı ve Siber Savaş 30
1.2. Siber Casusluk 31
1.2.1 Siber Ekonomik Casusluk 32
1.2.2. Siber Askeri Casusluk 32
1.3. Siber Terörizm 32
1.4. Siber Suç 32
1.5. Siber Aklama 32
1.6. Siber Uzay 33
1.7. Siber Zorbalık 33
2. SİBER SALDIRI TÜRLERİ VE İŞLEVLERİ İLE SİBER GÜVENLİKTE

SCADA (Merkezi Denetleme Kontrol ve Veri Toplama Sistemi) 34
3. HACKER (KIRICI) VE HACKİNG NEDİR? 36
3.1. Hacker Çeşitleri 38
3.1.1. Siyah Şapkalı Hacker 38
3.1.2. Beyaz Şapkalı Hacker 39
3.1.3. Gri ve Kırmızı Şapkalı Hacker 39
4. HACKER'LARIN İNTERNET SİTELERİNE SALDIRI NEDENLERİ 39
5. İNTERNET GÜVENLİĞİ VE SAYISAL VERİLERLE NESNELERİN İNTERNETİ 40
6. ULUSLARARASI BAĞLAMDA SİBER GÜVENLİK VE SİBER GÜVENLİK KURUMLARI 42
6.1. USGF (Uluslararası Siber Güvenlik Federasyonu) 44
6.2. NSA (Ulusal Güvenlik Ajansı) 44
6.3. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı) 45
6.4. ITU (International Telecommunication Union-Uluslararası Telekomünikasyon Birliği) 46
6.5. INTERPOL (Uluslararası Kriminal Polis Teşkilatı) 46
6.6. NATO (Kuzey Atlantik Antlaşması Örgütü) 48
7. ULUSAL SİBER GÜVENLİK STRATEJİSİ 48
8. SİBER SALDIRI KURBANI OLMAK NASIL ENGELLENİR? 51
8.1. Akıllı Telefonlardan Kaynaklanan Güvenlik Riskleri 58
8.2. İşletim Sisteminden Kaynaklanan Güvenlik Riskleri 58
8.3. Uygulama Yetkilerinden Kaynaklı Güvenlik Riskleri 59
8.4. Casus Yazılımlardan Kaynaklanan Güvenlik Riskleri 59
8.5. Tüketiciler için Akıllı Telefon Güvenlik İpuçları (Andorid - Apple IOS - Blackberry – Windows Phone) 61
8.6. Kurum ve Kuruluşlar Siber Saldırı Kurbanı Olmamak için Ne Yapmalıdır? 62

ÜÇÜNCÜ BÖLÜM
DİJİTAL VATANDAŞLIK VE ONLİNE ALIŞVERİŞ

1. DİJİTAL VATANDAŞLIK KAVRAMI VE AVRUPA İLE ABD'DE DİJİTALLEŞME ÇALIŞMALARI……64
2. SOSYAL AĞLAR VE SOSYAL MEDYA 68
2.1. Sosyal Ağlarda Gizlilik ve Güvenlik 69
2.1.1. Sosyal Önlemler 70
2.1.1.1. Çocuk Kullanıcılar için Önlemler 70
2.1.1.2. Yetişkin Kullanıcılar için Önlemler 70
2.1.2. Yasal Önlemler 71
2.1.3. Teknolojik Önlemler 71
2.2. Sosyal Ağlarda Yapılan Bir Güvenlik Çalışmasının Sonuçları ve Öneriler .. 72
3. ONLİNE (ÇEVRİMİÇİ) ALIŞVERİŞİ ETKİLEYEN NEDENLER VE TÜRKİYE'DE E-TİCARETİN GELİŞİMİ İÇİN DEĞERLENDİRİLMESİ GEREKEN BAŞLIKLAR 74
4. ONLİNE TÜKETİCİ DAVRANIŞI VE ONLİNE ALIŞVERİŞTE GİZLİLİK İLE GÜVENLİK 78
4.1. Bir Site Bağlantısının Güvenilirliğini Kontrol Etme 80
4.2. Web Sitelerinin Çerez Politikalarını Yönetme 81
4.3. Tüketiciler için Online Alışverişte Güvenlik İpuçları 82
5. E-TİCARET ÖDEMELERİNDE SATICI PERSPEKTİFİ VE DOLANDIRICILIK 83
6. ÇEVRİMİÇİ HUKUKTA GÜVENCE VE SORUMLULUK 85
6.1. Kişisel Verilerin Korunması 85
6.2. Türkiye'de Kişisel Verilerin Korunması Kanunundan Doğan Tüketici Hakları Nelerdir? 87
6.3. Avrupa'da Çevrimiçi Koruma ve Gizlilik 88
6.4 Ulusal ve Uluslararası Çevrimiçi Ticarette Tüketici Şikayet Merkezleri 89
6.5. Tüketici Mahremiyetinin Korunması 90
6.6. Türk Ceza Kanununda Bilişim Suçları 91
7. İLGİLİ LİTERATÜR ÇALIŞMALARI 95

DÖRDÜNCÜ BÖLÜM

YÖNTEM VE UYGULAMA

1.ARAŞTIRMANIN ÖNEMİ VE AMACI 97
2. ARAŞTIRMANIN VARSAYIMLARI VE SINIRLILIKLARI 99
3. ARAŞTIRMANIN KATKILARI 99
4. ARAŞTIRMANIN MODELİ VE HİPOTEZLERİ 100
5. ARAŞTIRMANIN EVRENİ VE ÖRNEKLEMİ 102
6. VERİ TOPLAMA ARACI VE ANKET SORULARININ HAZIRLANMASI .. 104
7. ARAŞTIRMANIN GÜVENİLİRLİĞİ 106

BEŞİNCİ BÖLÜM

BULGULAR VE ANALİZLER

1. ÖRNEKLEME İLİŞKİN GENEL DEĞERLENDİRME ANKETİNİN SONUÇLARI VE TANIMLAYICI İSTATİSTİKLER (FREKANS DAĞILIMLARI) 108
2. GENEL DEĞERLENDİRME ANKETİNİN ANALİZİ VE YORUMLANMASI 117
3. YAPISAL EŞİTLİK MODELLEMESİ (YEM) VE MODELLEMEYE İLİŞKİN TESTLERİN ANALİZLERİ 119
4. İLK DFA (DOĞRULAYICI FAKTÖR ANALİZİ) SONUCU MODELDEN ÇIKARILAN DEĞİŞKENLER 120
5. İKİNCİ DFA (DOĞRULAYICI FAKTÖR ANALİZİ) SONUÇLARI 121
6. DOĞRULAYICI FAKTÖR ANALİZİ MODELİNE İLİŞKİN UYUM İYİLİĞİ DEĞERLERİ VE TESTLERİ 121
7. HİPOTEZ TESTLERİNİN ANALİZLERİ VE SONUÇLARI 123

SONUÇ VE ÖNERİLER 125
KAYNAKÇA 132
EKLER 147

TABLOLAR

Tablo 1 : Sosyal Mühendislerin Özellikleri 12
Tablo 2 : Siber Saldırı Türleri ve İşlevleri 34
Tablo 3 : 2013-2017 Yılları İnternet, Bilgisayar ve Mobil Telefon Kullanıcı Oranları 41
Tablo 4 : Casus Yazılımların İşlevleri..... 60
Tablo 5 : Tüketiciler için Akıllı Telefon Güvenlik İpuçları (Android-Apple IOS-Blackberry- Windows Phone)..... 61
Tablo 6 : İlgili Literatür Çalışmaları 95
Tablo 7 : Araştırma Hipotezleri 101
Tablo 8 : Ankette Kullanılan Ölçekler ve Araştırmacıları 105
Tablo 9 : Ölçeğe İlişkin Güvenilirlik Analizi Sonuçları 107
Tablo 10 : Genel Değerlendirme Anketinin Analizi ve Yorumlanması 117
Tablo 11 : İlk DFA (doğrulayıcı faktör analizi) Sonucu Modelden Çıkarılan Değişkenler 120
Tablo 12 : İkinci DFA (doğrulayıcı faktör analizi) Sonuçları..... 121
Tablo 13 : Uyum İyiliği Değerleri 123
Tablo 14 : Hipotez Testi Sonuçları 123

ŞEKİLLER

Şekil 1 : Sosyal Mühendislik Ataklarının İzlendiği Döngü 4
Şekil 2 : Tersine Sosyal Mühendislik 5
Şekil 3 : Sosyal Mühendislerin İnsanları Etkileme Yolları 6
Şekil 4 : TCMB Konulu Kimlik Avı Denemesinde Kullanılan E-posta Örneği 8
Şekil 5 : Sosyal Mühendislik Saldırılarında Kullanılan Bazı Donanımlar 13
Şekil 6 : Sosyal Mühendislik Saldırılarının Yaşam Döngüsü 14
Şekil 7 : Sosyal Mühendislikte Örnek Senaryo.....15
Şekil 8 : Kurumlara Yönelik Sosyal Mühendislik Saldırılarının Sektörel Risk Analizi 21
Şekil 9 : Sosyal Mühendislik Koruma Modeli 23
Şekil 10 : Hacking Teknikleri 37
Şekil 11 : Dijital Vatandaşlıkta Hedef Kitle 66
Şekil 12 : Türkiye'de E-Ticaretin Büyümesi için Değerlendirilmesi Gereken Konular 76
Şekil 13 : Araştırma Modeli: Online Alışveriş Güvenlik Modeli (OAGM).….....101

GRAFİKLER

Grafik 1 : Hacker'ların İnternet Sitelerine Saldırı Nedenleri……40
Grafik 2 : Türkiye'de Online Alışveriş Sıklığı……..……77
Grafik 3 : Anket Katılımcılarının Öğrenim Gördükleri Bölümlerin Dağılımları ve Yüzdelik Oranları……..…….108
Grafik 4 : Katılımcıların Cinsiyet Dağılım Oranları…….....109
Grafik 5 : Katılımcıların Yaş Dağılım Oranları……..……....109
Grafik 6 : Katılımcıların 3. Soruya Verdikleri Yanıtların Oranları…….....110
Grafik 7 : Katılımcıların 4. Soruya Verdikleri Yanıtların Oranları…….....110
Grafik 8 : Katılımcıların 5. Soruya Verdikleri Yanıtların Oranları…….110
Grafik 9 : Katılımcıların 6. Soruya Verdikleri Yanıtların Oranları…….111
Grafik 10 : Katılımcıların 7. Soruya Verdikleri Yanıtların Oranları…….....111
Grafik 11 : Katılımcılarım 8. Soruya Verdikleri Yanıtların Oranları……..112
Grafik 12 : Katılımcıların 9. Soruya Verdikleri Yanıtların Oranları……...112
Grafik 13 : Katılımcıların 10. Soruya Verdikleri Yanıtların Oranları…….112
Grafik 14 : Katılımcıların 11. Soruya Verdikleri Yanıtların Oranları…….113
Grafik 15 : Katılımcıların 12. Soruya Verdikleri Yanıtların Oranları…….113
Grafik 16 : Katılımcıların 13. Soruya Verdikleri Yanıtların Oranları…….113
Grafik 17 : Katılımcıların 14. Soruya Verdikleri Yanıtların Oranları…….114
Grafik 18 : Katılımcıların 15. Soruya Verdikleri Yanıtların Oranları…….114
Grafik 19 : Katılımcıların 16. Soruya Verdikleri Yanıtların Oranları…….114
Grafik 20 : Katılımcıların 17. Soruya Verdikleri Yanıtların Oranları…….....115
Grafik 21 : Katılımcıların 18. Soruya Verdikleri Yanıtların Oranları…….115
Grafik 22 : Katılımcıların 19. Soruya Verdikleri Yanıtların Oranları…….116
Grafik 23 : Katılımcıların 20. Soruya Verdikleri Yanıtların Oranları…….116

DENKLEMLER

Denklem (1.a): Nicel Değişkenli Araştırmalar İçin Örneklem Hesaplama Formülü……...103

Denklem(1.2a): Örneklem Büyüklüğünün Hesaplanması……...…103

Denklem (1.2b): Örneklem Büyüklüğü Hesaplama Formülünün Araştırmaya Uyarlanması.....103

Denklem (1.3a): Örneklem Büyüklüğünü Belirlemeye Yönelik Farklı Bir Hesaplama Formülü……..……...103

Denklem (1.3b): Örneklem Büyüklüğü Hesaplamada Farklı Bir Formülünün Araştırmaya Uyarlanması…….....104

KISALTMALAR LİSTESİ

A.B.D.	:	Amerika Birleşik Devletleri
AB	:	Avrupa Birliği
ADSL	:	Asimetrik Sayısal Abone Hattı
BKZ	:	Bakınız
BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
CIA	:	ABD Merkezi İstihbarat Teşkilatı
CNIL	:	Fransız Veri Koruma Otoritesi
EULA	:	Son Kullanıcı Lisans Sözleşmesi
FAFT	:	Kara Paranın Aklanmasının Önlenmesine İlişkin Mali Çalışma Grubu
FBI	:	ABD Federal Soruşturma Bürosu
FEDMA	:	Avrupa Doğrudan Pazarlama Federasyonu
GPS	:	Global Konumlandırma Sistemi
INTERPOL	:	Uluslararası Kriminal Polis Teşkilatı
ISO	:	Uluslararası Standartlar Teşkilatı
ISO 27001	:	Bilgi Güvenliği Yönetimi Sistemi Standardı BGYS)
ISTE	:	Uluslararası Eğitimde Teknoloji Derneği
ITU (UNİON)	:	Uluslararası Telekomünikasyon Birliği
KVKK	:	Kişisel Verileri Koruma Kurumu
NSA	:	ABD Ulusal Güvenlik Ajansı
SCADA	:	Merkezi Denetleme Kontrol ve Veri Toplama Sistemi
STK	:	Sivil Toplum Kuruluşu
TCK	:	Türk Ceza Kanunu
V.B	:	Ve Benzeri
V.D.	:	Ve Diğerleri

TANIMLAMALAR

AAV	**:**	Kredi Kartı Gelişmiş Adres Doğrulama Sistemi,
AVS	**:**	Kredi Kartı Adres Doğrulama Sistemi,
Bakanlık:	**:**	Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı,
CSC -CVV	**:**	Kredi Kartı Güvenlik Kodu Programları,
Faktoring	**:**	Firmaların mal ve hizmet satışlarından doğan alacak haklarının temlik edildiği finansman tekniği,
Fraud	**:**	İnternette yapılan işlemlerde sistemin açıklarından istifade edilerek yapılan sahtekârlık ve dolandırıcılık olayları,
ISTE	**:**	Öğrencilerin çevrimiçi kimliklerini yönetmelerine yardımcı olan ve eğitimde bilgi teknolojilerinin kullanımıyla ilgili eğitimcilere hizmet veren kâr amacı olmayan organizasyon,
İnternet of Things (LoT)	**:**	Nesnelerin İnterneti,
Leasing (Finansal Kiralama)	**:**	Bir yatırım malının mülkiyetinin sözleşme sonunda kiracıya geçmesi,
Linux	**:**	Bilgisayar işletim sistemlerinin çekirdeği olan yazılım,
Proxy	**:**	Vekil veya yetkili sunucu. İnternete erişimde kullanılan ara sunucu. Network şifreleme sistemi,
SET (Secure Electronic Transaction) Güvenli Elektronik İletişim	**:**	E-ticaret sitesi ile ödeme şirketi arasındaki şifreleme protokolü. Güvenli elektronik işlemler
SSL Sertifikası	**:**	Veri güvenliğinin sağlanması için web sitelerinin kimliğini doğrulayan ve bilgileri şifreleyen protokol. Güvenli kilit sistemi,
TSL (Transport Layer Security) Taşıma Güvenliği Katmanı	**:**	Ağ üzerinde güvenli iletişim için tasarlanan şifreleme protokolleri,

GİRİŞ

Günümüzde online platformlar, tüketici gereksinimlerinin belirlenmesi, farklı kaynaklardan ürün, hizmet ve fiyat değerlendirmesinin yapılabilmesi gibi birçok esnek seçime imkân sağladığından gelişime açık bir yapıya sahiptir (Yanık,2014: 89). Dijital teknolojilerin gelişimiyle birlikte geleneksel yöntemlerle tüketicilere sunulan mal ve hizmetlerin tüketicilere akış yönü dijital ortamlara kaymıştır. Online (çevrimiçi) olarak adlandırılan internette, iletişim teknolojilerinin gelişmesi sosyal ağlarda gerçekleşen iletişimin ve bilgiye ulaşılma hızının artması, alışverişlerde yer, zaman ve mekân sınırlamasının bulunmaması online alışveriş sitelerinin karşılaştırılabilir olması ve uygun fiyat politikalarının bulunması gibi faktörler tüketicileri geleneksel alışveriş yöntemlerinden koparıp online ortamlarda alışverişe yönlendirmiştir. Bugün birçok firma online ticaret pazarından pay alabilmek için çevrimiçi ortamlarda ve sosyal ağlarda, tüketiciyle buluşmanın ve markalaşmanın yollarını arar olmuştur.

Günümüzün dijitalleşen dünyasında, tüketimin değişen yüzü olan online ticarette sosyal medya paylaşım ağlarının rolü büyük ölçüde artmıştır. Sosyal medyanın şimdiye kadar görülmemiş derecede tüm topluma nüfuz etmesi, tüketicilerin internet kullanım oranlarının artması ile birlikte sosyal medyada geçirdikleri sürenin artması günümüz ticaret hayatına etkin bir şekilde yansımıştır. Dolayısıyla geçmişin geleneksel satıcıları ve alıcıları yerini online alışveriş sitelerine, web sayfalarına ve sosyal ağlara bırakmıştır (Halis, 2012: 150). Bu noktada internet ticaretindeki en önemli problem güvenlik sorunu olmuştur. Çünkü tüketici gerçekte görmediği, tanımadığı ve fiziksel temasta bulunamadığı birçok kişiye tüm finansal bilgilerini teslim etmektedir. Dolayısıyla suç faaliyetlerin arttığı günümüz internet ortamında tüketici güven sorunu yaşamaktadır. Tüketiciler tarafından sıklıkla dile getirilen söylemler; internette alışverişin tehlikeli olduğu, müşterilerin kişisel bilgilerinin, kredi kartı bilgilerinin, diğer finansal ve kişisel varlıklarının internet ortamında güvende olmadığıdır. İnternette alışverişte bu tür güven sorunlarının aşılmasında etkili olacak temel faktör ise vatandaşların siber suçluları, suç faaliyetlerini ve suç tehditlerini tanıyıp kavramaları neticesinde oluşacak farkındalıkla birlikte siber saldırılara karşı dik durabilmeyi öğrenmek olacaktır.

Siber suçlarla mücadelede daha güvenli bir sanal dünya, beraberinde ulusal ve uluslararası düzeyde daha kârlı bir çevrimiçi (online) ticari hayatı getirecektir (Aksoy ve Sever, 2012: 154-162). Bilişim teknolojilerinin gelişimiyle birlikte artan bilgisayar ve internet kullanımı gerçek dünyanın yanında siber dünya yaratmıştır. Günümüzde dördüncü sanayi devrimi olan Endüstri 4.0, ülke ekonomileri ve çalışma hayatı üzerinde büyük katma değer yaratmaktadır. Endüstri 4.0'ın en önemli kollarından biri siber güvenliktir. Siber güvenlik kavramı bilişim sistemleri ve bilişim suçlarının ana maddesidir. İnternette alışverişin artmasıyla birlikte bilişim suçlarında da hızlı bir artış yaşanmaya başlanmıştır. Siber dünya kişilerin ve toplumların hayatlarında çok önemli kolaylıklar sağlamış olsa da kötü niyetli ve bilinçsiz kullanımlardan kaynaklanan birtakım dezavantajları da beraberinde getirmiştir. Dolayısıyla siber dünyanın gelişimine ayak uyduramayan devletler ve toplumlar bir noktadan sonra mutlaka çağın gerisinde kalmaya mahkûm olacaklardır (Şimşek ve Çınar, 2016: 3). Bu noktada online tüketicilerin siber dünyadaki güvenlik kanaatleri, çevrimiçi gizlilik ve güvenlik farkındalıkları önem kazanmaktadır. Tüketicilerin internet üzerinden yaptıkları alışverişlerde mağdur olmalarını engellemek ve kendilerini güvende hissetmelerini sağlamak amacıyla yapılan bu çalışmada; genç tüketicilerin sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisinin ölçülmesi amaçlanmış bu doğrultuda, online tüketicilere ve online ticari işletmelere yönelik siber alanda gerekli olan bilgi, taktik ve tedbir amaçlı bilgiler aktarılmıştır. Ayrıca yapılan analizler sonucu oluşturulan Online Alışveriş Güvenlik Modeli (OAGM) ile alanında özgün bir çalışma tamamlanmıştır. Sonuçlar kısmında ise yapılan tüm analizlerin değerlendirilmesi neticesinde online güvenlikte akademik ve sektörel yapılanmaya dair kamu ve özel sektörde online güvenlik politikalarına yönelik tavsiyelerde bulunulmuştur.

BİRİNCİ BÖLÜM
SOSYAL MÜHENDİSLİK İLE İLGİLİ TEMEL KAVRAMLAR

1. SOSYAL MÜHENDİSLİK KAVRAMI

Çoğu kişi birçok konuda kandırılma veya aldatılma olasılığının çok düşük olduğunu düşünmektedir. Konu güvenlik olduğunda akıllara ilk gelen genellikle teknik güvenlik tedbirleridir. Oysaki bilgi güvenliğinin sağlanmasında kilit nokta insan faktörüdür. İnsan faktörü, güvenlikte en zayıf halkadır (Mitnick ve Simon, 2017: 3). Bu durumun farkında olan saldırganlar, durumu kendi menfaatleri doğrultusunda yönetmektedirler. Bu saldırganlar, kurbanlarının güvenini kazanarak, kuşku uyandırmadan son derece akıllı ve kurnaz metotlarla ilerleyerek amaçlarına sinsice ulaşıp istedikleri bilgilere kolaylıkla ulaşabilmektedirler. Sosyal mühendislik kavramında saldırgan, insan faktörünü ileri düzeyde kullanan saldırı tekniklerinde, kişiyi etkileme ve ikna etme yoluyla normal şartlarda kişilerin gizlemeleri ve paylaşmamaları gereken bilgileri ustalıkla ele geçirebilmektedir. Tüm gizli ve kamuya açılmaması gereken kişisel bilgileri ele geçirme sanatına sosyal mühendislik denilmektedir. (www.bilgimikoruyorum.org.tr, TÜBİTAK Bilgem, 2018). ABD Federal Araştırma Bürosu olan FBI'ın en çok arananlar listesinde bulundurduğu, uzmanlık alanı bilgisayar korsanlığı olan Kevin Mitnick, sosyal mühendislik kavramını şu şekilde tanımlamıştır; "İnsanların saflığını kullanarak kişileri etkileyerek ikna ederek veya manipüle ederek kritik önem düzeyine sahip bilgilerin ele geçirilmesi" Bu tanıma bağlı kalarak en basit şekilde insanların güvenini kazandıktan sonra kişilere istemedikleri eylemleri yaptırmak olarak da tanımlanabilir (Barışkan, 2017: 3). Ayrıca Kevin Mitnick'in "Güvenlik bir teknoloji sorunu değildir. Bir insan ve yönetim sorunudur" tanımlaması güvenlik anlayışının insan odaklı olması gerektiğini iki cümle ile açıklamaktadır.

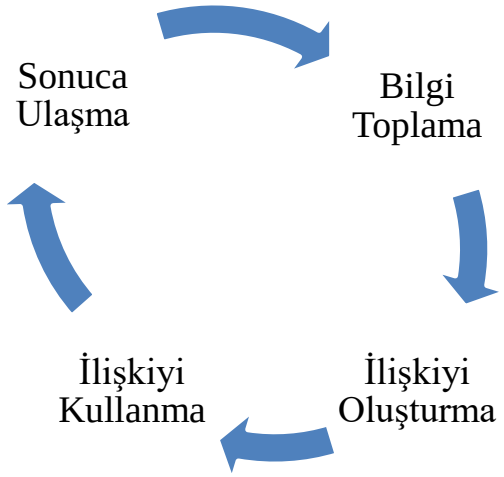
Sosyal mühendislik yöntemleriyle yapılan dolandırıcılık faaliyetlerinin başlangıcı Türkiye'de l948'li yıllara dayanır. Galata Köprüsünü satan Sülün Osman, İstanbul'un dolandırıcısı olarak tarihe geçmiştir. Asıl adı Osman Ziya Sülün olan bu şahıs çeşitli kamu mallarını (İstanbul Tramvayları, Galata Köprüsü, Galata Kulesi,

Kız Kulesi, Dolmabahçe Saat Kuleleri vb.) saf insanlara satarak ün yapmıştır. (https://gazeteistanbul.com/galata-koprusunu-satan-efsanevi-dolandirici-sulun-osman/, 2019, bkz.) Yine 1978 yılında kendilerini televizyoncu olarak tanıtan bazı kişiler, Ankara'nın Çubuk İlçesine bağlı Yazır Köyü sakinlerini, "su getiricez, köprü yaptırıcaz, çeşmeler yaptırıcaz" şeklinde çeşitli vaatlerle dolandırmışlardır.

(https://www.youtube.com/watch?v=xX04wGyHW6Q, 2019, bkz.) O yıllarda internet kullanımı olmadığı için sosyal mühendislik faaliyetleri yukarıda anlatıldığı gibi ilerlemiştir. Aslında sosyal mühendislik yani dolandırıcılık faaliyetleri, tarih boyunca denenmekle birlikte literatüre sosyal mühendislik olarak yakın zamanda geçmiştir. Mitnick'in sosyal mühendislik ile ilgili bir başka tanımlaması şu şekildedir. Sosyal mühendisler, "normalde insanların tanımadıkları birileri için yapmayacakları şeyleri yapmalarını sağlayan kişilerdir". Özetle sosyal mühendisler güvenlik zincirinin en zayıf halkası olan insanları kullanarak amaçlarına ulaşmaktadırlar (Mitnick ve Simon 2017: 3).

1.1. Sosyal Mühendislik Atak Döngüsü

Sosyal mühendislikte yapılan atakların sıralanışı Şekil 1 ile görselleştirilmiştir. Bilgi toplama ile başlanılan eylem devamında ilişkiyi oluşturma, ilişkiyi kullanma ve netice itibariyle sonuca ulaşmak ile sonlandırılmaktadır.



Şekil 1: Sosyal Mühendislik Ataklarının İzlendiği Döngü

Kaynak: Barışkan, M. A. (2017). Türkiye' de siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi, tezinden yararlanarak hazırlanmıştır.

Sosyal mühendis olmak insan psikolojisini en iyi şekilde anlayıp en iyi şekilde yönetebilmek demektir. Bir başka ifadeyle insanları en iyi şekilde etkilemenin yollarını bilerek risk almadan ve çok fazla zaman kaybetmeden en güvenilir şekilde bilgisayar sistemlerine sızabilme kabiliyetidir.

1.2. Sosyal Mühendislik Saldırı Tipleri

Sosyal mühendisler günümüzde statik ortamları (disk, teyp, cd, dvd vb.) kullanarak veya göndericiden alıcıya ulaşan dinamik ortamlardaki verileri, gizlilik kurallarını ihlal ederek ele geçirmektedirler. Saldırganlar yetkileri olmayan gizli bilgilere pek çok illegal yolla erişebilmektedirler. Örnek olarak şifreli dosyaların bulunduğu veri tabanlarının çalınması veya bilgisayar başında çalışan bir kullanıcının, kendisinin fark etmeyeceği şekilde gözetleyerek, şifre ve benzeri bilgilerinin ele geçirilmesi sosyal mühendislik saldırı tiplerinden bazılarıdır (Alagöz, ve Allahverdi, 2011: 51). Bilinen sosyal mühendislik saldırı tipleri aşağıda sıralanmıştır.

1.2.1. Tersine Sosyal Mühendislik

Bir sosyal mühendis başlangıçta hedef bir ağ belirler. Sonrasında hedefte bulunan sisteme karşı bir virüs veya teknik bir saldırı yapıldığını anlatan bir e-posta gönderir. Uygun zaman geldiğinde saldırıyı yapan sosyal mühendis, kendisini güvenlik danışmanı olarak tanıtarak yetkisiz sistemlerle mücadele etmek için kurulmuş bir şirket olduğu algısını yaratarak yardım etme arzusunu açıklar. Bu sistematik çalışmadan sonra hedefte bulunan kişi ya da şirket bu organizasyon ile iletişim kurup bağlantıya geçer. Tersine sosyal mühendisliğin aşamaları Şekil 2'de gösterilmiştir.

Şekil 2: Tersine Sosyal Mühendislik

Kaynak: A.Tosun. (2015). İnsan zafiyetlerini istismar ederek yapılan sosyal mühendislik saldırılarının siber güvenlik ile ilişkilendirilmesi tezinden yararlanarak hazırlanmıştır.

Bu noktadan sonra, saldırgan yani sosyal mühendis aslında kendi ağında istediği gibi çalışmayı hedeflemektedir. Sistemdeki problemi çözmek ve yardım etmek amacıyla girişimde bulunan sosyal mühendisin asıl amacı gizli verileri çalmak ve sisteme ulaşmak için kimlik bilgilerini ele geçirmektir. Özetle sosyal mühendis öncelikle sorun yaratmaktadır. Sonrasında yardım edecek kişi olarak kendini konumlandırmakta, sorunu çözdükten sonra ise kuruluşun güvenilir bir üyesi olmaktadır (Tosun, 2015: 8). Sosyal mühendislerin insanları etkileme yolları Şekil 3 ile görselleştirilmiştir.

Şekil 3: Sosyal Mühendislerin İnsanları Etkileme Yolları

Kaynak: A.Tosun. (2015). İnsan zafiyetlerini istismar ederek yapılan sosyal mühendislik saldırılarının siber güvenlik ile ilişkilendirilmesi, tezinden yararlanarak hazırlanmıştır.

1.2.2. Sırtında Gezdirmek (Piggyback Rides)

Bu tekniği kullanan sosyal mühendis yetkili bir çalışan edasında davranmaktadır. Hedefinde bulunan bir binaya giriş imkânı bulunan bir çalışanı takip eder. Örneğin elindeki ağır kutu nedeniyle kapıyı açamadığını ve bu sebeple rozetine ulaşamadığını ima ederek hedefindeki bina çalışanı gibi davranıp insanlardan yardım isteyerek binaya girmeye çalışır. Böyle bir durumda yetkili çalışan sosyal mühendise kapıyı kendi elleriyle açabilmektedir (Tosun, 2015: 9).

1.2.3.Teknik Yetkili Gibi Konuşmak (Kimliğe Bürünme, Techie Talk)

Böyle bir saldırıda sosyal mühendis yardım masası operatörü çalışanı gibi davranmaktadır. Örneğin; çalışana telefonla ulaşır, şirketin bilgi teknolojileri personeli edasında bir konuşma yaparak çalışandan şifresini güçlü bir şifre ile

değiştirmesini talep eder. Bu konuşma esnasında son derece teknik terimler kullanarak çalışanı yetkili olduğuna dair ikna edici bir konuşma yapar. Bu konuşma esnasında hedefinin diğer bir deyişle kurbanının şifresini ele geçirerek kendi menfaati doğrultusunda amacına ulaşmaya çalışmaktadır (Tosun, 2015: 10).

1.2.4.Kimlik Avı (Yemleme, Oltalama, Sazan Avlama, Phishing)

Kimlik avı saldırganın, sahtekârlıkla elde etmeye çalıştığı bir sosyal mühendislik aracıdır. Saldırgan, güvenilir bir üçüncü tarafın kimliğine bürünerek mağdurun hassas bilgilerini ele geçirmeye çalışır (T Jagatic, N Jahnson, ve diğerleri. 2005: 1). Örnek olarak bir kimlik avcısı çok sık kullanılan bir hizmetin kesintiye uğramasına sebep olarak aşırı kimlik doğrulama hataları oluşturup, kurbanın şifresinin kilitlenmesine neden olacak bir güvenlik tehdidi algısı oluşturup bu durumu kurbanına e-mail yoluyla ileterek güvenini kazanmaya çalışır. Böyle bir bilgi kurban tarafından memnuniyetle karşılanmaktadır. Bir başka örnekte kimlik avı saldırganı, internet tarayıcısı üzerinden kurbanının alışveriş tercihleri ve tarihleriyle ilgili bilgi edinerek kurbanını kendi menfaati doğrultusunda yönlendirebilmektedir. Kimlik avı saldırganı, hem teknik hem de sosyal güvenlik açıklarından faydalanmaktadır. Saldırgan, hedefinde bulunan kişilerin kamuya açık kişisel bilgileri elde etmek için sosyal ağlardan faydalanmaktadır. Saldırgan, gücünü artırmak için kurbanının kullandığı sosyal ağlardan, yakınlarıyla olan sosyal bağlantılarını tespit edip e-posta yoluyla kendisini yakınıymış gibi tanıtıp harekete geçmektedir. Bu yöntem bir kimlik avı saldırganı için son derece akıllıca ve kolayca kullanılabilen çok etkili bir yöntemdir (Aktaran; T Jagatic, N Jahnson, vd. 2005: 1-2).

TÜRKİYE CUMHURİYET MERKEZ BANKASI

Sayın müşterimiz;
Ağustos ayından itibaren T.C Merkez Bankası'nın aldığı karara dayanarak tüm internet bankacılığı sistemlerinde TCMB'ye bağlı tüm bankaların (AKBANK, ANADOLU BANK, ASYA BANK, GARANTİ BANKASI, FORTIS BANK, FİNANSBANK, HSBC BANK, ŞEKERBANK, T.C İŞ BANKASI, TURKEYFINANS, TEB, TEKFENBANK, TEKSTILBANK, KOÇBANK, KUVEYTTÜRK, YAPI VE KREDİ BANKASI, VAKIFBANK) SSL yazılımları ve internet bankacılığına hizmet eden bilgisayarlar güncellenmektedir. Bu güncelleme nedeniyle sistemler yenileneceğinden, hem aktif internet bankacılığı kullanıcılarını tespit etmek, hem de güvenlik açısından sizlere daha iyi bir hizmet verebilmek için bilgilerinizi teyit etmeniz gerekecek ve yeni veritabanımıza kaydedilecektir. Bilgilerinizin teyidi ve yeni veritabanına eklenmesi zorunludur. Teyit işlemi yapılmadığı taktirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilir, ya da TCMB Ankara Şubesi'nden bilgilerinizi teyit edebilirsiniz.

İnternet üzerinden teyit işlemini yapmak için aşağıdaki linke tıklayın;
http://tcmb.gov.tr.teyit.merkezbanka.org/guncelleme.php?sid=d3fd99df91df76dfs

DİKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB üzerinden gelmeyen mailleri güvenliğiniz için bize bildirin. Teyit işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Bütün teyit işlemleri TCMB tarafından organize edilmektedir. Teşekkürler.

Adres: İstiklal Cad. 10 Ulus, 06100 Ankara, Türkiye
Telefon : (312)310 3646
©TCMB 2006

Şekil 4: TCMB Konulu Kimlik Avı Denemesinde Kullanılan E-Posta Örneği

Kaynak: Alataş, Ş. & Atan, M. (2007). s.3. http://ab.org.tr/ab07/bildiri/154.pdf

Şekil 4 incelendiğinde internet adresinin taklit edilerek IP adresinin saptırılmaya çalışılmasıyla internet kullanıcısına saldırıda bulunulduğu tespit edilmektedir. Merkezbanka.org alan adı üzerinden http://tcmb.gov.tr.teyit..merkezbanka.org adresi ile kullanıcılar aldatılmaya çalışılmıştır. Fakat birçok kullanıcı TCMB'nın resmi internet sitesinin http://www.tcmb.gov.tr olduğunu bilmektedir. Verilen örnek olay tuzak bir saldırıyı özetlemektedir. Daha başarılı yemleme tekniklerinde kullanılan internet adresleri, kullanılan farklı sistemler sayesinde kullanıcıları inandırma konusunda daha başarılı olabilmektedir. (Alataş, 2007: 6).

1.2.5. Balina Avı (Whaling)

Sosyal mühendislikte saldırganların özellikle CEO'ları hedef aldıkları saldırı türüdür. Şirketlerin resmi web sitelerinde üst düzey şirket yetkililerinin biyografilerinde, eğitim bilgilerinden hobilerine kadar kişiye özel tüm bilgiler yayınlanabilmektedir. Bir sosyal mühendis site üzerinden yöneticiye ait her bilgiyi

ustalıkla kötüye kullanma potansiyeline sahiptir. Örnek olarak basketbola ilgisi olan bir yöneticiye, mezun olduğu okuldan basketbol turnuvasına katılması yönünde bir e-posta davetiyesi gönderildiğini varsayalım. İlgili yönetici gelen mail üzerinden rezervasyon işlemlerinin yapılması amacıyla bir web sitesine yönlendirildiğinde kredi kartı bilgilerinin, yönlendirilen siteye girmesiyle birlikte sosyal mühendiste amacına ulaşmış olacaktır. Giderek popüler olan balina avında, dikkatsizce kullanılan bu bilgiler kişileri ve şirketleri hedef haline getirmektedir (Tosun, 2015: 1-2). Şirketlerin genel müdür ve üst düzey yöneticilerine yöneltilen bu saldırın FBI verilerine göre 2015 yılından bu yana yüzde 270 oranında arttığı ifade edilmektedir. Son yıllarda sosyal mühendislik saldırılarının bu yönde artış göstermesi, siyah şapkalı bilgisayar korsanlarının iştahını kabartmaktadır (https://home.kpmg.com, 2018).

1.2.6. Telefon Oltalaması (Vishing)

Hedefte bulunan kurbana gönderilen e-postada, sahte link yerine bir telefon numarası gönderilmesidir. Hedefte bulunan kişinin belirtilen numarayı arayarak kişisel bilgilerini güncellemesi amaçlanmaktadır (Gündüz ve Daş, 2016: 11-18).

1.2.7. Kimlik Hırsızlığı

Hedefte bulunan şahsa ait kişisel bilgilerin, başkaları tarafından yetkisiz kullanılması suretiyle yapılan dolandırıcılık yöntemidir (Gündüz ve Daş, 2016: 11-18).

1.2.8. Sosyal Medya Ağı (Social Media Networking)

Facebook, Twitter, Instagram vb. siteler sosyal mühendislerin en iyi bilgi topladıkları sosyal ağlardır. Sosyal mühendisler sadece bu sayfaları tıklayarak hedefleri hakkında çok fazla bilgi toplayabilmektedirler. İnsanların nerelerde çalıştıkları, hobileri, neleri sevdikleri ya da sevmediklerinden, korkularına ve inançlarına dair birçok konu hakkında psikolojik analiz yapıp kişiler hakkında bilgi sahibi olan sosyal mühendisler, hedefte bulunan kişiye göre taktik değiştirip harekete geçmektedirler. İnsanların özel hayatlarını sosyal ağlarda paylaşmaya istekli olmaları, sosyal mühendislerin iştahını kabartıp işlerini kolaylaştırmaktadır. Kullanıcıların sosyal ağlarda özellikle yer ve konum bildirme servislerine izin vermeleri, sosyal mühendislerin daha rahat keşifte bulunup saldırıya geçmesine olanak sağlamaktadır. Hedefinde bulunan kişiye arkadaşlık isteği göndermek

suretiyle online arkadaşlık kuran bir sosyal mühendis, kurbanının eğitim durumu, yaşı, mesleği, çalıştığı kurumu ve hobileri hakkında bilgi sahibi olduğunda kullanacağı taktik değişecek ve kişiye göre kendini güncelleyerek saldırıya geçecektir (Tosun, 2015: 13)

1.2.9. Zihin Dili Programlanması (Mind Language Programming - MLP)

1970'li yıllarda ABD' de geliştirilen (MLP- Zihin Dili Programlaması) özetle çeşitli bilim dallarının ortak görüş bildirdiği zihni kullanma kılavuzudur. Günümüzde psikoterapi, kişisel gelişim ve iletişimde geniş uygulama alanları nedeniyle kabul görmektedir. Bireylerin fiziksel ve zihinsel performanslarını etkileme ve değiştirme konusunda stratejik ve teknik kolaylık sunan sisteme zihin dili programlaması denilmektedir (Tat, 2007: 57).

Bu teknikte sosyal mühendis, kendi beden dilini manipüle etmeye çalışır. Üzerinde çalıştığı kişiye çeşitli yollarla bilinçaltı mesajları vererek, kişinin sosyal mühendise karşı olumlu duygulara sebep olmasına ve sosyal mühendise karşı, yakınlık hissetmesine neden olacak duygular yaratılmak istenmektedir. Bir örnekle açıklamak gerekirse, sosyal mühendis vücut dilini hedefinde bulunan kurbanının vücut dili ile eşleştirerek harekete geçer. Daha sonra kurban ile ses seviyesinin hızı, solunum hızı, kullandığı kelimeler, aksan ve kelime dağarcığını eşleştirir. Sonraki süreç dokunsaldır. Hedef de bulunan kişiye hafifçe dokunularak yakınlık kurulmaya çalışılır. Bu eşleştirmeler ile bilinçaltı düzeyinde kurban ile bir uyum yakalanmaya çalışılmaktadır. Amaç duyusal, görsel, işitsel ve dokunsal duyuları kullanarak kişilerin sosyal mühendis hakkında olumlu duygulara sahip olmasını sağlamaktır. Tüm bu eylemler neticesinde bir şirketin sırları veya kritik önem düzeyine sahip bilgileri hakkında iz sürülebilmektedir. Çünkü kişiyle doğrudan iletişime geçilmesi için tüm adımlar atılmış olmaktadır (Tosun, 2015: 14).

Tüm bilgiler ışığında özetle bir sosyal mühendis aslında aynalama tekniğini kullanmaktadır. Hedefte bulunan kurbanın hareketlerinin tamamen taklit edilmesiyle birlikte sosyal mühendisi kendisiyle özdeşleştiren kurban, başka bir ifadeyle sosyal mühendise sempati duyarak güvenmektedir. Bu noktadan sonra bilgi güvenliği tehlikeye girmektedir.

1.2.10. Cinsiyet Cazibesini Kullanmak

Bir sosyal mühendis, hedefindeki kişi kadın ya da erkek olsun fark etmeksizin kurbanın, karşı cinsten etkilenme konusunda savunmasız olduğunu ve zafiyet yaşadığını fark ettiği anda bu tekniği yüksek başarı oranı ile mağdurun duygularını etkilemeye yönelik kullanarak istediği sonuca ulaşmaktadır. (Tosun, 2015: 15).

1.2.11. Dostça Yapılan Toplantılar ve Konuşmalar

Sosyal mühendisin hedefindeki kişiyi, iş dışında sosyal olarak bulunduğu ortamlarda takibe almasıdır. Spor kulüpleri, kafeler, barlar, eğlence merkezleri örnek olarak gösterilebilir. Konu çarpıcı bir örnekle açıklanabilmektedir. Örneğin hedefte bulunan kişinin devamlı olarak vakit geçirdiği bir gece kulübünü tespit eden bir sosyal mühendis, kişinin sarhoş olduğu anı kollayıp almak istediği tüm bilgileri (Örnek olarak ticari sırları ve şifreleri) kişi sarhoşken alabilmektedir. Hatta garson ya da barmene rüşvet vermek suretiyle de istediği sonuca ulaşabilmektedir. Bu tür mekânlar sosyal mühendisler için bulunmaz bir nimettir. Çünkü ofis ortamına göre hem saldırgan hem de kurban daha rahat tavır sergilemektedir (Tosun, 2015: 15).

1.2.12. Omuz Sörfü – Omuz Gezintisi (Shoulder Surfing)

Kullanıcıların sisteme eşirim için kullandıkları şifre veya parolaların, sisteme giriş sırasında sosyal mühendis tarafından gözetlenip keşfedilmesine omuz sörfü denilmektedir. Ayrıca kullanıcılar bu tür gizli bilgilerini unutmamak maksadıyla bir ajanda veya not defterine not ettiklerinde de bu tür materyallerin sosyal mühendis tarafından incelenmesi neticesinde gerekli olan tüm veriler ele geçirilmiş olacaktır. (Yalçın ve Gürbüz, 2015: 2)

1.2.13. Çöp Dalışı (Dumpster Diving)

Sosyal mühendislerin hedefindeki kişi ve şirketler hakkında işe yarar bilgilere ulaşmak maksadıyla gizlice çöplükleri karıştırıp bilgi toplamasına çöp dalışı denilmektedir (Gündüz ve Daş, 2016: 11-18)

2. SOSYAL MÜHENDİSLERİN ÖZELLİKLERİ

Sosyal mühendisler saldırılarını çoğunlukla internet ve telefon üzerinden gerçekleştirmektedir. Sosyal mühendis olarak adlandırılan saldırganların belirgin kişisel özellikleri Tablo 1 ile görselleştirilmiştir.

Tablo 1: Sosyal Mühendislerin Özellikleri

Sayı	Sosyal Mühendislerin Belirgin Özellikleri
1.	Çoğunlukla interneti ve telefonu kullanırlar.
2.	İyi giyinirler ve yardımsever davranışlarda bulunurlar.
3.	İkna kabiliyetleri yüksektir ve söz sanatlarını kullanmada ustalaşmışlardır.
4.	Amaçları, hedeflerinde bulunan kişilerin güvenini kazanmaktır.
5.	İnsanların, açgözlülük, korku, şehvet, suçluluk duygusu, ahlaki zorunluluk gibi insani zafiyetlerini sömürürler.
6.	Titizlikle hazırlanmış bir plan çerçevesinde kibar, etkileyici ve sempatik bir kişilik sergilerler.
7.	Yalan söyleme konusunda tereddütleri yoktur ve bunu ustalıkla yaparlar.
8.	Masum soruların arasına anahtar soruları katarak bilgi edinmede yeteneklidirler.
9.	Kullandıkları psikolojik yöntemler, acındırma, suçluluk hissettirme, sindirme, acil durum yaratma, yardım isteme ve yardım etmek istemektir.
10.	Teknik bilgi olarak donanımlı olmayabilirler fakat bir siber saldırgan tüm sosyal mühendislik yeteneklerine sahiptir.

Kaynak: Gündüz, M.Z.& Daş, R.Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri, makalesinden derlenerek hazırlanmıştır.2016, s.3

2.1. Sosyal Mühendislerin Bilgi Toplama Kaynakları ve Düşünme Biçimleri

Bir sosyal mühendisin, saldırıya geçmeden önce üzerinde çok iyi düşünülmüş bir ön hazırlık ve planlama aşaması bulunmaktadır. Bilgi toplama aşamasına geçildiğinde ise saldırgan, düşünme şeklini değiştirmek ve hedefte bulunan kişinin dünyasına göre bir yaklaşım sergilemek zorundadır. Sosyal mühendisler için ilk görünüşte anlamsız olan bilgiler bile büyük bir bilgi güvenliği zafiyetlerine sebep olabilmektedir. Örnek olarak hedef şirketin üst düzey yöneticilerinden birini bir günlüğüne takip etmek suretiyle, kişinin yemek yediği ve kahve içtiği yerleri tespit ettikten sonra bu mekânlarda tesadüfen iletişime geçilmiş gibi bir izlenim yaratılarak hedefte bulunan kişiden, sosyal mühendis için gerekli olan tüm bilgilerin alınması mümkün hale gelmektedir. Taraflar arasında, bulunulan ortamda tesadüfen başlamış süsü verilen iletişim, devamında posta yoluyla sürdürülebilmekte ve akabinde kişisel bilgilerin taraflar arasında paylaşılmasıyla saldırı sonlandırılmaktadır. Ayrıca bu saldırı esnasında veri toplamak için kullanılan tüm kaynaklar ayrı ayrı test edilebilmektedir. İyi bir sosyal mühendis böyle bir iletişim ortamında hedefinde bulunan taraf hakkında, her türlü bilgiye sahip olabilmekle birlikte hedefine yeteri kadar zamanda ayırabilmektedir (Hadnagy, 2011: 56 -59).

Sosyal mühendis yukarıda açıklanan bilgi toplama evresini tamamladıktan sonra hedefine yönelik plan hazırlama evresine geçmektedir. Elde edilen bilgiler, plana en iyi şekilde entegre edilir. Sonrasında operasyona geçmek için en iyi zaman

kollanır. Operasyon sırasında sosyal mühendis kurbanının her türlü hamlesini düşünmektedir. Mühendis kurbanından aldığı geri bildirimle hareket edip anlık karar verir ve hızlı bir tavır sergiler. Bu evrede empati ön plana çıkmaktadır. Çünkü her şey planlama dâhilinde gitmeyebilmektedir. Operasyon tamamlandığında iki durum söz konusudur. Başarılı ya da başarısız olunmuştur. Operasyon başarıyla bitirilse bile saldırı henüz bitmemiştir. Kurbanın, saldırgandan şüpheleneceği ve saldırgana karşı bir yaptırım içine gireceği düşünülen operasyonlarda, sosyal mühendis herhangi bir şüpheye yer vermemek için kurbanla iletişimini sürdürmektedir. Bu iletişim doğaçlama gerçekleşir amaç şüpheyi azaltmaktır. Operasyon başarısızlıkla sonuçlanmış olsa bile sosyal mühendis, hatalarını dürüst bir şekilde değerlendirip tecrübe kazanmış olacaktır. Fakat her sosyal mühendis başarı odaklıdır (www.turkhackteam.org, 2014).

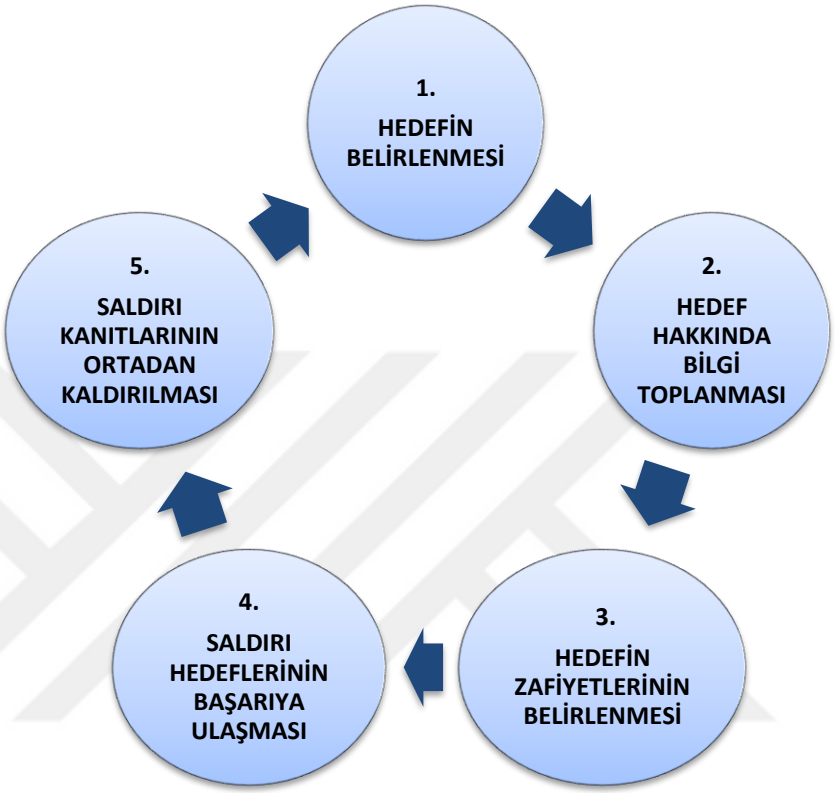
Şekil 5'de sosyal mühendislik saldırılarında kullanılan bazı donanımların fotoğrafları görülmektedir.

Şekil 5: Sosyal Mühendislik Saldırılarında Kullanılan Bazı Donanımlar

Kaynak: Ünal Tatar, "Sosyal Mühendislik Saldırıları", 4. Ağ ve Bilgi Güvenliği Sempozyumu, TÜBİTAK Bilgem, 25-26 Kasım 2011, s.11). (www.emo.org.tr, 2018)

Şekil 6 ile sosyal mühendislik saldırında saldırganın, hedefine yönelik saldırısının aşamaları ve detayları yaşam döngüsü ile görselleştirilmiştir. Saldırının başlangıç aşamasında ilk olarak hedef tespit edilmektedir. Akabinde hedef hakkında

bilgi toplanır. Elde edilen bilgiler ve toplanan veriler neticesinde kurbanın zafiyetleri belirlenerek saldırı gerçekleşir. Son aşamada ise saldırgan kanıtları ortadan kaldırmaya çalışacaktır.



Şekil 6: Sosyal Mühendislik Saldırılarının Yaşam Döngüsü

Kaynak: Gündüz, M.Z.& Daş, R. Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri, makalesinden yararlanarak hazırlanmıştır. 2016, s.2.

2.2. Sosyal Mühendislik Saldırısında Örnek Senaryo

Aşağıdaki örnek senaryo işe yeni başlayan bir personele yapılan sosyal mühendislik saldırısını anlatmaktadır. Bir kurumda işe yeni başlayan personel işe başlama sürecinden önce bilgi güvenliği eğitimlerinden geçirilmeden ve bu eğitimlerde gerekli görülen yeterliliğe ulaşmadan işe başlatılmış ise çalıştığı kurum için büyük bir risk oluşturmuş demektir. Şekil 7'de örnek senaryo yazmaktadır.

- Melda …….. ile mi görüşüyorum?
- Evet
- Merhaba Melda. Ben bilgi işlem teknik servisinden Çağdaş,
- Evet?
- Bizim birimden sizinle şirket güvenlik politikaları ve uygulamaları hakkında görüşen oldu mu?
- Hayır sanmıyorum
- Peki hemen başlayalım. Öncelikle hiç kimsenin şirket dışından getirdiği programları yüklemesine izin vermiyoruz. Özellikle lisansı olmayan yazılımlar solucan ve virüs içerir.
- Tamam.
- Şirket e-posta uygulamamızdan haberdar mısınız ?
- Hayır.
- Şuanda kullandığınız e-posta adresi nedir?
- Melda@herhangibirkurum.com.tr
- Kullanıcı adı olarak Melda ismini mi kullanıyorsunuz?
- Hayır K alt çizgi Kadir ismini kullanıyorum.
- Tüm yeni çalışanlarımızı bu konularda uyarıyoruz! Tanıdığınız insanlardan geliyor gibi görünen e-postalar yine virüs ve solucan içerebilir bu sebeple gönderici olarak görünen kişinin, mesajı size gerçekten gönderip göndermediğini her zaman kontrol etmeniz gerekir.
- Evet bunu duymuştum.
- Güzel. Her doksan günde bir şifrenizi değiştirmeniz gerekiyor. Doksan gün dolana kadar bekleyebilirsiniz. Fakat şifrenizin güçlü bir şifre olup olmadığından emin olmamız gerekiyor. Hem sayı hem de harf içeren bir şifremi kullanıyorsunuz?
- Hayır.
- Bunu düzeltmeliyiz. Şuanda kullandığınız şifre nedir?
- Oğlumun adını kullanıyorum, Berk.
- Bu şifre hem çok kısa hem de aile bireylerinin isimlerini içeren şifreler seçmemelisiniz. Şifrenizi yenilediğinizde benim yaptığımın aynısını yapabilirsiniz. Örneğin şifrenin sonuna içinde bulunduğumuz ayı ekleyin.
-Bunu hemen yaparsam mart ayı için sıfır-üç mü yoksa sadece üç mü kullanayım?
- Size kalmış nasıl isterseniz. Hangisi sizin için daha rahatsa onu kullanın.
- Anladım. Berk-03 daha iyi
- Peki. Değişikliğin nasıl yapılacağı konusunda yardımcı olmamı ister misiniz?
- Hayır gerek yok nasıl yapılacağını biliyorum.
- Güzel son olarak şunu söyleyeyim. Bilgisayarınızda virüs yazılımı var yalnız bunu güncel tutmamız önemli. Bilgisayarınız arada bir yavaşlayabilir. Bu anlarda bile otomatik güncellemeyi devre dışı bırakmayın tamam mı?
- Tabii dikkat ederim.
- Çok iyi. Bir sorununuz olduğunda bilgi işlem teknik servisiyle bağlantıya geçin.
- Olur. Teşekkür ederim.
- İyi günler, iyi çalışmalar Melda hanım.
- İyi günler

Şekil 7: Sosyal Mühendislikte Örnek Senaryo

Kaynak: MITNICK. D. KEVIN and SİMON L.WİLLİAM (2017) Aldatma Sanatı, Bilgi Güvenliğinde İnsan Faktörünün Kontrolü Kitabından Derlenerek Hazırlanmıştır. 8. Basım . ODTÜ Yayıncılık.Ss.57-58.

3. SOSYAL MÜHENDİSLİK SALDIRILARINA KARŞI ALINACAK TEMEL BİREYSEL GÜVENLİK ÖNLEMLERİ

Bilişim sistemlerinde güvenliğin sağlanması sadece teknolojik çözümlerle mümkün değildir. Çünkü en güvenilir sistemlerin arkasında bile insan bulunmaktadır. Güvenlik zincirindeki en zayıf halka ise insandır. Bu sebeple değişik zamanlarda değişik davranışlar sergileyen insanoğlu, güvenlik sürecinde çeşitli zafiyetler gösterebilmektedir. Aşağıda bu zafiyetlerin önlenmesi için çeşitli önlemler ortaya konulmuştur (Gündüz ve Daş, 2017: 14).

Birçok bilim kurgu filminde insanlara karşı makinelerin savaştığı senaryolar görülmektedir. Bu filmlerde savaşları bazen makineler bazen insanlar kazanmaktadır. Yalnız bu tür filmlere çoğu zaman insanoğlunun istemeyerek kendi yıkımını hazırladığı senaryolar konu edilmektedir. Teknolojik bir yolda çılgınca koşan insanoğlu, kendi faydasını maksimize etmek ve yeni teknolojilere uyum sağlayabilmeyi geç öğrendiğinden bu süreçte kendi insanlığını da unutabilmekte veya kaybedebilmektedir. 1960'lı yıllarda günümüz dünyası yazılmış olsaydı muhakkak inanılmayacak bir bilim kurgu filmi olarak kabul edilebilirdi. Günümüzde insanoğlunun ve toplumun görülmemiş bir şekilde yeniden inşa edilmesi iyi bir yaşam ve iyi bir toplum için birçok teknolojinin ciddi ve titiz kullanımını gerektirmektedir. İnsanoğlu yaşamını sürdürdüğü ilk günden bugüne kadar teknolojiyle şekillenmiş ve bu teknolojiyi kullanarak diğer insanları da şekillendirmek suretiyle etkisi altında bırakmıştır. Hatta kullanılan son teknolojilerle, radyo ve televizyon gibi kitle iletişim araçlarıyla, insanların makinelere dönüştürülmesi konusunda önemli mesafeler alınmıştır. Tüm bu entegrasyon çabalarına rağmen teknolojik yollarla, insani yolların ölçeği ve kapsamı henüz kesişmemiştir. Bilgi ve iletişim teknolojilerinin her yerde konuşlandırılması ve nesnelerin interneti tüm sistemlerin otomasyonunu sağlamıştır. Bu otomasyon teknolojinin gerektiği her yerdedir. Günümüzde teknolojinin ve sosyolojinin gerektirdiği çevresel faktörlerin kapsamı benzeri görülmemiş bir mühendislik çerçevesinde değerlendirilmelidir. Tüm bu değerlendirmeler akıllara şu soruları getirmektedir;

- Teknoloji sistemleri insanlığımızı ne zaman değiştirir ya da azaltır?

- Bizleri insan yapan nedir? İnsanlar ne zaman ve nasıl programlanabilir?
- Ne olduğunu nasıl tespit edebiliriz ve ne yapabiliriz?

Teknoloji ve insanlık kavramları soyut ve karmaşık kavramlardır. Bu sebeple birçok engel bulunmaktadır. Bu noktada teknolojinin getirilerini doğru ölçüp değerlendirmek için gerekli araçlara ve bilgiye sahip olmamız gerekmektedir (Frischmann, 2014: 2-3). Bu açıklamalar doğrultusunda sosyal mühendislik saldırılarına karşı en iyi savunmanın farkındalık olduğu bilinmektedir. Kişiler sosyal mühendisliğin ne kadar kolay kullanılabileceği konusunda eğitilmeli tehdit varsa tespit edilerek karşıt önlemler alınmalıdır. Bu noktada farkındalık eğitimleri en iyi güvenlik çemberini oluşturmaktadır. Ayrıca farkındalık üzerine posterlerin yaygın kullanımı da saldırılara karşı etkili bir yöntem olacaktır. Fiziksel erişim halinde saldırılara karşı durabilmek için karşı tarafa sorular sormaya da istekli olmak gerekir. Çünkü soru sormak karşı tarafı ölçmenin ve değerlendirmenin en iyi yoludur. Yüz ve vücut ifadeleri de insanlarla iletişim kurma yollarından biridir. Ancak karşı taraf sizinle telefonda görüşmekte ise diğer iletişim kanalları yoluyla fikir sahibi olunamayacağından şüpheliden, ulaşılabilecek bir telefon numarası istenerek alınan numaradan karşı tarafın sizin tarafınızdan aranması suretiyle izlenecek yol, daha güvenilir bir yol olacaktır. Şunu da özellikle belirtmek gerekmektedir. Bu telefon numarası hiç bir şeyi garanti etmemektedir. Fakat potansiyel bir sosyal mühendisin bu sorudan sonra tekrar sizinle irtibata geçme olasılığı düşecektir (Long, 2008: 112-113).

Sosyal mühendislikte herkes başarılı bir şekilde hedeflenebilmektedir. Bu kavram üzerinde bir dizi olay yaşanmaktadır. Bu noktada yaşanan güvenlik probleminde bir diğer öncelikli sorun, bilgi güvenliğini tamamlama ihtiyacı ve insan unsuruna yönelik korunma ve karşıt önlemleri kullanmada yaşanan bilgi eksikliğidir.

Sosyal mühendislik saldırılarına en iyi örneklerden biri günümüzde yaygınlaşan kimlik avı saldırılarıdır. Online diğer adıyla çevrimiçi ortamlarda gerçekleşmekte olan bu saldırılarda kişisel bilgilerin paylaşımı amaçlanmaktadır. Saldırgan genellikle kurbanın mail adresine bir e-posta ya da reklam gönderir. Sık kullanılan sitelerin taklitleri de kişinin mailine gönderilebilmektedir. Örnek olarak gönderilen bir e-posta, sanki bankadan geliyormuş gibi bir izlenim yaratılarak kişiden banka hesap numarasını onaylaması istenebilmektedir.

Kimlik avı sitelerinin isteyebileceği bilgiler şunladır;

- Kullanıcı adları ve şifreler
- Vatandaşlık numaraları
- Banka hesap numaraları
- PIN'ler (Kişisel Kimlik Numaraları)
- Kredi Kartı Numaraları
- Annenizin kızlık soyadı
- Doğum gününüz

Bir site tarafından kişisel bilgiler istenildiğinde çok dikkatli olunmalıdır. Sitenin yasallığı doğrulanmadan asla bilgi verilmemelidir. E-posta adreslerine gönderilen e-posta bağlantısına tıklamadan önce başka bir pencereden, ulaşılmak istenen siteye erişim sağlanıp sitenin güvenilirliği doğrulandıktan sonra e-postanın açılması en güvenilir yol olacaktır. Güvenilir siteler asla şifreleri veya kişisel bilgileri isteyen iletiler göndermemektedirler. Çevrimiçi bilgi dağıtıcısı ve arama motoru olan Google, arama yardım sayfasında, kimlik avı saldırılarını önleme ve bildirmeye yönelik detaylı bilgilendirme yapmıştır. Ayrıca bu saldırıdan korunmak için yararlanabilinecek diğer yöntemler kimlik avı dolandırıcılıkları başlığı altında; şikâyetler, aldatıcı ve haksız ticari uygulamalar bağlantılı " http://www.ftc.gov/ftc/contact.shtm " Federal Ticaret Komisyonu web sitesini irtibat adresi olarak göstermiştir. Amerika Birleşik Devletleri dışındaki bir ülkede bulunan şirketlere yönelik şikâyetlerde ise "http://www.econsumer.gov" bağlantılı web sitesini irtibat adresi olarak göstermiştir. (https//support.google.com, 2018).

Bir şirket ya da kurum, paranın satın alabileceği en iyi güvenlik teknolojilerini satın almış olabilir, uzmanların önerdiği en iyi güvenlik uygulamalarını çalıştırabilir, en iyi sistem yapılandırmasını ve en iyi güvenlik yamalarını kullanarak dikkatli ve tedbirli davranabilir. Fakat bu şirket yine de savunmasızdır. Çünkü güvenliğin en zayıf halkasını insan oluşturmaktadır (Mitnick and Simon 2017: 3).

Sosyal mühendis denilen kişi, kurbanın düşünmesine fırsat vermeden hareket etmesini sağlayan kişidir. Örnek olarak kurbanın e-posta adresine gönderilen bir mail, konu hakkında aciliyet yaratıyorsa amaç kişinin düşünmesini engelleyerek bu ortamdan istifade etmektir. Bu sebeple kişi son derece serinkanlı davranmalı, öfke,

telaş ve heyecana kapılmadan kendini denetleyebilecek düzeyde soğukkanlı olmalıdır. Sosyal medya üzerinden yapılan bilgi paylaşımları başka bir kritik noktadır. Kişilerin bu platformlarda kişisel bilgilerine yer vermesi veya bir anlık dalgınlıkla yaptıkları bir paylaşım, kendileri ve çevreleri adına çok pahalıya patlayabilmektedir. Bu saldırganlar, saldırı sırasında kuvvetli referanslar kullanarak güvene dayalı arkadaşlık ilişkileri kurmaya çalışmaktadırlar. Bu gibi durumlarda tanınmayan kişilere karşı son derece uyanık ve hassas olunmalıdır (www.turkhackteam.org).

Genel anlamda sosyal mühendislik saldırılarına karşı alınabilecek temel bireysel önlemler şunlardır;

- Şifre korumalı ekran koruyucular kullanılmalıdır.
- Kişisel şifreler ve kişiye özel bilgiler (kredi kartı numarası ve şifresi vb.) bir başkasına söylenmemelidir. Bu tür özel bilgiler, kâğıtlara yazılıp ortalıkta bırakılmamalıdır.
- Bilgi güvenliği için birden fazla e-posta kullanımının faydalı olduğu bilinmelidir.
- Kritik önem düzeyine sahip kişisel bilgiler (TC kimlik numarası, doğum yeri, doğum tarihi, telefon numarası vb.) sosyal medyada (Instagram, Twitter, Facebook vb.) kesinlikle paylaşılmamalı, bu bilgilere kötü niyetli insanlarında ulaştığı unutulmamalıdır. Sosyal mühendisliğe karşı alınacak en etkili yol insanların kendi kendilerine oluşturdukları güvenlik duvarlarıdır.
- Kalabalık mekânlarda, cep telefonu veya bilgisayar üzerinden veri girişi yapılırken omuz sörflerine (saldırganın sizi fark edemeyeceğiniz şekilde gözetlemesi) karşı uyanık olunmalıdır.
- Tanınmayan kişilerin isteklerine, telefon ve internet gibi ortamlarda yanıt verilmemeli her zaman şüpheci davranılmalıdır.
- Fiziksel temasın mümkün olduğu ortamlarda, tanımadık kişilerden gelen isteklere karşı temkinli olunmalı, sosyal mühendislerin en çok yardım talebini kullandıkları unutulmamalıdır.
- Telefonda kendisini polis, asker, savcı vb. şekilde tanıtarak bankaya para yatırılması gerektiğini söyleyen kişilerle karşılaşıldığında 155 polis hattına ihbar edilmelidir.

- Kişisel bilgileri ele geçiren sosyal mühendisler, bu kişiler adına habersizce telefon hatları çıkartabilmektedirler. Kişiler kullandıkları telefon numaralarının kontrolünü e-devlet şifresi ile mobil hat sorgulamadan takip etmelidir (Gündüz ve Daş, 2016: 5).
- Kişisel verilerin çalınması veya kişisel verileri içeren cihazların kaybolması durumunda kişisel verileri kanuna aykırı işleyen ve kullanan kişileri şikâyet etmek için Kişisel Verileri Koruma Kurumunun ALO 198 numaralı Veri Koruma Hattı ile iletişime geçilmelidir. (https://www.kvkk.gov.tr/Icerik/4118/Videolar, bkz.2019)

4. SOSYAL MÜHENDİSLİKTE KURUMSAL RİSK BİLİNCİ VE SİSTEM DEĞERLENDİRMELERİ

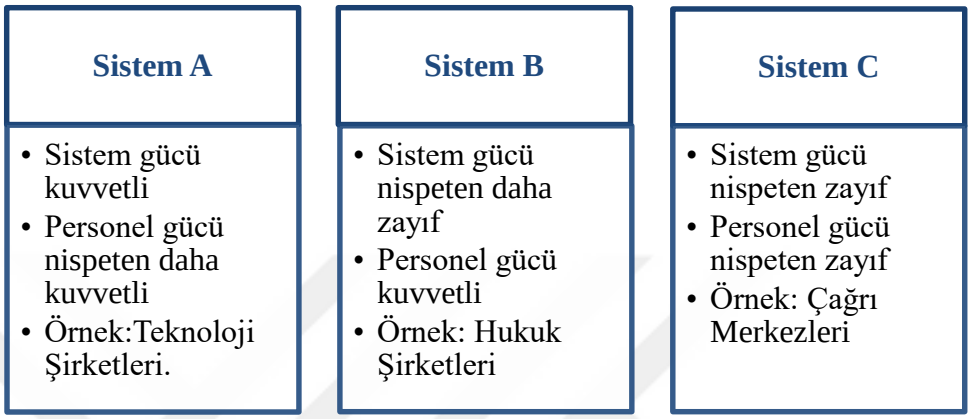
Günümüzde çoğu kurum sosyal mühendislik saldırılarının hedefindedir. Bu sebeple saldırılara karşı risk altındadırlar. Bilgisayar güvenlik sistemlerinin hiçbiri insan unsurundan bağımsız değildir. Bu sistemdeki en zayıf halka insandır. İnsan unsurunun yer aldığı bir sistemde sosyal mühendislik saldırılarına karşı %100 güvence sağlanamamaktadır. Fakat saldırılara karşı kurumların savunma mekanizmaları, doğru çalıştığı takdirde riskleri minimuma indirmek mümkündür. En etkili savunma yöntemi ise çalışanların kurumlarının güvenlik politikalarından haberdar olmalarını ve kurum güvenlik politikalarına uyumlarını destekleyen eğitim ve öğretim faaliyetleridir (Bağcı, 2016: 51).

4.1. Sistem Değerlendirmeleri (Sistem A - Sistem B - Sistem C)

Bilgi güvenliğinin göreceli bileşenlerini anlamak yönetim sistemi ve organizasyon yapısı içindeki riskleri doğru tanımlamak birçok durumda organizasyonu pahalı saldırılardan kurtarmak demektir. Bu noktada organizasyon içindeki sistemik iyileştirmeler içerisinde yer alan eğitim ve bilinçlendirme faaliyetleri verimli olmaktadır. Genel olarak organizasyonlarda ki sistem gücü karşılaştırması, farkındalık sağlayacak ilk adım olmaktadır. Organizasyonların, sosyal mühendislik sistemi gücü haritalaması incelendiğinde karşımıza A, B ve C olmak üzere 3 sistem çıkmaktadır. Sistem gücü karşılaştırmaları yapıldığında Şekil 8'e ulaşılır (Mann, 2008: 156-157).

Her kurum farklı sektörde ticari faaliyetlerini sürdürmektedir. Şekil 8'de kurumlara yönelik sosyal mühendislik saldırılarının sektörel risk analizi verilmiştir.

Toplamda sadece üç sektöre yönelik hazırlanan risk analizinde dar bir çerçeve çizilmiş olsa da genel anlamda hizmet sektöründe faaliyette bulunan kurumların, sosyal mühendislik saldırılarına karşı daha savunmasız ve risk altında oldukları görülmektedir.



Şekil 8: Kurumlara Yönelik Sosyal Mühendislik Saldırılarının Sektörel Risk Analizi

Kaynak: Ian Mann, "Hacking the Human Techniguesand Security Countermeasures" 2008:157'den derlenerek hazırlanmıştır.

Sistem A'da bulunan bilgi sistemleri, güçlü sistemik güce sahiptir. Sosyal mühendislik tehditleri ve cevap verme yetenekleri bakımından personel güçleri nispeten daha yüksektir. Bu durum organizasyon anlayışlarının bir ölçütüdür. Bu kategoriye giren sistemik öğeler güçlü kimlik doğrulamayı içerir. Örnek olarak teknoloji şirketleri verilmektedir. Bu şirketler teknik yeterliliklerinden dolayı gelişmişlerdir. En yüksek personel gücü bu sistemlerde ölçülmüştür.

Sistem B'de personel gücü kuvvetlidir ancak zayıf sistemlere sahiptirler. Bu durum çalışanları hedef almak ve zayıf yönlerini sömürmek adına hackerler için bir fırsattır. Bu sistemde yasal uygulamalar ve çalışanların profesyonel standartları, güçlü geleneklere sahip firmalar için iyi bir örnek olabilir. Fakat çalışanların hackerlara karşı savunmasızlığı değerlendirildiğinde personelin sosyal mühendisliği test etme yeteneği, sistem içerisinde yetersiz kalmaktadır. Bu sisteme örnek olarak hukuk firmaları verilebilir. Bu tür firmalarda iki önemli risk faktörü sosyal mühendislik korunmasını zorunlu kılmaktadır. Hukuk firmaları içindeki sistemler

incelendiğinde organizasyon içindeki iletişimin açık niteliği ve bilgi akışı kıdemsizliğinin getirdiği risk ilk faktör olarak değerlendirilebilir. Organizasyon yapısı içinde sistemsel harcamalar için görülen isteksizlik ikinci risk faktörüdür. Bu tür ortaklık kuruluşları genellikle kâr odaklı kuruldukları için teknik desteğe yatırım yapmama eğilimine sahiptirler. Bu organizasyonların bilgi güvenliği mekanizmaları korunduğunda müşterileri de korunmuş olmaktadır.

Özellikle büyük kuruluşlar sistem C ile eşleşmektedir. Personel gücü nispeten zayıftır. Örnek olarak çağrı merkezleri gösterilmektedir. Bu merkezlerin yapısı personel maliyetlerini düşürmek üzere baskılanmıştır. Personel gücü sınırlı olmasına rağmen kadro sayısı yüksektir. Bu tür organizasyonlarda personel eğitimi ve kalkınma yatırımları yetersiz kalmaktadır. Zayıf personel gücünün olduğu organizasyonlarda, sistematik güçte zayıflamaktadır. Sosyal mühendislerin hedeflerine girmemeleri için organizasyonlarının korunma düzeylerini yükseltmeleri gerekmektedir (Mann, 2008: 158-159).

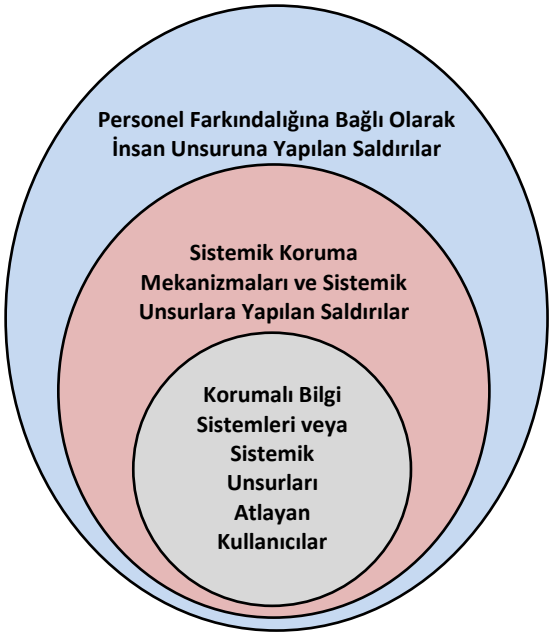
4.2. Sosyal Mühendislik Koruma Modeli

Sosyal mühendislik saldırılarına karşı organizasyon içinde bulunan personelin yetkinliğini ve gücünü ölçmek için organizasyonlar tarafından test çalışmaları yapılmalıdır. Fakat yapılan test çalışmalarında emek yoğun olduğundan ve yüksek düzeyde uzmanlık gerektirdiğinden bu tür ölçümler sınırlı sayıda yapılabilmektedir. Ayrıca bu test çalışmaları organizasyonun tamamında değil küçük bir grup üzerinde yapılmaktadır. Küçük gruplar üzerinde yapılan çalışmalarda ise net sonuçlara ulaşılamamaktadır. Bununla birlikte test aşamasında olan çalışanların test sırasında edinmiş oldukları bilgileri birbirleriyle paylaşmış oldukları bir ortamda, bu çalışmaların sağlıklı yürütülmesi pek mümkün olamamaktadır. Şirket organizasyonlarının tamamı üzerinde sosyal mühendislik testlerinin derinlemesine incelenmesi için çalışanların kişilik profillerini değerlendirmeye alacak bazı tekniklerin kullanılması gerekmektedir. Organizasyon içinde çalışan personelin, kişilik profilleri değerlendirmeye alındığında bir sosyal mühendisin işine yarayacak şekilde saldırıya yanıt verme veya saldırıya meydan okuma eğilimleri incelenmelidir. Bu noktada yapılacak çalışmada güvenlik açıklarını anlamaya yönelik, farklı kişilik grupları içerisinde (Satış, yönetim, araştırma, finans, güvenlik, vd.) farklı kişilik profili soruları oluşturulmalıdır. Çalışanlardan hızlı yanıt alabilmek ve çok düşündürmeden ilk tepkilerini ölçebilmek için basit bir format hazırlanmalı ve

bireysel cevaplarının yöneticileriyle paylaşılmayacağı konusunda çalışanlara güvence verilmelidir (Mann, 2008: 161-163).

Sosyal mühendislik koruma modelinde, sistemik gelişmelerin büyük çoğunluğu sosyal mühendisliğe karşı güçlü bir savunma sağlamaktadır. Fakat birçok durumda bu sistemler başarılı bir şekilde bir hacker tarafından kullanıcının kandırılarak ikna edilmesi suretiyle sistemsel ihlale neden olacak saldırılara olanak sağlamaktadır. Bu sebeple personel bilinçlendirme faaliyetleri çok daha güçlü ve tutarlı bir savunma katmanı oluşturacaktır.

Şekil 9 incelendiğinde personel farkındalığının ilk tepki ve en önemli savunma katmanı olduğu görülmektedir. Bir sosyal mühendislik saldırısında, potansiyel anlamda ilk olarak bu katman ihlal edilecektir. Bu nedenle stratejik anlamda sadece sistemik korunma mekanizmalarına güvenmek yüksek risk içermektedir. Personel farkındalığına bağlı olarak insan unsuruna yapılacak saldırıların niteliği derecesinde organizasyon içerisindeki bilgi ve sistemler savunmasız kalacaktır. Bu nedenle etkili bir savunma oluşturabilmek için personel farkındalığı katmanını, sistemik koruma katlarıyla birleştirmek gerekmektedir. Şekilde katmanların geçilmez olduğu varsayılmıştır (Mann, 2008: 176-177).



Şekil 9: Sosyal Mühendislik Koruma Modeli

Kaynak: Ian Mann, "Hacking the Human Techniguesand Security Countermeasures" 2008:177'den derlenerek hazırlanmıştır.

4.3. Kurumlarda Bilgi Güvenliği Bilincinin Yayılması

İnsan faktörü bilgi güvenliği faktöründeki en zayıf halkadır. Kullanıcılar bilinçli ya da bilinçsiz bilgi ağı kullanımları ile kurumlarını tehditlere açık hale getirmektedirler. Güvenlik programları ise çoğunlukla insan faktörü yerine teknik kontrollere odaklanma eğilimindedir. İnsana bağlı güvenlik riski hiçbir zaman yok edilemese de kontrol edilebilir bir seviyeye indirilebilir. Kullanıcıların bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması şirket yönetimi için kritik öneme sahiptir. Sosyal mühendislik ataklarına karşı etkili bilgi güvenliği bilinçlendirme programının geliştirilmesi için şu adımlar izlenmelidir.

- Kurumun bilgi güvenliği politikası açık ve kısa ifadelerle yazılmalı ve kurumun bilgi güvenliği konusundaki önceliklerini yansıtmalıdır.
- Başarılı bir bilgi güvenliği programının geliştirilmesindeki ikinci adım kurum personelinin mevcut eğitim ihtiyaçlarının belirlenmesidir.
- Güvenlik ihtiyacının tespitinden sonraki aşama, üst yönetimin ve kurum içinde otorite sahiplerinin desteğinin alınmasıdır.
- Sonraki adım, hedef kitlenin belirlenmesidir. Kurum çalışanlarının tümü işlerini yürütebilmek için aynı düzeyde güvenlik bilincine ihtiyaç duymamaktadır. Bu sebeple tüm kullanıcılar gruplandırılmalıdır. Bu gruplandırma kullanıcının durumuna göre bilinç seviyesi, teknik bilgi seviyesi, unvanı, yetki seviyesi ve işin fonksiyonuna göre yapılmalıdır.
- Her grup için üst seviyede kilit mesajlar oluşturulmalıdır.
- Bilinçlendirme programından sonraki adım mevcut iletişim araçlarının belirlenmesidir. Bu araçlar, herkese ya da kişiye özel gönderilen e-postalar, sesli postalar, sisteme giriş mesajları, yazılı yayın olan posterler ya da broşürler, yüz yüze eğitimler, toplantılar, sunumlar, eğitim ve güvenlik seminerleri ve hatırlatıcı malzemeler (kalem, silgi, anahtarlık, not kâğıtları vb.) olmalıdır.
- Başarılı bir bilinçlendirme çalışmasındaki sondan bir önceki adım ise mesajların tutarlı ve etkili iletimi için stratejik bir çerçevenin geliştirilmesidir. Bu çerçevenin taktikleri; işe alım sırasında yapılacak bilgilendirme, aylık şirket bültenleri, şirket yemek ve eğitimleri, yıllık güvenlik seminerleri,

güvenlik konusundaki başarılar için teşvik ödülleri, oyunlar ve yarışmalar olmalıdır.

- Bilinçlendirme faaliyetlerinin ölçülebilmesi ise son adımdır. Bu aşamada ileride meydana gelebilecek gelişme ve gerilemeler ölçülebilir. Ölçüm, kalitatif (niteliksel) ölçütlere dayandırılarak yapılmalıdır (www.denetim.net, Emiral 2004).

4.4. Sosyal Mühendislik Saldırılarına Karşı Alınacak Temel Kurumsal Güvenlik Önlemleri

Sosyal mühendislik saldırılarına karşı alınabilecek temel kurumsal güvenlik önlemleri aşağıda sıralanmaktadır (Gündüz ve Daş, 2017: 21-23).

- Çöpe atılan belge ve tüm dokümanlar, kırpıcılardan geçirilmeli veya okunamayacak şekilde yırtılmalıdır.
- Kişisel şifreler kesinlikle kimseyle paylaşılmamalı ve görünür yerlere asılmamalıdır.
- Temiz masa / temiz ekran politikası uygulanmalıdır.
- Kurum içinde işten ayrılan personellerin uyması gereken prosedürler hazırlanmalı ve bu kişilerin kullandıkları sistemlerin parolaları hemen pasif hale getirilmelidir.
- Kuruma ziyaretçi olarak gelen kişilerden kimlik alınmalı, gerekirse kurum içerisinden bir kişi bu kişiye refakat etmelidir.
- En yakın kişilerin dahi bazen sosyal mühendislik teknikleriyle birbirlerini avlayabilecekleri unutulmamalıdır.
- Bilgi güvenliği için birden fazla e-posta kullanmanın bazı durumlarda daha etkili olabileceği bilinmelidir.
- Klavye türü giriş birimlerinden şifre girilirken başkalarının sizi fark edilmeyecek şekilde gözetlemesi anlamına gelen omuz sörfü eylemlerine karşı dikkatli olunmalıdır.
- Kurum içinde hassas bölgelere 24 saat aktif olan güvenlik kameraları yerleştirilmelidir.
- Çalışanlara internette verdiği tüm kişisel bilgilere ve paylaşımlara birilerinin ulaştığı hatırlatılarak kontrollü hareket etmeleri istenmelidir. Özellikle hassas nitelikte kişisel bilgilerin (TC kimlik numarası, telefon numarası, doğum yeri,

doğum tarihi vb.) her yerde özellikle sosyal medyada (Instagram, Facebook, Twitter vb.) paylaşılmamasına dikkat edilmelidir.

- Sosyal mühendislik yöntemlerini barındıran kimlik avı e-postaları detaylı incelendiğinde genel ve net olmayan ifadeler kullanılır. İmla kurallarının acemice kullanıldığı görülür. Gereksiz ve alâkasız vaatlerde bulunulur ve olayın çok acil olduğuna dair kişiyi paniğe sokacak ifadeler kullanılır. Kişinin verilen talimatları hemen yerine getirmesi konusunda panik yaratılmaya çalışılır. Bu tür psikolojik e-posta saldırılarına karşı bilinçli olunmalıdır. Ayrıca kişinin önceden bilmediği linklere yönlendirilmesinin amaçlandığı e-postalara karşıda dikkatli olmak gerekmektedir.
- Periyodik olarak sosyal mühendislik saldırı testini de içeren bilgi güvenliği testleri gerçekleştirilmelidir.

Genel olarak kurumların bilgisayar ve bilgisayar sistemleri üzerinde almış oldukları önlemler ile riskleri sıfıra indirmek mümkün olamamaktadır. Hiçbir kuruluş sistemlerinin %100 güvenli olduğunu düşünmemelidir. Risk ve saldırılara karşı alınması gereken temel önlem sürekli uyanık olmak ve güvenlik politikaları uygulamalarını yapılan güncellemeler doğrultusunda takip etmektir. Ayrıca yüksek seviyede güvenlik için kurumsal bilgi güvenliği standartlarının uygulanması da korunmada önemli bir etken olarak değerlendirilmektedir. (Canbek ve Sağıroğlu, 2007: 10)

Kurumlar açısından bilginin üretilmesinden kullanımına kadar gelen her aşamada olası tüm tehditlere yönelik uygulamalar Uluslararası Standardizasyon Örgütü (ISO) tarafından standartlar ile belirlenmiştir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı olarak belgelenmektedir. Çağımızda işletmeler kurum imajı, saygınlığı, rekabet avantajı gibi birçok finansal nedene bağlı olarak ISO'nun yayınlamış olduğu standartları belgelendirmek için büyük miktarlarda kaynak ayırmaktadır. ISO 27001 Standardının işletmelerin öz sermaye kârlılığını etkilediği bilinmektedir. (Önder,2018: 90-97).

Özetle sosyal mühendislerin kurum içi ve kurum dışı bilgi toplama kaynakları; telefon yoluyla ikna, e-posta yoluyla kandırmaca, çöplük karıştırma, masaüstü testleri ve fiziksel erişimdir. Kurum içi güvenlik testlerinin geneli değerlendirildiğinde sosyal mühendislik testlerinin risk sıralaması seviyesi orta

düzeyde kabul edilmektedir. Kurumsal bilgi güvenliğini etkileyen en zayıf halka insandır. Bu noktada güvenlik bilincinin zayıflığının belirlenmesinde sosyal mühendislik teknikleriyle yapılan güvenlik testleri büyük öneme sahiptir. Günümüzde teknolojik tedbirlerin ilerlemesi nedeniyle kurumların bilgi güvenliğinde yazılım ve donanımdan kaynaklanan güvenlik açıkları minimize edilmiştir. Bu sebeple saldırganlar, insan zafiyetlerinden faydalanarak ilerlemektedir. Sonuç olarak kurumsal bilgi güvenliğinde tehditleri engelleyebilmek amacıyla sosyal mühendislik tekniklerinin her kademede bulunan kullanıcılar tarafından bilinmesi gerekmektedir. Ülkemizde sosyal mühendislik kavramı henüz net olarak anlaşılmamıştır. Kurumlar ve çalışanlar nezdinde farkındalık yaratılmalıdır (Vural ve Sağıroğlu, 2011: 97-102).

5. SOSYAL MÜHENDİSLİK FAALİYETLERİ VE YASALARDA SOSYAL MÜHENDİSLİK

Sosyal mühendislik kavramı özünde hacker (bilgisayar ve ağlara izinsiz giriş yapan kişi) kavramını da barındırmaktadır. Hacker kavramı ise siber güvenlik (bilişim sistemleri alt yapı güvenliği) kavramıyla ilişkilidir. Teknolojinin gelişmesi ve tüm nesnelerin birbirlerine entegre olmasıyla birlikte evrensel güvenlik kavramı üzerinde bireylerin sorumluluğu her geçen gün artmaya devam etmektedir. Günümüzde konu ile ilgili ne kadar önlem alınmış olunsa da hâlâ modemini standart şifresiyle tutan ev telefonunu, ADSL şifresi yapan insanlar mevcuttur. Bu noktada bir sosyal mühendisin, aynı zamanda bir hacker olarak saldırı eylemini nasıl gerçekleştirdiği örnek bir olayla açıklanabilmektedir.

Günümüzde bilgisayarların, IP adreslerini tespit eden ve IP adreslerinden, kişilerin yerini tespit eden siteler (https://iplogger.org/ vb. 2018) hackerlar tarafından sıkça kullanılmaktadır. Hatta YouTube kanalında, program kullanmadan IP adresi bulma ve buna benzer konular üzerine onlarca video çekilmiş ve bu videolar tıklanma rekorları kırmıştır (bkz. https://www.youtube.com/watch?v=p7SC3ZlCxvg, Bilen Adam, 2019 Programsız IP Adresi bulma). Tespit edilen IP adresinden kişinin açık ev adresine ulaşılabilmektedir. Ev telefonunu ADSL şifresi yapan bir kişi üzerinden örnek verilecek olunursa ilk etapta IP adresine ulaşan hacker, bu adresten modemin şifresini öğrenip modemin tüm bilgilerini görebilmektedir. Şifre olarak 7 haneli ev telefonuna ulaşan hacker hedefinde olan kişinin IP adresinden, alan kodunu da (il kodu) aldıktan sonra eve telefonla ulaşıp çeşitli sosyal mühendislik

teknikleriyle istediği kişinin cep telefonu, T.C. Kimlik numarası gibi ulaşmak istediği tüm bilgilere ulaşabilmektedir. Kişilere yönelik sosyal mühendislik saldırılarının büyük çoğunluğu internet tabanlıdır. Öyle ki internette tarama yapmak ve belirli özelliklere sahip cihazları tespit etmek için tasarlanmış bir arama motoru olan "Shodan" üzerinden tarama yapılarak internete açık olan sistemleri ve cihazları aygıtlarıyla tespit edip bu arama motorundan çeşitli raporlara ulaşılabilmektedir.(https://www.shodan.io/explore, 2018 bknz). Shodan, aygıt arama motorunda en çok aranan aygıtın webcam olduğu bilinmektedir (https://eksisozluk.com ,2018). Sosyal mühendisleri hacker'lardan üstün kılan şey saldırının sadece teknik bilgiyle veya sistemle çözülemeyeceğinin bilinmesidir. Tüm hackerlar en güvenli sistemin fişi çekik sistem olduğunu bilir. Fakat en güvenli sistemlerin dahi alt üst edilebileceği tek sistemde sosyal mühendisliktir. Bu sebeple bilgisayar sistemlerini güvenli kılabilmenin tek yolu yazılımı güvenli yapmak değil aynı zamanda kullanıcıları da eğitmektir (https://www.merdincz.com, Zorba,2013). Küreselleşmenin getirmiş olduğu birbirine bağlılık ve bağlantılılık ilişkileri çerçevesinde, dünya üzerinde var olan her şey birbiriyle ilişkili hale gelmiştir. Teknolojinin getirisi olan dijital gelişmelerle birlikte insanların birbirleriyle saniyeler içerisinde bağlantı kurarak harekete geçmeleri devletleri yeni bir güvenlik tehdidi olan siber güvenlik tehlikesiyle karşı karşıya bırakmıştır (Yılmaz,2017: 24).

Gelişen ve değişen teknolojiyle birlikte bilişim suçlarına yönelik işlenen asayiş suçlarında artış yaşanmıştır. Bilişim sistemlerinin sağladığı fırsat ve kolaylıklarla birlikte insanların kullanmış oldukları bilgisayar ve cep telefonu gibi teknolojiler, yeni suç işleme yöntemlerine de zemin hazırlamaktadır. Artan bilişim suçlarında ve bu tür suçlarda haksız kazanç sağlamaya yönelik alınacak en etkili tedbir kamunun bilinçlendirilmesidir. Dolandırıcılık suçu ekonomik suç türleri arasında incelenir. Dolandırıcılık suçu 5237 sayılı Türk Ceza Kanunu'nun (TCK) 157. Maddesinde "*Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak kendisine veya bir başkasına yarar sağlamak*" şeklinde tanımlanmaktadır. Bu tanımdan dolandırıcılık suçunun kişilerin mal varlıklarına yönelik işlenen bir suç olduğu tespit edilmiş olup kişilerin mal varlıklarının korunması amaçlanmaktadır. Ayrıca aldatıcı davranış ve hileli hareket taşıyan hareketlerle, kişiler arasında olması gereken güven, iyi niyet ve irade özgürlüğünün ihlal edildiği durum açıklamalı olarak belirtilmektedir. TCK'nın 158. Maddesinde ise

nitelikli dolandırıcılık suçunun halleri belirlenmiştir. Dolandırıcılık suçunun nitelikli hallerinin 1. fıkrasında "*Kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan ya da algılama yeteneğinin zayıflığından yararlanılması*" konusundan bahsedilmektedir (Sönmez, 2017: 48-50). Bilişim suçlarında en çok dikkat çeken nokta " bilişim suçu " ve " bilişim yoluyla işlenen suçlar " ayrımının uygulamada birbirleriyle çok sık karıştırılmasıdır. Bilişim yoluyla işlenen suçlar; Bilişim teknolojilerinin kullanılmasıyla işlenen hırsızlık, dolandırıcılık, kişisel verilerin yayılması, özel hayatın gizliliği, tehdit ve hakaret içeren suçlar iken, Bilişim suçları; tüm teknolojilerin kullanılmasıyla kanuni olmayan yollarla, kişisel ya da kurumsal bilgisayarlar üzerinden sistemlere zarar vermek olarak tanımlanmaktadır (Dijle ve Doğan, 2011: 43-53).

Bilişim sistemlerine girerek bu sistemleri bir araç olarak kullanan dolandırıcılık suçlarında eylemler, suçun doğası gereği devamlı değişkenlik gösteren çok esnek ve hareketli bir yapıya sahiptir. Günümüzde internet kullanımının son hızla artmakta olduğu bilindiğine göre sosyal mühendislik dolandırıcılıklarının tüm kullanıcıları hedef alabileceği görünen bir gerçekliktir. Yapılan araştırmalar sosyal mühendislik yöntemlerinin doğrudan ya da dolaylı olarak siber suçlar arasında saldırganlar tarafından çok yüksek oranda kullanıldığını kanıtlamaktadır. Üstelik son kullanıcıların büyük çoğunluğunun sosyal mühendislik saldırılarına uğradıklarının farkında bile olamadıkları tespit edilmiştir. Sosyal mühendislik saldırılarının ağ sistemleriyle ilgili çok fazla teknik bilgi gerektirmemesi ise saldırganları bu yola teşvik eden önemli bir unsurdur (Gündüz ve Taş, 2016: 17-18).

Sosyal mühendislik ile hesap çalmanın cezası nedir? 5237 sayılı Türk Ceza Kanunu incelendiğinde bilişim suçlarına yönelik tanımlamalarda "sosyal mühendislik" kavramının olmadığı ve tanımlanmadığı görülmektedir. Yine Türk Ceza Kanunu'nda bilişim suçlarına yönelik Yargıtay kararları incelendiğinde; bilişim suçlarının konusunun çoğunlukla "suçun vasfında hata lehe kanun uygulaması, görevsizlik ihlali, dolandırıcılık, nitelikli dolandırıcılık, görevsizlik, lehe kanun uygulama hatası, resmi belgede sahtecilik, malvarlığına ilişkin etkin pişmanlık" hükümlerinin uygulandığı görülmektedir (Turan ve Külcü, 2013: 14-23).

İKİNCİ BÖLÜM

SİBER GÜVENLİK İLE İLGİLİ TEMEL KAVRAMLAR

1. SİBER GÜVENLİK VE TEMEL KAVRAMLAR

Çağımızda siber güvenlik kavramının önemi küresel bir konu haline gelmiştir. Bugün elliden fazla ülke kendi siber güvenlik strateji belgesini ana hatlarıyla yayınlamıştır. Bu stratejiler özetle siber uzayda resmi bir duruş olarak değerlendirilebilir. Uluslararası Telekomünikasyon Kurumu, Union (ITU) siber güvenlik kavramını özetle; araçlar ve politikalardan oluşan bir güvenlik topluluğu olarak tanımlamaktadır (Solms ve Niekerk, 2013: 97). Siber saldırıların kaynakları hakkında FBI ve Cybercrime Bilgisayar Güvenliği Enstitüsü tarafından yapılan ortak çalışma sonunda güvenlik ihlallerinin %71'inin içerdekiler tarafından gerçekleştirildiği ortaya çıkarılmıştır (Byres ve Lowe, 2004: 216). Siber güvenlik kavramı çok boyutlu bir kavramdır. Literatürde siber güvenlik ile ilgili temel kavramlar şöyle sıralanmaktadır.

1.1. Siber Saldırı ve Siber Savaş: Bir bilgisayar virüsünden gelen saldırıdır. Bu saldırılar neticesinde örnek senaryolar şu şekilde sıralanabilir; Finansal kayıtların karıştırılması ya da borsanın yönlendirilmesi, uçak kazalarına yol açan hava trafik kontrol sisteminin karartılması, bir nükleer reaktörün kapatılması sonucunda ciddi boyutta ekonomik ve fiziksel hasara neden olunması sayılabilecek örnekler arasındadır. Bu senaryoların tamamı şimdiye kadar gerçekleşmiştir. Siber saldırı eylemleri siber savaş olarak tanımlanmaktadır. Bu noktada hükümetlerin, eşgüdümlü politika önerileri geliştirmesi ve koordineli eylem planları hazırlamaları büyük önem arz etmektedir. Siber saldırının mevcut tanımları ve ilgili terimleri arasında farklılıklar bulunmaktadır. Siber savaşı "eylemler'' olarak tanımlayan güvenlik uzmanı Richard A. Clarge, bir ülkenin başka bir ülkenin bilgisayarlarına hasar vererek bozulmasına neden olacak sonucu amaçlaması olarak tanımlamıştır. Benzer şekilde eski NSA ve CIA yönetmeni Michael Hayden, siber savaşı kasıtlı girişim olarak değerlendirerek bir ülkenin başka bir ülkenin bilgisayarlarını devre dışı

bırakması veya yok etmesi olarak tanımlamıştır. Bu tanımlarla birlikte siber suç, siber saldırı ve siber savaş arasındaki ayrımı yapmak zordur. Ancak sonuç olarak savaşın çok daha tehlikeli derecede geniş bir uygulama alanı bulduğu anlaşılabilmektedir. (Aktaran; Hathaway ve diğerleri, 2012: 823-824). Günümüzde siber savaş sırasında uyulması gereken hukuk kurallarını düzenleyen hiçbir bağlayıcılığı ve caydırıcılığı olmayan sadece referans kaynak niteliği taşıyan Tallin El Kitabı dışında uluslararası alanda yapılmış bir çalışma bulunmamaktadır (Çeliktaş, 2016: 127).

1.2. Siber Casusluk: Siber casusluk, bir ülkenin veya bir kurum ya da organizasyonun, hassas ve kritik önem düzeyine sahip bilgilerini, siber ortamın araç olarak kullanılarak gizlice ele geçirilmesi eylemidir. Bu eylem bireysel ya da kolektif olarak parasal menfaat elde etmek amacıyla da yapılabilmektedir. Veya bir devletin başka bir devlete zarar vermesi amacıyla da bir girişimde bulunulabilmektedir. Sonuç olarak icra edilen siber casusluk faaliyetleri siber savaşların nedeni olarak değerlendirilir (Yayla, 2013: 196). Haziran 2008 ve Mart 2009 arasında, Çin siber casusluk iddialarına odaklanan bir araştırma ekibi Hindistan, Avrupa ve Kuzey Amerika da saha bazlı araştırmalar yürütmüştür. Bu araştırma ekibi güvenliği ihlal edilmiş bilgisayarlardan veri almak suretiyle bu bilgisayarların sunucularını inceleyerek geniş kapsamlı bir bilgisayar ağını açığa çıkarmıştır. Bu geniş ağın 103 ülkede en az 1.295 virüslü bilgisayardan oluştuğu tespit edilmiştir. Araştırmacılara göre kod adı GhostNet olan geniş çaplı Çin casusluk ağı, hassas bakanlıklara ve elçiliklere sızmak için tasarlanmıştır. Toronto'daki Uluslararası Çalışmalar Merkezi'nin on aylık bu araştırması sonucunda GhosNet'in sadece bilgisayarlarda bilgi aramakla yetinmeyip e-postaları tıkladığını aynı zamanda bu bilgisayarları, dev dinleme cihazlarına dönüştürdüğü ortaya çıkarılmıştır. Bu virüs bilgisayara bulaştıktan sonra bilgisayar korsanları tarafında web kamerası ve mikrofonları açılarak ortamdaki tüm konuşmalar kayıt altına alınabilmektedir. GhosNet'in hedefinde bulunan bilgisayarların neredeyse %30'una yakın bir oranının güvenlik düzeyi yüksek kabul edilen dışişleri bakanlıkları, elçilikler, uluslararası örgütler, haber medyası ve aralarında STK'lar (Sivil Toplum Kuruluşları) gibi kurum ve kuruluşların bilgisayarlarının yer aldığı ve içeriklerinin casusluk yoluyla ele geçirdiği ortaya çıkarılmıştır (Deibert ve diğerleri 20019: 5-6).

1.2.1 Siber Ekonomik Casusluk: Şirketlerin, kurumların ve bireylerin, fikri mülkiyetini ticari ve teknik sırlarını ya da değeri yüksek bilgilerini, siber ortam ve araçlarını kullanarak çalma eylemidir. Bu tür hırsızlıklar, kendi başlarına çalışan suçluların yanı sıra, firmalarca (rakiplerinden bilgi çalma)veya devletler tarafından desteklenmektedir (Alkan, 2017: 20).

1.2.2. Siber Askeri Casusluk: Bir devletin siber ortam ve araçlarını kullanarak başka bir devletin içine sızması yolu ile askeri kurum veya tesislerden bilgi sızdırmasıdır (Alkan, 2017: 20).

1.3. Siber Terörizm: Terör örgütlerinin faaliyetlerinde, siber ortamın sunduğu kolaylıkları, uygulamaları, araçları, altyapıları, teknik ve teknolojileri, boşlukları, zararlı yazılım ve içerikleri bulup kullanarak, tuzak kurarak veya yeni yöntemler geliştirerek belirlenen hedef doğrultusunda ulusları, toplumları veya kişileri yönlendirme, sindirme, zarar verme, yıldırma, bezdirme ve çıkar elde etme amacıyla yapılan faaliyetlerdir (CyberMag, 2017, 14.sayı; 19).

1.4. Siber Suç: Avrupa komisyonu siber suçu üç şekilde tanımlamıştır. İlki elektronik haberleşme ve bilgi sistemleri üzerinden işlenen dolandırıcılık ve sahtecilik suçu şeklinde tanımlanmaktadır. İkinci olarak yapılan tanım; yasadışı içeriğin elektronik ortam üzerinden yayılmasıdır. Irkçılık, nefret söylemleri ve cinsel çocuk istismarı gibi suçlar siber suç türlerine örnektir. Üçüncü tanımlama ise; bilgi sistemleri hizmetinin aksatılması, durdurulması veya hacklenmesidir (Anderson ve diğerleri, 2013: 11).

1.5. Siber Aklama: Günümüzde geleneksel yöntemlerle kara para ile mücadele yöntemleri arttığından ve geleneksel yöntemlerle kara para aklama eylemi zorlaştığından aklayıcılar için yeni aklama yöntemlerinin bulunması zorunlu hale gelmiştir. Sonuç olarak kara para aklama gerçek dünyadan siber dünyaya taşınarak internet, akıllı kartlar ve elektronik para gibi araçlarla, siber ortamlarda kara para aklanmaya başlanmıştır. Siber aklama konusuna FAFT (Kara Paranın Aklanmasının Önlenmesine İlişkin Mali Çalışma Grubu) her ne kadar dikkat çekmiş ve bazı tavsiyeler getirmiş olsa da öneriler sadece tavsiye niteliğinde kalmıştır. Kara para aklama konusu gereği ulusal değil uluslararası boyuttadır. Bu sebeple FAFT'ın önerilerine sadece üye ülkeler değil üye olmayan ülkeler tarafından da uyum sağlanmalıdır (Yazıcı, 2008: 166). ABD Hazine Bakanlığı Mali Suçlar bölümünde

yapılan bir araştırmada, siber aklayıcıların her üç ayda bir bilgisayardaki yazımları değiştirerek resmi makamları şaşırtmaya çalıştıkları ve izlerini kaybettirmeye yönelik davranış sergiledikleri ortaya çıkarılmıştır (İpek, 2000: 30).

1.6. Siber Uzay: Siber alanda, sunucular, web sayfaları, hizmetler vb. araçlar birbirlerine bağlıdır. Bu araçlar karşılıklı olarak birbirlerine bağımlı olduklarından birlikte çalışırlar. Bu noktada her alan üzerindeki hâkimiyet farklı teknoloji gerektirmektedir. Çünkü siber alanda fiziksel araçlar, büyük oranda hâkimiyetini kaybetmektedir. Bu noktada hâkimiyet taktik ve teknolojiye kalır. Siber uzay dört bileşenden oluşur. Bunlardan birincisi kullanıcıdır. İkincisi paylaşılan bilgilerdir (yazı, resim, video vb.).Üçüncü bileşen yazılım ve protokollerden oluşmaktadır. Dördüncü bileşen ise fiziksel alt yapıdır. Martin Libicki'ye göre siber uzayda dört katman bulunmaktadır ve katmanların her birine hükmetmek için gerekli araçlar şu şekilde sıralamıştır. İlk katman fiziksel kablolardan ve anahtarlardan oluşur ve bu katman tahrip edici fiziksel bir güç tarafından yönetilebilmektedir. İkinci katman bu sistemlerin kontrolünü elinde bulundurarak hâkimiyetini sağlayabilmektedir. Üçüncü katman, verilerle ilgili katmandır. Bilgiye erişimin kontrol edilmesi ve sansürlenmesi yoluyla hâkimiyet kurulabilir. Dördüncü katmanda ise bilişsel ya da pragmatik değerlendirmenin hâkimiyeti söz konusudur. Katmanların tamamı göz önüne alındığında siber uzayda güç sahibi olabilmek için bilginin ve yeteneğin analiz edilerek geliştirilmesinin büyük öneme sahip olduğu bilinmektedir (Aktaran; Korhan, 2017: 86).

1.7. Siber Zorbalık: İnternetin yaygınlaşmasıyla birlikte genç nesil teknolojik araçlarla iç içe yaşamaya başlamıştır. Dijital araçlar bir taraftan insanların hayatını kolaylaştırırken diğer taraftan bir takım zorlukları da beraberinde getirmiştir. Bu zorluklar arasında gençlerin sanal ortam üzerinden birbirlerine hakaret etmeleri, birbirlerini küçük düşürerek utandırmaları ya da birbirlerine karşı tehditlerde bulunmalarına yönelik karşı tarafa kasıtlı zarar verme amaçlı yapılan saldırı ve şiddet eylemlerini kapsayan olayların tümüne siber zorbalık denilmektedir. (Küçük, 2016: 10). Günümüzde teknolojinin pozitif yönleri her ne kadar fazla olsa da hesaba katmadığımız negatif yönleri de bulunmaktadır. Siber zorbalık sadece yetişkinler arasında değil özellikle gençler arasında giderek yaygınlaşmaktadır Başka bir deyişle; özellikle gençleri daha çok etkileyen internetin karanlık yüzüne siber zorbalık denilmektedir. Çoğunlukla E-posta, mesajlaşma, sohbet odaları, cep

telefonları, cep telefonu kameraları ve web siteleri gençler tarafından sıkça kullanılan siber zorbalık araçları olarak bilinmektedir. Uluslararası düzeyde de küresel bir sorun olan siber zorbalık henüz devletler tarafından hak ettiği ilgiyi görememektedir (Campbell, 2005: 68).

2. SİBER SALDIRI TÜRLERİ VE İŞLEVLERİ İLE SİBER GÜVENLİKTE SCADA (MERKEZİ KONTROL VE VERİ TOPLAMA SİSTEMİ)

Literatürde tanımlanan siber saldırı türleri ve bu saldırıların işlevleri Tablo 2 ile özetlenmiştir.

Tablo 2: Siber Saldırı Türleri ve İşlevleri

No	Saldırı Türü	İşlevi
1.	**Snifffing**	Kelime anlamı koklamaktır. Bir ağ üzerinde bulunan bilgisayarlar arasındaki veri trafiğinin dinlenmesi anlamına gelir. Amaç tüm verilerin yakalanarak saklanmasıdır. Şifreleri ve transfer edilen dosyaları yakalamaktadır. Korsanların en çok kullandığı yöntemlerden biridir. Korunmak için bilgisayarlar arasındaki bağlantıların şifreli olması gerekmektedir.
2.	**Hizmet Dışı Bırakma:**	DoS saldırı türü olarak bilinmektedir. Hizmet dışı bırakma, hizmeti aksatma veya hizmeti tamamen yok etme anlamına gelir. Amaç sistemin devre dışı kalmasını sağlamaktır. Tek bir IP adresi üzerinden saldırı yapıldığı durumlarda tespit edilebilmektedir. Fakat bu saldırılarda çok fazla makine kullanıldığından IP adreslerinin tespiti güçleşir. DoS saldırıları siber tehditler arasında ikinci sıradadır.
3.	**IP Aldatması (IP Spoofing):**	Bilgisayarlar arasındaki bağlantı, çeşitli protokoller aracılığıyla sağlanmaktadır. Bilgisayar, bağlantı yapmak istediği bilgisayara kendi kimliğini tanıtır. Bağlanılan bilgisayara, gerçek kimliğin gösterilmeyerek gizlenmesine IP aldatması denir. Bu aldatma genellikle bir web sitesini işlemez hale getirmek amacıyla saldırı esnasında kaynağı gizlemek için kullanılır. Bu tür saldırıların önlenebilmesi için IP adreslerini değiştirme hakkı kaldırılmalıdır.
4.	**Sosyal Mühendislik:**	İnsanların iletişim, güven ve düşünce tarzları gibi insani zafiyetlerinden faydalanılarak siber güvenlik süreçlerinin etkisiz hale getirilmesidir.
5.	**SQL Enjeksiyonu:**	Veri tabanından yapılan sorgulama işlemini hedef alan bir saldırıdır. Sorgulama dili yapısı kullanılarak saldırı gerçekleştirilir ve bütün kayıtlara ulaşılır.
6.	**Arka Kapılar (Backdooors):**	Kimlik kanıtlama süreçlerini atlatarak, bilgisayara uzaktan erişmeyi sağlayan yöntemler arka kapı olarak adlandırılmaktadır. En sık karşılaşılan arka kapı yöntemi, sistemde dinleme ajanı iliştirilmiş bir portu açık tutmaktır. Birçok virüs bir bilgisayara ulaştığında arka kapıyı açmayı dener.
7.	**Oltalama Phishing):**	Temel amaç internet kullanıcısının kandırılarak dolandırılmasıdır. Kullanıcıya ait tüm özel bilgiler phishing yöntemiyle ele geçirilir (kredi kartı bilgileri, banka hesap numaraları, şifreler ve parolalar vb.). Bu dolandırıcılık yöntemi yalnızca bankacılık siteleri değil, sohbet siteleri, arkadaşlık siteleri, alışveriş siteleri ve havayolları siteleri gibi birçok sitede ortaya çıkmaktadır. Bunlarla birlikte ATM cihazları kullanılırken dikkatli davranılmalıdır. ATM makinaları üzerine yerleştirilen mikro kamera kart okuyucu ve sahte tuş takımı (Pinpad) gibi aygıtların yerleştirilmesi neticesinde kredi kartı bilgileri dolandırıcılar tarafından ele geçirilmektedir.
8.	**Casus Yazılım (Spware):**	Çoğunlukla internetten bedava indirilen programlar ile bilgisayara bulaşan programcıklardır. Program indirilirken dikkat edilmeyen son kullanıcı lisans sözleşmesinin (EULA) içerisinde bulunan ‘’I Agree’’ kabul edildiğinde programın kurulumu kullanıcı tarafından kabul edilmiş demektir. Böylelikle casus yazılım programı çalışmaya başlar ve kullanıcının bilgisayarında yapmış olduğu tüm işlemleri ve verileri arka planda depolamaya başlar. Casus yazılım programcıları bu eylemi casusluk olarak değerlendirmemektedirler. Onlara göre bu durum gönüllü veri paylaşımıdır. Çünkü kullanıcı lisans sözleşmesiyle veri aktarımının kabul edildiği kullanıcı tarafından onaylanmıştır.
9.	**Virüsler:**	Virüs dosyalara bulaşıp yayılan özel bir zararlı yazılım türüdür. Bir sistemdeki olası virüs belirtileri şunlardır; İnternet sitelerinde dolaşırken reklam pencerelerinin açılması, telefonlardaki kötü amaçlı yazılımlar, bilgisayarın işlemez hale gelmesi, internette aktif durumda değilken veri trafiğinin devam etmesi, bazı uygulamalara internetten bağlanılması.

No	Saldırı Türü	İşlevi
10.	**Truva Atları:**	Faydalı bir fonksiyonmuş gibi gözüken fakat arka planda güvenlik ve gizlilik mekanizmalarını aşarak zararlı fonksiyonlar içeren bir sistemin meşru olarak yetkilendirilmesidir. Truva atları bilgisayarı uzaktan yönetmek amacıyla arka kapı açan programlardır. Bedava mp3, oyun veya yetişkinlere yönelik siteleri ziyaret eden kullanıcılar farkında olmadan zararlı ve kötü niyetli programları da bilgisayarlarına indirmiş olmaktadırlar. Ayrıca lisanslı yazılımların yasa dışı kopyalarının veya aktivasyon kodlarının dağıtıldığı "warez" olarak adlandırılan siteler içinde aynı durum söz konusudur. Yukarıda anlatılan yöntemlerle bilgisayarlara kurulan bu programlar arka planda kullanıcının sistemine uzaktan erişim imkânı sağlar. Böylelikle sistemi, istediği gibi yapılandıran bilgisayar korsanları, kullanıcıların şifrelerine ve diğer kişisel bilgilerine ulaşmış olurlar.
11.	**Solucanlar:**	**S**olucanlar aynı virüsler gibi kendilerini bir bilgisayardan başka bir bilgisayara kopyalamak için tasarlanmışlardır. Solucanların en büyük tehlikesi büyük miktarlarda çoğalabilme yetenekleridir. Bilgisayarda dosya ve veri transferi yapan sistemi bir kez ele geçirdikten sonra istedikleri gibi yollarına devam edebilirler. Truva atları bilgisayarın internete bağlandığı durumlarda devreye girerken solucanlar, ağda kendi başlarına yayılabilen programlardır. Virüs ise bulaşmak için kendine yeten bir program değildir. Virüs kendini başka dosyalara ilave ederek yayılır. Eğer virüslü dosya açılmazsa virüs yayılmaz. 2011 yılında 15 milyon bilgisayara bulaştığı tahmin edilen "Conficker" isimli solucan, zayıf şifrelere sahip kullanıcı hesapları aracılığıyla ağ üzerinde yapılan paylaşımlar ve bilgisayarlara takılan taşınabilir bellekler vasıtasıyla yayılmıştır.
12.	**Bot:**	Bilişim dünyasında robot anlamında kullanılır. Robot teknolojilerinin internet üzerinde geliştirdikleri ajan yazılımı grubudur. Genellikle web tabanlı arama motorlarının çekirdeklerinde yer alan özel amaçlı tarayıcı yazılımlar ya da örümcek yazılımları olarak bilinirler. Çok fazla bot türünden bahsedilebilmektedir. Ticari veri madenciliği, e-posta, oyun, alışveriş, sohbet, hisse senedi ve kamusal haber gibi hedeflenen bilgi türüne göre adlandırılan botlar mevcuttur. İnternet üzerinde faaliyet göstermek üzere tasarlanmışlardır.
13.	**Zombi Ordular (Botnerler):**	Bu tehdit grubunda en tehlikeli olanlar zombi bilgisayarlar olarak kabul edilir. Burada kilit nokta, bilgisayar kullanıcısının haberi olmadan, bilgisayarının en ağır suçlarda araç olarak kullanılmasıdır. Bir bilgisayarın zombi ordusunun parçası haline gelmesinin en önemli sebebi genellikle bilgisayarda ''firewall'' denilen güvenlik duvarının olmamasıdır. Botner'in parçası haline gelen bilgisayarlar, bir web sitesine aynı anda yönlendirilerek siteyi hizmet veremez hale getirmek için kullanılır.
14.	**Bukalemun:**	Kullanıcı adlarını ve şifrelerini ele geçiren programdır. Özellikle çok kullanıcılı sistemlerde kullanıcı adı ve şifrelerini, taklit yeteneği ile gizli bir dosyaya kaydederek sistemin bakımı için geçici bir süre kapatılacağına ilişkin hile ve aldatmacalar uygulayan programdır.
15.	**Klavye İşlemlerini Kaydeden Programlar (Keyloggers):**	Kullanıcının fark etmeyeceği şekilde klavyede dokunulan her tuşu, arka planda kayda alarak önceden belirlenen mail adreslerine raporlayan programdır. Özetle tuş kaydedici programlar denilebilir. Özellikle bankacılık işlemleri gerçekleştirirken klavyeden şifre girilmemesi ve rakamların üzerlerinde beklenilmemesi bu tür programların kurbanı olmamak için dikkat edilmesi gereken noktalardır. Günümüzde internet üzerinden kredi kartıyla alışveriş yapılan sitelerin bir kısmında, SMS şifreleri yoluyla, ilave güvenlik desteği sunulmasına imkân sağlayacak ek güvenlik destekleri olmasına rağmen, güvenlik seviyesi yüksek platformlar oluşturulmamaktadır. Benzer risk sosyal medyada da bulunur. Bu yazılımlar aynı zamanda aldatan eşi takipte, işverenlerin çalışanlarını izlemesinde ve çocukların internette nasıl vakit geçirdiklerinin takibinde kullanılmaktadır.

Kaynak: ARSLAN, M. E. Siber Güvenlik ve Siber Saldırı Türleri. Makalesinden derlenerek hazırlanmıştır. Ss.3-10.

Siber Güvenlikte SCADA (Merkezi Denetleme Kontrol ve Veri Toplama Sistemi); kritik altyapılar olarak tanımlanan elektrik üretim, iletim ve dağıtım tesisleri, haberleşme, ulaşım, iletişim ve gaz üretimi gibi farklı tesislerde, denetim amaçlı olarak kullanılan ve bu sistemlerin güvenliğini artırmaya yönelik geliştirilen bir yazılımdır (Irmak ve Erkek, 2018: 16). Kapsamlı ve gözetleyici olan bu kontrol ve veri toplama sistemi sayesinde bir tesise ve işletmeye ait tüm cihazların kontrolünden, üretim planlamasına, çevre kontrol ünitelerinden yardımcı işletmelere kadar tüm birimlerin otomatik kontrolü ve gözetlenmesi sağlanabilmektedir. Aynı

zamanda, içinde bulunulan anda ve geçmişte yaşanan olay ve alarmları, günü tarihi ve saatinde gözlemlemeye olanak sağlayan geniş kapsamlı bir sistemdir. (http://www.wikizeroo.net, 2018).

Günümüzün rekabetçi pazarlarında maliyetleri azaltmak ve verimliliği artırmak için endüstriyel şirketler, dijital SCADA ağlarını modernize etmek zorundadır. SCADA ağları üzerinde kötü niyetli saldırı potansiyeli her zaman mevcuttur. Bu durum kamu güvenliğini tehlikeye sokmaktadır. SCADA ağlarının dış ağlarla bağlantısı büyümeye devam ettiği sürece siber güvenlik riskinin artması da devam edecektir. Bu noktada ağların, güvenliğini iyileştirmek ve siber saldırıları önlemek için SCADA ağlarının güvenliğinin sağlanması kritik bir ihtiyaçtır. Fakat ağın güvenliğinin sağlanması hususunda birçok teknik zorluk hâlâ devam etmektedir (Igure, Laughter ve diğerleri.2006: 498,506).

SCADA sistemlerinin haberleşmesinde en sık kullanılan haberleşme protokollerinden Mobdus TCB protokolünde, kimlik doğrulama ve veri iletiminde haberleşme olmaması gibi zafiyetler bulunmaktadır. Bu zafiyetler istismar edilerek manipüle edilebilmektedir. Bu sisteme gerçekleştirilen bir saldırıda Linux işletim sistemiyle önemli işletmelerin, otomasyon sistemlerinin kontrol edilerek değiştirilebileceği ve basit sistemlerle karmaşık sistemlere zarar verilebileceği ispatlanmıştır. Bu sebeple basit siber saldırılardan karmaşık siber saldırılara kadar yapılan tüm saldırı senaryolarında her aşamada tüm saldırlar teknik detaylarıyla ele alınıp değerlendirilmelidir. Sonuç olarak kritik alt yapı sistemlerinin güvenliğinde kullanılan SCADA sistemlerinin kullanılmasında insan hayatını, toplum düzenini ve ekonomik kayıpları, ulusal ve uluslararası düzeyde sekteye uğratabileceği düşüncesiyle güvenlik bilincinin oluşturulması ve buna uygun tasarlanma çalışmaları gerekmektedir. Konuyla ilgili ülkemizde elektrik üretim, iletim ve dağıtımında kullanılan kontrol sistemleri ile haberleşme protokollerinin tekrar gözden geçirilerek düzenlemelisi siber güvenlik açısından yüksek önem düzeyine sahiptir (Irmak ve Erkek, 20018: 16).

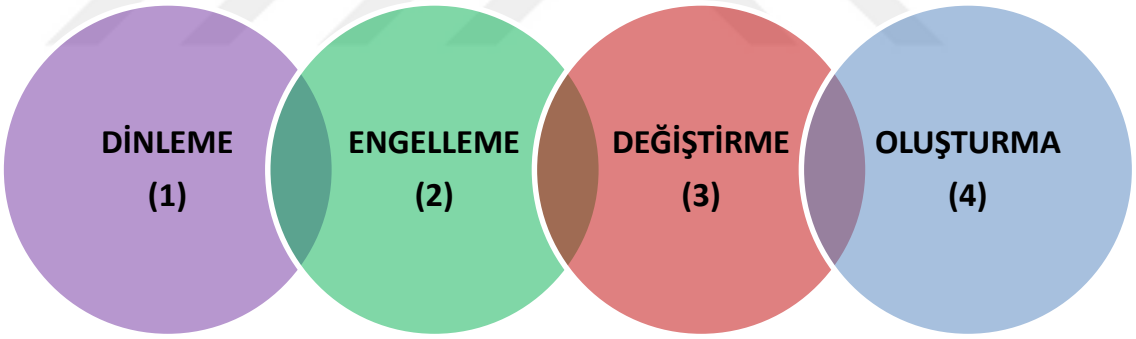
3. HACKER (KIRICI) VE HACKİNG NEDİR?

Bilgisayar korsanı olan dijital hırsızlar, sanal alemin askerleri, elektronik sınırların liderleri vb. bir çok isimle anılan bu kişiler hacker (kırıcı) olarak tanımlanmaktadır. Gerçekleştirdikleri eylemlere göre bu kişilerin kahraman mı

yoksa suçlumu olduklarının cevabı aslında çatışma halindedir. Bir bakıma hacker yani kırıcı hem bir üstat, hem bir korsan, hem de bir eylemcidir. Bu sebeple; Kırıcı Nedir? Kimdir? Ne Yapar? Sorularına toplumsal kitle iletişim araçlarından, ticari güçlerden, devlet ve muhaliflerden farklı yanıtlar geldiğinden konunun tanımlanması konusunda çatışmalar yaşanmaktadır. Bilinen gerçek şudur ki hackerlar gerçekleştirdikleri eylemlerle bilgisayar ve internet kültürünü doğrudan etkilemektedirler. Genel anlamda hacker: Bilgisayar ve bilgisayar ağı gibi sistemlerin içsel işleyişinde derin bilgi sahibi olan bir sistemlerde güvenliği kıran veya çökerten, kaynak kodları açık olan programları yazan ve paylaşan kişiler olarak tanımlanabilmektedir. (Eriş, 2009: 1-11).

Hacking kavramı ise genel olarak teknik araçlarla yasaklanmış sistemlere zorla girmeye çalışmaktır. Hacking eyleminde hacker, teknik güvenlik boşluklarından fırsatlar ve avantajlar elde etmeye çalışmaktadır (Bağcı, 2008: 43-51)

İnternette gerçekleştirilen hacking teknikleri temel olarak dört kategoriye ayrılır. Şekil 10 ile hacking teknikleri gösterilmektedir.



Şekil 10: Hacking Teknikleri

Kaynak: Berkay, A.(2009) Hack Teknikleri. Yayınlanmış ders notlarından derlenerek hazırlanmıştır.

1.Dinleme: Bu eylemde izin verilmemiş yetkisiz bir taraf öncelikle kaynağa erişim sağlar. Yetkisiz olarak adlandırılan taraf bir şahıs veya bir program ya da bir bilgisayar olabilir. Bu eylemde ağdaki tüm verilerin ve dosyaların kopyasına ulaşabilmektedir.

2.Engelleme: Sistemin bir kaynağı yok edilir ya da kullanılamaz hale getirilir. Bilgisayar donanımının bir kısmının bozulması, iletişim hatlarının kesilmesi ya da dosya yönetim sisteminin kapatılması engelleme eylemine örnektir.

3.Değiştirme: Yetkisiz taraf kaynağa erişimin sağlanmasıyla birlikte üzerinde değişiklik yapar. Farklı işlemler gerçekleştirmek üzere dosya ya da program değiştirilebilmektedir. Ağ üzerinden iletilen bir mesajın içeriğinin değiştirilmesi konuya örnektir.

4. Oluşturma: Yetkisiz yani izinsiz taraf sisteme yeni nesneler ekler. Ağ üzerinden gerçek olmayan sahte mesajlar yollanması veya bir dosyaya ilave kayıtlar yapılması gibi (Berkay, 2009: 5).

3.1. Hacker Çeşitleri

Hackerların iyi niyetli mi yoksa kötü niyetli mi olduklarının ayrımı şapka renklerine göre belirlenmektedir. Hackerların eylemlerini kimin ya da kimlerin adına yaptıkları şapka renklerinin belirlenmesinde en önemli unsurdur. Hackerların eylemlerinde şapka renkleri amaçlarına göre farklılık göstermektedir. Şapkalarda beyaz renk masumiyeti, siyah renk kötülüğü, gri renk net olmayan niyetleri, kırmızı renk ise farklılığı temsil etmektedir (Kara, 2013: 11).

3.1.1. Siyah Şapkalı Hacker

Siyah şapka kısaca hacker'ın gelecekteki karanlık ve kirli planlarını temsil etmektedir. Siyah şapkalıların faaliyetleri ve karanlık planlarının tespit ve rapor edilmesinde beyaz şapkalı hacker'ların rolü büyüktür. Bilgisayar güvenliğini istismar eden ve çoğunlukla anti sosyal kişilikte olan siyah şapkalıların tüm eylemleri kötü niyetle yapılmaktadır. Amaç bilgisayar sistemlerine saldırarak karşı tarafa zarar vermektir. Bu noktada gri şapkalılar siyah şapkalıların izinden giden vekiller olarak tanımlanabilir. Hackerlar topluluğunda özenle gizlenen teknik bilgi ve becerilere sahiptirler. Ayrıca zengin veri kaynağı ve arama motoru kayıtlarına sahiptirler. Proxy (Network şifreleme sistemi) kullanırlar, böylece girdikleri sistemlerde kimliklerini gizleyip izlerini silmektedirler (Mahmood ve diğerleri, 2010: 431-433).

3.1.2. Beyaz Şapkalı Hacker

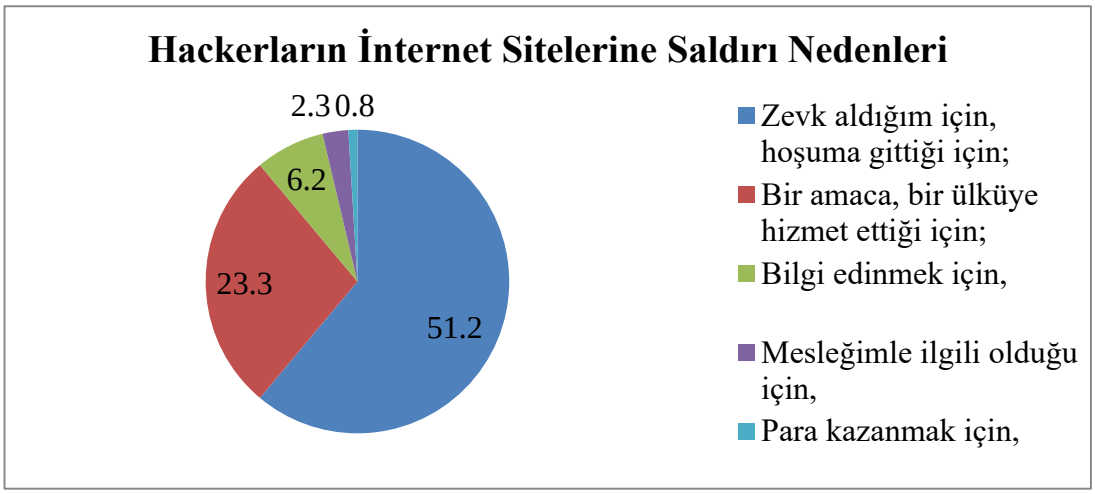
Beyaz şapkalı hacker'lar literatürde etik hacker olarak geçmektedir. Başka bir deyişle bu kişiler güvenlik zırhları olarak tanımlanabilmektedir. Günümüzde kontrol edilebilen ve tüm teknolojik cihazlarda bulunan güvenlik açıkları nedeniyle etik hackerlar için gerekli olan sertifikasyon eğitimleri giderek önem kazanmaktadır. Kötü niyetli olan siyah şapkalı hacker'lara yetişebilmek ve engel olabilmek için teknik anlamda bilgilerini güncelleyip aynı zamanda etik becerini güçlendirmek beyaz şapkalıların eğitim ve yönetim stratejileridir. Bir hırsızı en iyi yine bir hırsız yakalar. Bu noktada beyaz şapkalıların, niyetleri ve akıllarının nasıl çalıştığı önem kazanmaktadır. Özellikle kurumsal ağların karşılaştığı tehditler nedeniyle etik hackerlar için yükselen bir talep ortaya çıkmaktadır (Caldweell, 2011: 10-13).

3.1.3. Gri ve Kırmızı Şapkalı Hacker

Gri şapkalı hackerlar nadiren de olsa siyah şapkalı hackerlar gibi saldırılar düzenleseler de çoğunlukla yasal sınırlar içerisinde hareket etmektedirler (Dilsiz, 2012: 135). Bununla birlikte gri şapkalı hackerların, siyasi ve toplumsal değişim üzerindeki etkileri belirsizdir (Korhan, 2017: 81). Günümüzde kırmızı şapkalı hacker olduğunu savunan kişiler mevcuttur. Kırmızı şapkalılar, ne siyah nede beyaz şapkalı hacker olmaya eğilimi olmayan kişiliklerdir. Bu kişilerin bir hacker olma kültürü olmadıklarından kırmızı şapkalılar olarak tanımlanmaktadır (Kara, 2013: 14).

4. HACKER'LARIN İNTERNET SİTELERİNE SALDIRI NEDENLERİ

2009 yılında Türkiye'de yapılmış olan bir doktora çalışmasında, bilgisayar korsanlarının kültürü değerlendirmeye alınmış ve bilgisayar korsanlarının odaklandığı sitelere üye olan 258 Türk bilgisayar korsanına çevrimiçi anket uygulanmıştır. Elde edilen verilere göre katılımcıların % 51,2'si zevk aldığı için %23,3 'ü bir amaca hizmet ettiği için %6,2 'si bilgi edinmek için %2,3 'ü mesleğiyle ilgili olduğu için %0,8'i ise para kazanmak amacıyla bilgisayar korsanlığı yapmaktadır (Eriş, 2009: 164). Hackerların internet sitelerine saldırı nedenleri Grafik 1 ile görselleştirilmiştir.



Grafik 1: Hacker'ların İnternet Sitelerine Saldırı Nedenleri

Kaynak: Eriş, U(2009).Türkiye'de Kırıcı Hacker Kültürü. Yayınlanmış Doktora Tezinden Derlenerek Hazırlanmıştır. S.164.

5. İNTERNET GÜVENLİĞİ VE SAYISAL VERİLERLE NESNELERİN İNTERNETİ

Orijinal ismi İnternet of Things (loT) olan ''Nesnelerin İnterneti'' kavramı teknoloji liderlerinden Kevin Ashton tarafından 1999 senesinde Procter & Gamble şirketi için hazırlanan sunumda kullanılmıştır. Yıllar içinde gelişen teknolojiler ile birlikte milyarlarca insanın bilgisayarlar ve taşınabilir mobil araçlarla internete bağlanmaları kolaylaşmıştır. Sonraki adım birbirine bağlanan bilgisayarların, birbirine bağlı olan nesneler ile bilgi alışverişinde bulunmaları olmuştur. Bilgisayarlardan elektrikli aletlere, elektrikli aletlerden telefonlara, telefonlardan, akıllı binalara ve akıllı ulaşım sistemlerine kadar akıllara gelebilecek tüm nesnelerin birbirleriyle bağlantıda olmaları nesnelerin interneti olarak tanımlanmaktadır. Her geçen gün gelişmekte olan nesnelerin interneti, yakın gelecekte yüksek bir ivme kazanarak insanoğlunun hayatına tamamen entegre olacaktır. Genel anlamda nesnelerin interneti birbirine bağlanarak bilgi aktaran akıllı bir ağ ile oluşturulmuş cihazlar sistemidir. Tüm bu teknolojik gelişmeler tartışmasız hayatımızı kolaylaştırmaktadır. Fakat bu noktada kilit sorun, akıllı nesnelerle birlikte yaşanabilecek bilgi güvenliği problemidir. Günümüzde elektronik cihaz üreticilerinin tamamı ürünlerini akıllı kelimesini kullanarak pazarlamaktadır. Akıllı telefonlar, televizyonlar, arabalar, daireler, ısıtma, soğutma, havalandırma, ışıklandırma, yangın

ve hırsız alarmları, bilgisayarlı kasa ve kapı kilit sistemleri, ulaşım sistemleri vb. birçok ürünün üzerinde aslında yüksek derecede güvenlik açıkları bulunmaktadır. (Turak, Beceni 2015: 3-8).

Bir ağa veya internete bağlı olan bir bilgisayar veya bir cihaz buradan gelebilecek olası her türlü tehlikeye karşı savunmasızdır. Savunmasız olan bilgisayar ve cihazlara; virüsler, truva atları, solucanlar, casus yazılımlar ve tuş kaydedicilerin bulaşmasıyla birlikte kişisel verilerimiz hacker'lar tarafından ele geçirilmektedir. Tüm bu tehlikelerden korunabilmek için bilgisayarlar ve cihazlarda antivirüs yazılımı ve güvenlik duvarı yazılımının birlikte kullanılması tavsiye edilir. Bu noktada ücretsiz olarak kullanılmak istenilen antivirüs ve güvenlik duvarı yazılımlarına özellikle dikkat edilmeli ve özenle seçilmelidir (Zeydan, 2006: 326).

Bilgi Teknolojileri ve İletişim Kurumunun (BTK) 2016 yılı, faaliyet raporu incelendiğinde toplam da 19.948.897 adet Uluslararası mobil cihaz kimliğinin (IMEI), Mobil Cihaz Kayıt Sisteminde (MCKS) kayıt altına alındığı görülmektedir. Söz konusu kayıt altına alınan cihazların ithalat, imalat ve yolcu beraberinde getirilen cihazlardan oluştuğu görülmektedir. İthalatçı başvurusuyla kayıt altına alınan cihazların sayısı 17.601.966, imalat yoluyla kayıt altına alınan cihazların sayısı 1.572.991, yolcu beraberinde getirilen cihazların sayısının 773.940 olduğu görülmektedir (www.btk.gov.tr/ BTK 2016 Yılı Faaliyet Raporu.s.96).

Tablo 3 ile 2013 ve 2017 yılları arasında internet, bilgisayar ve mobil telefon kullanıcı oranları gösterilmektedir.

Tablo 3: 2013-2017 Yılları İnternet, Bilgisayar ve Mobil Telefon Kullanıcı Oranları

Milyon Bazında	2013	2014	2015	2016	2017
16-74 Yaş Bireylerin Bilgisayar Kullanım Oranları	49,9	53,5	54,8	54,9	56,6
16-74 Yaş Bireylerin İnternet Kullanım Oranları	48,9	53,8	55,9	61,2	66,8
Geniş Bant İnternet Abone Sayısı	32,57	41,2	48,57	62,24	68,87
2G-3G ve 4,5G Mobil Telefon Abone Sayısı	69,7 (2G-3G)	71,9 (2G-3G)	73,7 (2G-3G)	51,7 (4,5G)	64,6 (4,5G) 13,4 (2G-3G)

Kaynak: http://www.udhb.gov.tr T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Strateji Geliştirme Başkanlığı, "İstatistiklerle ulaştırma denizcilik ve haberleşme 2003-2017" raporundan derlenerek hazırlanmıştır. Ss.75-81.

6. ULUSLARARASI BAĞLAMDA SİBER GÜVENLİK VE SİBER GÜVENLİK KURUMLARI

Günümüzde uluslararası düzeyde birçok ülke siber alanda yetersizdir. Gelişmekte olan ve gelişen pazarlarda birkaç ülke dışında ülkelerin siber güvenlik mevzuatlarında eksiklikler görülmektedir. Bu durum birkaç faktörle ilişkilendirilebilir. Bu faktörlerin başında siber alanın ulusal ve uluslararası düzeyde hafife alınması gelmektedir. İçinde bulunduğumuz siber dünyada, siber yargı uzmanlarının yetiştirilmesinde ki eksiklikler nedeniyle hukuki alanda yasaların ve mevzuatların geliştirilmesi de gecikmektedir. Diğer taraftan ülkelerde yabancı yatırımcıların artması, gelişmekte olan ülkeleri siber güvenlik yasalarını geliştirmeye teşvik etmektedir. Günümüzde yatırımlar artarak artan oranda elektronik araçlar üzerinden yapılmakta, imzalarda dahi e-imza kullanılmaktadır. Bu gelişmeler ülkeleri e-işlemlerle ilgili yasalarını geliştirmeye itmektedir. Bu durum siber güvenlikte reaktif (tepki oluşturan) bir yaklaşımdır. Siber alanda başarının anahtarı ise yasal düzenlemelerin proaktif (mevcut koşulların seyrini değiştirmek) olarak değiştirilmesi ve yürürlüğe konulmasıdır. Başka bir cephede, siber uzay aslında küresel anlamda bir meydan okuma olduğundan konu dünya üzerindeki tüm ülkeler için bir fırsat ve uluslararası düzeyde kritik bir ihtiyaçtır. Sonuç olarak yenidünyayı yöneten yasaların geliştirilmesinde işbirliğine ihtiyaç duyulmaktadır. Siber alan sınırsızdır çünkü zaman ve mekândan bağımsız saldırıyı mümkün kılar. Suçluları ise yasal boşlukları kötüye kullanır. Bu açıdan değerlendirme yapıldığında ülkelerin uluslararası alanda işbirliği yapmaları, bölgesel işbirliği üstlerini kurmaları, bilgi alışverişinde bulunarak en iyi uygulamaları paylaşmaları, yasama eğitimiyle birlikte tüm personel ve kolluk görevlilerini eğitmeleri büyük önem arz etmektedir.

Avrupa'daki ITU (Uluslararası Telekomünikasyon Birliği) siber suçlar sözleşmesi, gelişmekte olan ülkeler için örnek bir modeldir. Fakat siber suçlarda hala küresel bir yönetim mevcut değildir. Siber suçlarda en önemli konu siber hukukun inşası ve uygulamadaki başarısıdır. Bu noktada kamu ve özel sektör işbirliği önem kazanır. İşbirliğindeki en iyi başlangıç ise personel gelişimi ve eğitimi olacaktır. Sonraki aşama vatandaşların bilinçlendirilmesinde işbirliği çalışmaları yapılmasıdır.

Çünkü özellikle gençler, hem ekonomik hem de sosyal açıdan siber suçlularla karşı karşıyadır. Bu alanda kültürel bilincin oluşmasına yardımcı olacak bilinç ve anlayışın geliştirilmesine yönelik politikaların, yasaların ve stratejilerin geliştirilmesine yönelik çalışmalar yapılması siber güvenliğin büyüyerek gelen çok yönlü maliyetini azaltacak ve ulusal düzeyde iyi bir başlangıç yapılmasına imkân sağlayacaktır. Siber güvenlikte uluslararası düzeyde çağımızdaki en büyük sorun siber yasaların olması, fakat etkili yaptırım mekanizmalarının olmamasıdır. Çoğu yasa siber suçluları caydırmak için gerekli olan dişlerden yoksundur. Bu bakımdan cezalar etkisiz ve yetersiz kaldığından daha sert yasaların yürürlüğe konulması gerekmektedir. (Shalhoup ve Al Qasimi, 2010: 230-232).

Avrupa ülkelerinden biri olan Almanya 2018 yılı içinde yapmış olduğu bir açıklamada kendi siber silahlarını geliştirmek için İçişleri ve Savunma Bakanlıkları tarafından desteklenen bir siber güvenlik ajansı oluşturmayı planladıklarını basına duyurmuştur. Alman ordusu mevcut durumda ABD tarafından geliştirilen askeri yazılımlara bağlıdır. Fakat yeni kurulan ajansla birlikte siber güvenlikte, askeri bürokrasiyi azaltıp Ar-Ge faaliyetlerini arttırmayı hedeflemektedir (https://www.cnnturk.com/ , 2018). Diğer taraftan ABD siber güvenlik için bağımsız bir komutanlık kurmuştur. ABD Stratejik Kuvvetler Komutanlığına bağlı bir alt komutanlık olan Siber Güvenlik Komutanlığı 2018 yılı içinde bağımsız bir komutanlığa dönüştürülmüştür. Bu bağlamda Siber Güvenlik Komutanlığı, aynı çatı altında bulunduğu Ulusal Güvenlik Ajansından (NSA) ayrılmıştır. Bu nedenle ABD tarafından yapılan siber güvenlik operasyonlarında önemli bir artış olması beklenmektedir. Pentagondan yapılan açıklamada ise 2018 Eylül sonuna kadar komutanlığın dönüşümü tamamlanarak personel sayısının 800'den 6.200'e çıkartılacağı basına duyurulmuştur. (https://www.trthaber.com/ ,2018). Araştırmalar, tarihteki en büyük ekonomik kaynak transferlerine neden olan yenilik ve yatırım teşviklerini riske atacağı umulan siber suçların, 2021 yılına kadar her yıl 6 trilyon dolar küresel maliyete neden olacağını göstermektedir. Öyle ki 2021 yılına kadar en fazla prim büyümesinin siber sigorta ürünlerinde olacağı açıklanmaktadır. (http://www.milliyet.com.tr, 2018). Siber güvenlikte yaşanabilecek tüm tehditler değerlendirmeye alındığında ihtiyaç duyulan tedbirlerin başında koordinasyon ön plana çıkmaktadır. Bununla birlikte bilinçli bir kullanıcının yerini hiçbir teknolojinin dolduramayacağı yapılan değerlendirmeler arasındadır (Öğün ve Kaya, 2013: 174).

Araştırmalar uluslararası düzeyde siber savunma yeteneklerini artıran ülkelerin, diğer ülkelere kıyasla kıymetli varlıklarını koruyabilmede üstünlük sağladığını göstermektedir (Shafgat and Masood, 2016: 135).

6.1. USGF (Uluslararası Siber Güvenlik Federasyonu)

Kurumun temel amacı siber saldırılara ulusal düzeyde hazırlıklı olunmasını sağlamaktır. Federasyonun amacı tüzüğünde şu şekilde tanımlanmıştır.

Türkiye Cumhuriyeti Anayasası ve Kanunları doğrultusunda, kendisine bağlı derneklerin amaçlarını gerçekleştirmelerine yardımcı olmak, bu amaçla kendisine bağlı dernekler arasındaki koordinasyon ve işbirliğinin en üst düzeye çıkarılması temel olmak üzere, siber güvenlik teknolojileri ile siber savunma teknolojilerinin kullanımını yaygınlaştırmak, siber tehlikelere karşı farkındalık oluşturmak, siber güvenlik teknolojilerindeki gelişmelerden de faydalanarak bu alanda, siber saldırılardan da korunmak için alınabilecek önlemler konusunda farkındalık yaratmak için bilişim ve siber güvenlik alanlarında çalışan kişi ve kurumlar arasında işbirliğini sağlamak, özellikle kamu ve özel sektörde faaliyet gösteren gerçek ve tüzel kişiler arasında farkındalığın ve işbirliğinin geliştirilmesi yönünde çalışmalar yapmak, yurt içi ve yurt dışında etkinliklerde bulunmaktır (www.usgf.org.tr , 2018).

6.2. NSA (Ulusal Güvenlik Ajansı)

Uzmanlık alanı kriptoloji olan kurumun resmi kuruluş tarihi 1952 yılıdır. Genel merkezi ABD Maryland'ta bulunmaktadır. Ulusal güvenlik sorunlarının üstesinden gelmek için kurulan NSA, ihtiyaç duyduğu yetenek ve araçları geliştirmek için okullarla ve üniversitelerle ortaklaşa çalışmalar düzenlemektedir. Bu çalışmalar arasında;

- Yaz kampları gibi beceri geliştirme programları açmak,
- Siber güvenlik kariyer alanı için müfredat geliştirilmesini teşvik amaçlı çalışmalar düzenlemek,
- Sponsorluk becerileri ve araştırma ödevi yarışmaları düzenlemek,
- Stajyer öğrenciler için olanaklar yaratmak,
- Araştırma hibeleri vermek, araştırma laboratuvarları ve projeleri finanse etmek; NSA'nın okullarla ortaklaşa düzenlediği eylemler arasındadır.

Kurum yaptığı bu ortaklıklarla; bilim, teknoloji, mühendislik ve matematik alanlarında yeni nesil uzmanların yetiştirilmesine olanak sağlamaktadır. Bu ortaklıklar aynı zamanda ABD'yi siber saldırılardan koruyabilecek yetenekli siber güvenlik uzman havuzunu genişletmektedir. Kurumun ortaklıkları incelendiğinde hem üniversite seviyesinde hem de ilköğretim seviyesinde ortaklıklara fırsat verildiği görülür. NSA, öğrenci, eğitimci ve akademik araştırmacılar için her düzeyde çeşitli organizasyonlar kurup yeni fırsatlar yaratarak katılımcıları teşvik eder. NSA ayrıca siber operasyonlarda, akademik mükemmeliyet merkezlerini kurmuştur. Bu oluşumda hedef, dijital bir ulus oluşturarak siber güvenlikte güvenli bir ulusu destekleyebilecek vasıflı işçi havuzunun genişletilmesidir (https://www.nsa.gov, 2018). ABD, siber güvenlikte en dikkat çekici yatırımları yapan ülkelerin başında gelmektedir. ABD bütçe çalışmalarında, sağlıktan sosyal güvenliğe, uzay araştırmalarından Ar-Ge'ye kadar birçok alanda kısıntıya giderken siber güvenlik harcamalarında 800 milyon USD (%21) artış planlamaktadır. ABD'nin siber güvenlik bütçesi incelendiğinde 2013 yılında siber güvenlik harcamalarına 3.9 Milyar USD bütçe ayırırken 2014 yılında 4.7 Milyar USD bütçe ayırdığı görülmektedir. 2013 ve 2014 yılları siber güvenlik bütçesinin tamamı incelendiğinde sadece bir yılda siber güvenlik bütçesinde %21 artış olduğu görülmektedir (Alkan, 2017: 23).

6.3. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı)

Avrupa Birliği'ne bağlı ağ ve bilgi güvenliğinden sorumlu olan ajanstır. 2004 tarihinde kurulmuş olup merkezi Yunanistan'ın Kandiye kentinde yer almaktadır. Ajans, tavsiye ve çözümler sunmak için üye devletler ve özel sektör ile birlikte çalışmaktadır. Yaptığı çalışmalar arasında, Pan-Avrupa Siber Güvenlik Alıştırmaları, Ulusal Siber Güvenlik Stratejilerinin Geliştirilmesi, güvenli bulut benimseme çalışmaları, veri koruma sorunları, gizlilik artırıcı teknolojiler ve gelişmekte olan teknolojiler üzerine çalışmalar yer almaktadır. ENISA, faaliyetlerini üç alanda sunar. Bunlardan ilki önerilerde bulunmak, ikincisi politika oluşturmak ve uygulamaları destekleyen çalışmalarda yer almak, üçüncüsü ise AB çapında operasyonel ekiplerle doğrudan işbirliği yaparak "Hands On" çalışmalarında yer almaktır (https://www.enisa.europa.eu/, 2018).

6.4. ITU (International Telecommunication Union- Uluslararası Telekomünikasyon Birliği)

ITU, Paris'te 1865 yılında uluslararası telgraf birliği olarak kurulmuştur. 1934 yılında bugünkü adını almış 1947 yılında ise Birleşmiş Milletlerin uzman bir kuruluşu olmuştur. Şuan ki merkezi İsviçre, Cenevre'dir. Dünya çapında 12 bölge ve bölge ofisine sahiptir. Günümüzde 193 ülkeye ve 800 özel sektör kuruluşuna ve akademik kurumlara üyedir. ITU, Birleşmiş Milletler bilgi ve iletişim teknolojileri konusunda uzmanlaşmış bir kurumdur. Küresel boyutta radyo spektrumunu ve uydu yönergelerini tahsis ederek ağların ve teknolojilerin sorunsuz bir şekilde birbirlerine bağlanmasını sağlayan teknik standartları geliştirmektedir. Üç ana faaliyet alanı bulunur;

- **Radyokomünikasyon:** Uydular aracılığıyla gerçekleştirilen telefon görüşmeleri, televizyon programları, uydu navigasyonu ve çevrimiçi haritalara erişimi sağlar. Uzay hizmetleri aracılığıyla sera gazı gibi verilerin izlenmesi ve iletilmesinde hayati öneme sahip çalışmaları yürütür. Bu anlamda bir kasırganın veya küresel iklimin nasıl değiştiğinin tahmin edilmesine yardımcı olur. Ayrıca radyo frekans spektrumunun ve uydu yönergelerinin uluslararası yönetimini koordine etmektedir.
- **Standardizasyon:** Bilgi teknolojilerinin işleyişinde önerilerde bulunur. Telefon görüşmeleri, internet erişimi, ulaşım protokolleri gibi telekomünikasyon standardı sistemlerinin, yerel ve küresel çalışmalarına izin vermektedir.
- **Gelişme:** Büyümekte olan pazarlarda küresel bazda bilgi teknolojileri liderliğini yaparak en iyi politikaların hayata geçirilmesine hizmet eder. Uluslararası düzeyde dijital uçurumu birleştirmeyi amaçlar. En önemli faaliyetlerinden biride sektörün en güvenilir ve kapsamlı bilişim ve iletişim teknolojileri istatistiklerini düzenli olarak yayımlamaktır (https://www.itu.int , 2018).

6.5. INTERPOL (Uluslararası Kriminal Polis Teşkilatı)

1923 yılında uluslararası alanda polis işbirliğini sağlamak amacıyla kurulmuştur. 1956 yılında teşkilatın yeni ismine dâhil edilmiştir. Genel merkezi Fransa Lyon'da bulunur. 192 üyesiyle dünyanın en büyük polis teşkilatı kuruluşudur.

INTERPOL siber suçlara karşı küresel mücadele yürütür. Çoğu siber suç, ulus ötesi niteliktedir. Siber suçları kooperatif düzeyinde araştıran INTERPOL, kendini yasa uygulayıcı kurumların doğal ortağı olarak tanımlamaktadır. Bu amaçla özel sektörle birlikte çalışarak siber istihbarat ile yerel yasaların uygulanmasını sağlar. Siber suçlarda ana girişimleri şu konular üzerine odaklanmaktadır.

- Operasyonel araştırmacılara destek vermek,
- Siber zekâ ve analiz,
- Dijital Adli Tıp,
- İnovasyon ve Araştırma,
- Kapasite geliştirme ve ulusal siber olaylar (https://www.interpol.int/, 2018)

Ayrıca Singapur'da bulunan Global İnovasyon Kompleksi (IGCI) aracılığıyla dijital suçların tespiti ve önlenmesi konusunda küresel bir koordinasyon kuruluşu olmayı taahhüt etmektedir. 2014 yılında açılan bu modern araştırma ve geliştirme tesisi, yasa uygulayıcılardan önemli özel sektör ortaklıklarına kadar küresel siber güvenlik uzmanlarından oluşmaktadır. Kurum siber suçlarla mücadelede en yeni eğitim teknikleri ve araçlarının geliştirilmesi üzerine proaktif çalışmalar yapmaktadır. Türkiye 13 Haziran 1956 yılından beri INTERPOL'e üye ülkeler arasındadır.

INTERPOL organizasyonunun yasal çerçevesi teknolojik gelişmelere uyum sağlamayı taahhüt etmektedir. Bu kapsamda birçok bilgi ve iletişim teknolojileri projeleri bulunur. Bilişim hukuku projelerinden iki tanesi aşağıda açıklanmaktadır;

- **EVIDANCE2 e- CODEX projesi:** INTERPOL, AB içinde elektronik delil alışverişini kolaylaştırarak karşılıklı hukuki yardım çerçevesinde e- CODEX üzerinden dijital kanıtların değişimi için uluslararası iş birliğini sağlamak(https://evidence2e-codex.eu/, 2018).
- **TITANIUM projesi (Yeraltı Piyasalarda İşlemlerin İncelenmesi):** Sanal para birimlerini ve karanlık ağlardaki yer altı piyasaları içeren terörist faaliyetlerini araştırmakla görevlidir. Hukuki yürütme ajanslarını desteklemek amacıyla tasarlanan yeni verilere dayalı teknikleri ve çözümleri araştırır (https://www.titanium-project.eu/, 2018).

6.6. NATO (Kuzey Atlantik Antlaşması Örgütü)

1949'da Kuzey Atlantik Anlaşmasına dayanarak kurulan uluslararası askeri ittifaktır. Merkezi Belçika'nın başkenti Bürükselde bulunur. NATO'nun şu anda 29 üye ülkesi bulunmaktadır. Son olarak 2017 yılında Karadağ üye olmuştur. NATO'nun resmi internet sitesinde, üyelerinin özgürlüğünü ve güvenliğini siyasi ve askeri yollarla garanti etmeye çalışmasının temel amacı olduğu belirtilmektedir. NATO'nun kuruluş anlaşmasının toplu savunma maddesi olan Washington Antlaşmasının 5. Maddesi uyarınca ya da Birleşmiş Milletlerin görevi altında diğer ülkeler ve uluslararası kuruluşlarla işbirliği içerisinde olduğu belirtilmektedir (https://www.nato.int/nato-welcome/index.html, 2019). Türkiye'nin Şubat 1952'de NATO'ya üyeliği kabul edilmiştir (Türkman, 2014: 144). NATO'nun siber savunmaya yaklaşımı Galler'de ki 2014 NATO Zirvesinde netleşmiş, siber savunma NATO'nun temel kolektif bir savunma görevi olarak kabul edilmiştir. 2016 yılında Varşova Zirvesinde Müttefikler siber uzayı; tıpkı hava, deniz ve kara gibi bir operasyon alanı olarak tanımlamıştır. Varşova zirvesinde NATO'ya üye tüm müttefikler ulusal ağlarının siber savunmasında altyapılarını güçlendirmek için Siber Savunma Kararını kabul etmiştir. Bu kararda her bir müttefikin kendi siber savunmasından sorumlu olduğu ancak NATO'nun müttefiklerine birçok yönden yardımcı olacağı yer alır. Müttefikler 2017 yılında NATO'nun siber savunma yeteneklerinin güçlendirilmesi amacıyla yeni bir siber operasyon merkezi kurma kararı almıştır. Siber operasyon merkezi üzerindeki çalışmalar devam etmektedir (NATO, 2018).

7. ULUSAL SİBER GÜVENLİK STRATEJİSİ

Ulusal siber güvenlik politikalarımızın sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlamak görevi 20 Ekim 2012 yılında, 2012/3842 karar sayılı, Bakanlar Kurulu Kararı ile T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na verilmiştir. Karar ile birlikte siber güvenlikte alınacak tedbirleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak bu eylemlerin uygulanmasını ve koordinasyonunu sağlamak amacıyla; Siber Güvenlik Kurulu Kurulmuştur (http://www.resmigazete.gov.tr/, 2018) Bu kapsamda T.C. Ulaştırma, Denizcilik ve Haberleşme bakanlığının görevleri şunlardır:

- Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak,
- Kamu Kurum ve Kuruluşlarına ait bilgi ve verilerin güvenliği ile birlikte mahremiyetinin güvenceye alınmasını sağlamaya yönelik usul ve esasları hazırlamak,
- Ulusal siber güvenliğin sağlanmasında kamu kurum ve kuruluşlarında, teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasının test edilmesini sağlamak,
- Ulusal bilgi teknolojileri, iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırıları izlemek, müdahale ve önleme sistemlerini oluşturarak, ilgili merkezleri kurmaya, kurdurmaya ve bu sistemlerin denetimi, işletimi ve güçlendirilmesine yönelik çalışmalar yapmak,
- Ulusal siber güvenliğin sağlanmasında milli çözümlerin gelişimine öncülük etmek, siber saldırılara müdahale araçlarının gelişimi ve üretimini konularında teşviklerde bulunarak, kullanımlarını sağlamak,
- Ulusal siber güvenlik için kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek,
- Bu karar çerçevesinde diğer ülkeler ve uluslararası kuruluşlarla işbirliği yapmak,
- Ulusal siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı arttırma çalışmalarını yürütmek,
- Siber Güvenlik Kurulunun sekretarya hizmetlerini yürütmek,
- Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esasları belirleyerek güvenlik belgesi vermektir.

İlgili bakanlar kurulu kararının içeriğinde 5809 sayılı Elektronik ve Haberleşme Kanununa eklenen Ek madde 1 ile de Siber Güvenlik Kurulunda yer alacak bakanlık, kamu kurum ve kuruluşları ile üyeleri, Ulaştırma Denizcilik ve Haberleşme Bakanı'nın başkanlığında aşağıdaki gibi sıralanmıştır;

- Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,

- Milli Savunma Bakanlığı Müsteşarı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,
- Kamu Düzeni ve Güvenliği Müsteşarı,
- Milli İstihbarat Teşkilatı Müsteşarı,
- Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,
- Bilgi Teknolojileri ve İletişim Kurumu Başkanı,
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı,
- Mali Suçlar Araştırma Kurulu Başkanı,
- Telekomünikasyon İletişim Başkanı,

İle Ulaştırma Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır (https://www.btk.gov.tr/siber-guvenlik-kurulu, 2018).

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığının ismi T.C. Ulaştırma ve Altyapı Bakanlığı olarak değişmiştir. Şu anda uygulamada olan stratejisi, 2016-2019 Ulusal Siber Güvenlik Stratejisidir (http://www.udhb.gov.tr, 2018) Bu strateji kapsamında Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş ve Siber Olaylara Müdahale Ekipleri (SOME) oluşturulmuştur. Ulusal Siber Olaylara Müdahale Merkezi olan USOM, ülkemizin siber güvenliğine karşı siber ortamlarda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve etkilerinin azaltılması ve ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi amacıyla belirlenen aktörlerle Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde kurulmuştur. (https://www.usom.gov.tr/index.html, 2018) BTK'nın idari yaptırımlar yönetmenliğinde yaptığı son değişiklikle USOM'a verilen yetkiler arasında; siber güvenlikle ilgili gerekli tedbirleri almayan firmalara yönelik bin liradan, 1 milyon liraya kadar para cezası verme yetkisi tanınmıştır. Son bir yılda 6 binden fazla zafiyet ve açıklık belirleyen USOM konuyu ilgili firmalara iletmiş yayınlamış olduğu yönetmenlikle bu zafiyetleri gidermeyen firmalara idari para cezası kesme yoluna gitmiştir. (http://www.hgm.gov.tr, 2018)

8. SİBER SALDIRI KURBANI OLMAK NASIL ENGELLENİR?

Siber güvenlikte en önemli kavram farkındalıktır. Siber güvenlikte farkındalığın ölçülmesi için kişinin bilgi güvenliğine yönelik öğrenme arzusundaki davranışlarını engelleyen en önemli unsur kişinin ön yargılarıdır. "Benim telefonumda ve bilgisayarımda önemli bir bilgi ya da veri yok, bu sebeple herhangi bir siber saldırıyla karşılaşma ihtimalim yok" diyen bir kullanıcı bu düşüncesi nedeniyle verilerini koruma ihtiyacı hissetmemektedir. Bu sebeple kişi konu hakkında harekete geçmeyecek, bilgi birikimini arttırmayacak ve olası bir siber saldırıyla karşılaşma durumunda uygun davranış modeli sergilemeyecektir. Fakat aynı kişiden cep telefonu istendiğinde, cep telefonunu asla bir başkasına teslim etmeyecektir. Çünkü kişi, o ana kadar önemsiz gördüğü bir telefon numarasını, bir arkadaşından gelen mesajı ya da tek başınayken çektiği bir fotoğrafı bile bir başkasının bilmesini ve öğrenmesini istememektedir.

Özetle tüm kullanıcıların günlük hayatta gerçekleştirdiği sıradan işlemlerde bile kişisel verilerin gizliliği kullanıcılar için en önemli unsurdur. Kişiler ellerinin altında bulunan teknolojileri kullanırken yeri ve zamanı geldiğinde en ufak bir bilginin dahi saldırganlar tarafından kolaylıkla kullanılabileceğini bilmelidirler. Öyle ki önemsiz gibi görülen bu bilgiler siber saldırganlar için büyük engelleri aşmak için kullanılmaktadır. Bu sebeple siber güvenlikte, farkındalık unsurundan bahsedebilmek için öncelikle ön yargılardan sıyrılarak benim başıma gelmez anlayışını terk ederek gerçekçi bir yaklaşımla bilgi güvenliği konusunu benimsemek çok önemlidir. Bilgi güvenliğinde tehditlerden ve olası saldırılardan etkin olarak korunmak ve uygun davranış modeli sergileyebilmek için yapılması gereken ilk iş bilgi sahibi olmaktır. Sonrasında bilgiyle birlikte gelen farkındalığın davranışa dönüştürülmelidir (Erol, 2016: 52-53) Olası siber saldırılara karşı korunabilmek için nelerin bilinmesi ve yapılması gerektiği aşağıda sıralanmıştır.

- Çevrimiçi veya çevrimdışı fark etmeksizin kişisel bilgiler paylaşılmamalıdır. Ev adresleri, konum ve yer bilgileri, aile fertlerinin isimleri ve telefon numaraları gibi kişileri tanımlayıcı bilgiler korunmalıdır. Özellikle gençler, çevrimiçi oldukları durumlarda arkadaşlarıyla bu tür kişisel bilgilerin paylaşımı konusunda dikkatli olmalılardır.

- Casus yazılım koruma yüklemesi mutlaka yapılmalı ve casus yazılım korumasının saygın bir şirket olduğundan emin olunmalıdır. Bunun için şirketin web sitesinden gerekli kontroller yapılmalıdır.
- Çevrimiçi sipariş, alışverişler ve sosyal medya kullanımlarında önemi olmayan yani sıklıkla kullanılmayan yeni bir hesap açılıp bu hesap üzerinden iletişim kurulmalıdır. Yabancılarla ve satıcılarla yeni oluşturulan hesap üzerinden iletişime geçmek, kişisel hesapların spam ve casus yazılımlardan korunmasına yardımcı olacaktır.
- Kullanılan e-posta isimleri için takma isimler kullanılmalıdır. Ayrıca sosyal medya hesapları üzerinde cinsiyeti nötr hale getirmek, fotoğraflar için konum atmamak ve profil fotoğrafı yerine bir görsel kullanmak siber ataklardan korunmaya yardımcı olmaktadır.
- Çevrimiçi bir siteye kayıt yapılırken tüm alanlar doldurulmamalıdır. Özellikle doğum tarihi gibi özel bilgilerin paylaşıldığı alanların doldurulmasından kaçınılmalıdır. Ev adresi gibi özel bilgilerin doldurulduğu alanlara ise daha güvenilir olan iş veya okul adreslerinin girilmesi daha güvenilir olacaktır. Ayrıca herhangi bir siteye kayıt olmadan önce sitenin gizlilik politikaları, dikkatlice okunmalıdır. Güvenilir olmayan siteler, gizlilik politikalarını sık sık değiştirdiklerinden gizlilik politikasının değiştirildiği son tarih kontrol edilmelidir.
- Sosyal medya sohbet odalarında (Twitter, Facebook, Instagram vb.) neler konuşulduğuna ve paylaşıldığına dikkat edilmelidir. Özellikle arkadaş çevrelerinden ve ailelerden konu hakkında tedbirli davranmaları istenmelidir. Çünkü gönderilen resimler, konumlar, beğeniler ve tüm etiketlemeler, bireysel ve ailesel veri gizliliğini ihlal etmektedir. Sosyal medya kullanıcısı özel hayatında tanımadığı kişilerin arkadaşlık isteklerini kabul etmemelidir. Sosyal medya üzerinde mümkün olduğunca az hesap açmaya özen gösterilmelidir.
- Banka hesap kartlarının, kredi kartlarının, E-postaların, sosyal medya hesaplarının ve cep telefonlarının giriş şifrelerinin, yılda en az iki kere değiştirilmesi, kişiyi siber saldırılara karşı korumaktadır. Ayrıca sosyal medya hesaplarında, sorulan güvenlik sorularına verilen yanıtların başkalarınca tahmin edilmesinin zor olması ve de kolay hatırlanabilir olması gerekmektedir. Örnek olarak; en sevdiğiniz yiyeceği soran bir güvenlik sorusuna, fıstık ezmesine alerjiniz varsa, fıstık ezmesi

olarak yanıt verilmelidir. Çünkü burada bir şaşırtma vardır. Ayrıca kullanıcı bu cevabı unutmaz.

- Şüpheli E-postalardan gelen maillere ve şüpheli telefonlardan gelen görüşmelere karşı temkinli olunmalı, her mesaj açılmamalı ve her bağlantıya tıklanmamalıdır. Özellikle kişisel bilgiler (T.C. Kimlik Numarası, doğum tarihi, anne kızlık soyadı vb.) şüpheli platformlarda, kesinlikle paylaşılmamalıdır. Çünkü bilinmeyen her bağlantıda en zararlı kötücül yazılım olan keylogger programları tanımlanmış olabilir. Bu tür yazılımlar; resim, fotoğraf, müzik, film, video gibi farklı formattaki dosyaların içine gömülerek bilgisayar kullanıcısının klavyede bastığı tüm tuşları arka planda kayıt altına almak suretiyle kişisel bilgileri ve şifreleri ele geçirmek üzere tasarlanmış programlardır (http://www.ensonhaber.com, 2018). Ayrıca bir siber saldırgan, bankaların gönderdiği metinleri ve banka yetkililerini taklit etmede ustadır. Bu tür bir telefon saldırısında telefon kapatılmalı, arayan numaraya tekrar dönüş yapılmalıdır.
- Her birkaç ayda bir kullanılan isim, soy isim ve telefon numarası için internet araması yapılmalıdır. Çünkü siber saldırganlar, kullanıcılar adına çalıntı bir sosyal medya hesabı, web sitesi ve blog açma eğilimine sahiptirler.
- Tüm tüketiciler çekmiş oldukları banka kredileri ve banka kredi kartlarının kullanım durumunu yılda en az bir kere, kredi kayıt bürolarından rapor isteyerek kontrol etmelidir. Ortada endişe edilecek bir durum olduğunda ise rapor yılda birkaç kere talep edilmelidir. Herhangi bir kimlik hırsızlığına kurban olmamak için gerektiğinde bürokrasiden ödeme yapmak koşuluyla yardım alınmalıdır. Bireysel kredi raporu, Findeks kredi kayıt bürosundan alınabilmektedir. Bireyler bu kuruma üye olmak koşuluyla bankalar ve diğer finansal kurumlardaki kredi ve borç limitlerini ve kredi notlarını takip ederek finansal kontrollerini sağlayabilmektedirler. (bkz. https://www.findeks.com/findeks-hakkinda, 2018).

Findeks'in vermiş olduğu hizmetler arasında şunlar yer almaktadır;

- **Kredi Notu Hizmeti:** Bankalara yapılmış olunan ödeme ve kredi kullanım alışkanlıklarını gösteren puanlamadır.
- **Risk Raporu Hizmeti:** Halen açık olan ve son 5 yıl içerinde kapanmış olan kredilerin ödeme detayları bulunmaktadır.
- **Uyarı Hizmeti:** Kredi notu, limit ve borçlardaki değişiklikleri haber vermektedir.

- **İzleme Hizmeti:** Bankalardaki tüm kredi ve kredi kartı bilgilerine tek seferde ulaşmayı sağlamaktadır.
- **Not Danışmanı Hizmeti:** Kredibilitenin nasıl daha iyi yönetileceğine ve kredi notunun yükselmesine yardımcı olmaktadır.
- **Takipçi Hizmeti**: Kimlik, iletişim ve finansal bilgilerin internetteki güvenliğinden sorumludur (bkz. https://www.findeks.com/findeks-hakkinda, 2018).

- Kurumsal üyelik işlemlerinde ise kredi kayıt şirketine başvurabilecekler; bankalar, faktoring, leasing, sigorta şirketleri, varlık yönetim şirketleri, tüketici finansman şirketleri ve diğer kurumlardır(bkz. https://www.kkb.com.tr/uyelik, 2018). İnternet adresi üzerinden üyelik koşuluyla kredi kayıt bürosunun, finans sektörü ve reel sektöre yönelik tüm ürün ve hizmetlerinden faydalanılabilmektedir.
- Banka ve kredi şirketlerinden hizmet alan kişiler, hesap hareketleriyle ilgili herhangi bir değişiklik yapılmasına, kendisi dışında kimsenin yetkili olmadığını, kurumlara bildirmelidir. Gerekirse tüm hesaplar için ayrıca özel talimatlar verilmeli ve yapılan tüm değişiklikler için bilgilendirme istenmelidir.
- Çevrimiçi bankacılık işlemleri ve diğer tüm önemli işlemler için günlük kullanımda olmayan özel bir bilgisayar kullanılmalıdır. İnternette gezinmek, oyun oynamak, sosyal medya kullanımı gibi günlük aktiviteler için farklı bir bilgisayar kullanılmalıdır. Bu uygulama, virüslerin bilgisayarda toplanmasını engelleyeceğinden daha güvenli bir siber ortam oluşmasına katkı sağlayacaktır.
- Şüpheli bir durumla karşılaşıldığında tüm şifreler hemen değiştirilmeli, kredi raporu kontrol edilmeli ve tüm olaylar belgelenmelidir. Ayrıca bilgisayar, bir teknoloji uzmanına kontrol ettirilmelidir. Bir siber saldırganla karşı karşıya kalındığı düşünüldüğünde, mümkün olduğunca hızlı hareket edilmelidir. Çünkü hız, siber saldırganın manevra yeteneğini kırmaktadır.
- Çevrimiçi yazışmalarda çoğunlukla iş adresleri kullanılmalı, gerekmedikçe ev adresleri yayınlanmamalıdır. Ayrıca çevrimiçi yazışmalarda takma isim kullanılması, kişiyi ve çevresini olası saldırılara karşı koruyacaktır.
- Kişiye özel bir blog veya web sitesinin bulunması durumunda, siteye yorum yapılabilmesi için ziyaretçilerin siteye kaydolması zorunlu kılınmalıdır. Ya da siteye yorum yapanların, IP adreslerinin takip edilebileceği izleme seçeneği etkinleştirilmelidir. Bloglar ve web siteleri çoğunlukla spam'ları filtreleyecek

ayarlara sahiptir. Bu sebeple kabul edilebilecek gönderiler için mutlaka bir site yönetim politikası oluşturulmalıdır. Örneğin; bir başkası tarafından yapılan yorumlar bir onay sürecinden geçirilmeli, yorum okunduktan sonra siteye aktarılmasına izin verilmelidir. Ayrıca tüm yorumlar düzenli olarak okunarak kontrol edilmelidir. Bununla birlikte sitenin kontrol panellerinin ve web sayaçlarının kullanılması, siteyi kimlerin görüntülediğinin belirlenmesine imkân sağlamaktadır. (Moore ve Edvards, 2014: 160-166).

- Ulusal Siber Olaylara Müdahale Merkezi olan USOM'un ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditlerle ilgili kendisine ulaştırılan ihbarları değerlendirerek söz konusu tehditlerin tespit ve bertaraf edilmesi için Kamu Kurumları ve özel kişilerle koordinasyonu sağlamaktadır. Ayrıca siber saldırılara karşı farkındalığın artırılmasına yönelik bilinçlendirme faaliyetleri bulunmaktadır. (https://www.usom.gov.tr/index.html bkz, 2018).
- Parola kullanmanın önemi ve parola oluşturmanın kriterleri iyi bilinmelidir. Saldırganların, kolay parolaları çok kısa sürede kıracağı unutulmamalıdır. Güvensiz ortak ağlarda (internet kafe vb.) kişisel işlem riskli olduğundan parola kullanılmamalıdır. Parola kimseyle paylaşılmamalı ve periyodik olarak değiştirilmelidir. Tüm hesaplar için farklı parolalar kullanılmalı, parola hatırlatma soruları ve cevapları tahmin edilmesi zor olacak şekilde seçilmelidir.
- Bilgi Teknolojileri ve İletişim Kurumunun (BTK) tüketicilere yönelik eğitici ve bilgilendirici içerikleri takip edilmelidir. Kurumun Güvenli Web sayfasında, internetin bilinçli kullanımına yönelik birçok içerik mevcuttur (http://www.guvenliweb.org.tr/, 2018) adresinden içeriklere ulaşılabilir. Ayrıca sitede çocuklara yönelik eğitici ve bilgilendirici içerikler mevcuttur. (http://www.guvenlicocuk.org.tr/, 2018) adresinden içeriklere ulaşılabilir. Bilgi güvenliğine ilişkin güncel gelişmeler BTK (Bilgi Teknolojileri ve İletişim Kurumu) aracılığıyla takip edilmelidir.
- İnternetten uygulama indirilirken; indirilme sayısı, kullanıcı yorumları ve kaynak mutlaka incelenmelidir. Ayrıca mobil cihazlara yönelik zararlı yazılımların takip edilmesi, kullanıcıları koruyan bir diğer etkili faktördür.
- E-postalarda yer alan linklerin ve dokümanların, zararlı yazılım barındırabileceği bilinmelidir. E-posta adresleri herkesin ulaşabileceği bir şekilde paylaşılmamalı, E-posta eklerinin uzantıları kontrol edilmeli, kaynağı belli olmayan E-postalar

açılmamalıdır. Kritik bilgiler E-posta ile açık olarak gönderilmemeli bu tür paylaşımlarda mutlaka şifreleme yöntemi kullanılmalıdır. İndirilen dosyalar güvenlik uygulamaları ile taratılmadan indirilmemelidir.

- Güvenlik uygulamaları (Antivirüs, paket izleme) kullanılmalı ve bu uygulamalar düzenli olarak güncellenmelidir.
- Bilgisayar işletim sistemi güncel tutulmalı ve parola korumalı ekran koruyucusu kullanılmalıdır. Bilgisayar başından ayrıldığında ekran kilitlenmelidir. Bilgisayarların şifre kaydetme özellikleri kullanılmamalıdır.
- Lisanssız uygulamaların riskli olduğu bilinmeli, ücretsiz uygulamalara karşı tedbirli davranılmalı, güvenli internet paketleri tercih edilmelidir.
- Web ortamına yüklenen fotoğraf, doküman vb. araçlarla birlikte sosyal medya paylaşımları üzerinden konum bilgisine erişilebileceği bilinmelidir.
- Web sayfalarının TLS, SSL gibi şifreli iletişim sertifikalarına sahip olup olmadığının nasıl kontrol edileceği bilinmelidir. SSL Sertifikası olan yani (https://) ile çalışan sitelerde, internet tarayıcısının alan adının yazılı olduğu yerde "GÜVENLİ" ibaresi bulunmaktadır. SSL Sertifikası olmayan siteler için ise "Bu Site Güvenli Değil" veya "Korumasız Bağlantı" gibi ibareler bulunur. Bu ibareler Google arama motorunda ziyaretçilere gösterilmektedir. Google SSL Sertifikası olan sitelere arama sıralamalarında öncelik vermektedir. SSL Sertifikası olmayan siteler ise Google Arama Motorunda yapılan arama sıralamalarında geriye düşmektedir (https://www.globalnet.com.tr, 2019).
- Kişisel bilgisayarlar el değiştirdiğinde eski bilgisayarda bulunan sabit disk imha edilmeli ya da güvenli silme işlemlerinden geçirilmelidir.
- Veri taşıma araçları (USB, CD, DVD vb.) Zararlı yazılımlara karşı taratmadan kullanılmamalı, internet tarayıcısına ilişkin güncellemeler yapılmalıdır.
- Modem şifreleri belirli aralıklarla değiştirilmeli, modem ayarlarında güvenli şifreleme yöntemleri seçilmelidir. Bilgisayar ve cep telefonları kullanılmadığı zamanlarda modem kapatılmalıdır.
- İnternetten alışveriş yaparken 3D secure gibi güvenilir yöntemler kullanılarak satın alma işlemlerinde, sanal kart kullanılmalıdır. Güvenli şifreleme yöntemini kullanmayan e-ticaret sitelerinden alışveriş yapılmamalı ve telefonda kredi kartı bilgileri kimseye verilmemelidir (Erol, 2016: 87-93).

- Web sayfalarına kredi kartı bilgileri kaydedilmemeli, şüphelenilen web sayfaları için Whois bilgisi mutlaka kontrol edilmelidir. (https://www.whois.net/, 2018) Özellikle online alışverişte whois bilgisinin sorgulanması sitenin kayıt altında olup olmadığının belirlenmesinde ve ticari bilgilere erişimde büyük kolaylık sağlamaktadır. Bir web sitesi herhangi bir adres bilgisi ve telefon numarası göstermez ise kesinlikle şüpheli yaklaşılmalıdır.
- Cep telefonlarına sadece gerekli olan uygulamalar yüklenmeli, uygulamaların içerikleri ile izin isteklerinin uygunluğu ve kapsamı kontrol edilmeli, telefonların çalınması ya da kaybolması durumunda, BTK aracılığıyla e-Devlet üzerinden (https://www.turkiye.gov.tr/, 2018) telefonun kullanıma kapatılması sağlanmalıdır. Ayrıca telefonlarda ekran kilidi, tuş kilidi, sim kilidi, otomatik ekran kilidi vb. güvenlik önlemleri kullanılmalıdır.
- Tarayıcı adres çubuğundaki URL bağlantısı kontrol edilmeli, adres çubuğundaki yazım hataları ve beklenmeyen isimlere dikkat edilmelidir. Herhangi bir kişisel ya da finansal bilgi verilmeden önce sitenin güvenli bir bağlantıda olup olmadığı "https" adresi için de bulunan 's' ve asma kilit sembolü ile mutlaka kontrol edilmelidir.
- İstenmeyen reklamlardan ve tekliflerden şüphelenilmelidir. Bu nedenle spam filtreleri açık tutulmalıdır. Şüpheli spamlar silinerek eklerinin açılamamasına dikkat edilmelidir. (https://www.interpol.int, 2018) Ücretsiz virüs taramalarından bazıları şu adreslerden temin edilebilmektedir.

Kaspersky: (https://www.kaspersky.com/free-virus-scan, 2018)

Trend Micro: (https://www.trendmicro.com/, 2018)

- Kullanıcılar, interneti daha bilinçli, güvende ve etkin kullanabilmek için İnternet Yardım Merkezinden destek alabilmektedir(https://www.internetyardim.org.tr/, 2018 bkz.)
- Kişisel verilerin korunmasına yönelik kanunlar takip edilmeli ve herhangi bir saldırı esnasın da ihbar da bulunulacak kurumlar iyi bilinmelidir. İhbar edilecek adresler aşağıdaki gibidir.

1. USOM'a yapılacak ihbarlar için (https://www.usom.gov.tr/ihbar-bildir.html, 2018)
2. BTK' ya ihbar edilecek zararlı içerikler için (https://www.ihbarweb.org.tr/, 2019)

3. Emniyet Genel Müdürlüğüne ihbar için https://www.egm.gov.tr/sayfalar/ihbar.aspx , 2019) bağlantıları kullanılmalıdır
4. Kişisel verilerin çalınması durumunda ihbar için ALO 198 numaralı Veri Koruma Hattı ile iletişime geçilmelidir.

8.1. Akıllı Telefonlardan Kaynaklanan Güvenlik Riskleri

Dünyada dijital teknolojilerin gelişimine paralel olarak ülkemizde de akıllı telefon kullanımında ciddi miktarda artış kaydedilmiştir. Teknolojinin hayatımıza kazandırmış olduğu avantajlar, beraberinde birtakım risklere de neden olmuştur. Bu noktada her geçen gün artan mobil güvenlik tehditlerine karşı tüketicilerin bilinçlendirilmesi ve birtakım tedbirleri almaya sevk edilmesi büyük öneme sahiptir.

8.2. İşletim Sisteminden Kaynaklanan Güvenlik Riskleri

Akıllı telefonlarda risklerin başında işletim sisteminden kaynaklanan sorunlar gelmektedir. Bu noktada kullanıcıların alabileceği önlemler yok denecek kadar az, güvenlik riskinden etkilenen kullanıcı sayısı ise sanılandan çok fazladır. Risk grubuna örnek olarak Carrier IQ programı verilebilir. Android, Blackberry, İOS ve Symbian işletim sistemlerine sahip telefonlarda, genellikle telefona yüklenmiş olarak satın alınan bir programdır. Bu programın, kullanıcı verilerini kendi merkezine gönderdiği bilinmektedir. Carrier IQ uygulaması telefonların en alt seviyesinde telefonlar da anlaşılmayacak şekilde yüklü olarak bulunmaktadır. Çalışmaya başladığından itibaren kullanıcıya herhangi bir uyarıda bulunmaz. Ayrıca uygulamanın kullanıcı tarafından bulunması ve kaldırılması da mümkün değildir. Telefona yüklenmiş olarak gelen ve kaldırılamayan uygulamanın çalışma mantığı, kullanıcı tarafından yapılan tüm işlemlerin yakalanıp kayıt edilmesidir. Kullanıcının bulunduğu yerden, internette kullandığı şifrelere, telefon rehberinden, gönderdiği mesajların içeriğine kadar tüm bilgiler uygulama tarafından kayıt altına alınmaktadır. Carrier IQ Firması bu iddiaları yalanlamış olsa da kayıtlar kullanıcı bilgilerinin eşsiz bir kod ile tutulduğunu göstermektedir. İşletim sistemi risklerinden bir diğeri de değiştirilmiş işletim sistemlerinin kullanılmasıdır. Burada tüm sorumluluk işletim sisteminin kodlarını değiştiren kişilerin inisiyatifinde olmaktadır. Custom ROM ve Jailbreak gibi işletim sistemleri, içeriği farklı kullanıcılar tarafından değiştirilmiş işletim sistemleridir. Dünyanın herhangi bir yerindeki yazılımcı tarafından tasarlanarak geliştirilmiş işletim sistemleri çok büyük riskleri de beraberinde

getirmektedir. Android Custom ROM'lardan en popüler olanları CyanogenMod ve Jailbreaktır. Bu kullanıcılar, akıllı telefonlarının işletim sistemlerinin kontrolünü cihaz üreticilerine değil tamamen başkalarının eline bırakmış kullanıcılardır (https://bid.usak.edu.tr 2014: 8-10).

8.3. Uygulama Yetkilerinden Kaynaklı Güvenlik Riskleri

Akıllı telefonlarda bulunan risklerden bir başkası uygulamalardan kaynaklanan risklerdir. Yapılan araştırmalar iOS ve Android uygulamalarının nerdeyse yarısının fonksiyonlarını yerine getirirken kullanıcı bilgilerini alıp bunları kendi veri merkezlerine gönderdiğini göstermektedir. Kullanıcılara ait bilgiler reklam şirketlerine ya da bu bilgileri talep eden firmalara belirli ücretler karşılığında satılmaktadır. Uygulama telefona yüklenmeden önce kullanıcı tarafından birtakım izinler istemektedir. Bu izinler neticesinde; rehber bilgilerine ulaşma, internette ziyaret edilen sitelerin konum bilgisine ulaşma, çağrı, ses, video vb. kullanıcıya ait birçok kişisel bilgi ve kişisel veriler, uygulamalar tarafından ele geçirilmektedir. Android, dünya üzerinden en çok kullanılan mobil işletim sistemidir. Anroid'in resmi uygulama marketi olan Play Store'a her gün binlerce yeni uygulama yüklemektedir. Bu durum Android kötücül yazılım geliştirenlerin ekmeğine yağ sürmektedir. Çünkü yapılan araştırmalar mobil tabanlı saldırıların %99'unun Android tabanlı olduğunu ispatlamaktadır (Kabakuş, Doğru ve Çetin 2015: 15). İOS için uygulama marketi olan "Apple Store"de uygulamaların kontrolü daha sıkı gerçekleştiğinden bu markette riskli uygulamaların bulunma ihtimalinin daha düşük olduğu belirtilmektedir. Fakat yine de kullanıcılara yükleyecekleri uygulamalarda daha dikkatli davranmaları önerilmektedir.(https://bid.usak.edu.tr , 2014: 10-12)

8.4. Casus Yazılımlardan Kaynaklanan Güvenlik Riskleri

Akıllı telefonlarda bulunan en büyük güvenlik risklerinden bir diğeri casus yazılımlı uygulamalardır. En önemli özellikleri telefonda yüklü olup olmadıklarının anlaşılamamasıdır. Ayrıca bu uygulamaların kaldırılması da mümkün değildir. Casus yazılımların amacı kullanıcıya ait tüm bilgilerin bir merkezde toplanarak talep eden kullanıcıya online gönderilmesidir. Casus yazılım reklamlarının yapıldığı internet sayfalarında "Çocuklarınızın güvenliği için onları takip edin! Telefonunuzun çalınması halinde verilerinizi ve telefonunuzu takip edin! Çalışanlarınızın iş telefonlarını takip edin! vb." ifadelerle casus yazılım pazarı genişletilmeye

çalışılmaktadır. Casus yazılımlar ile yapılabilecek işlemler Tablo 4 ile gösterilmektedir.

Tablo 4: Casus Yazılımların İşlevleri

NO	İŞLEV	TANIM
1.	**Ortam Dinlemesi Yapılması**	Kullanıcının haberi olmadan telefonun mikrofonundan dinleme yapılarak seslerin kaydedilmesi.
2.	**Gizli Kamera Kullanımı**	Kullanıcının haberi olmadan bulunulan ortamın, gizlice fotoğraflarının çekilip hedefe yönlendirilmesi.
3.	**Arama Bilgileri**	Kullanıcının coğrafi takibi ve anlık konum bilgilerinin kayıt altına alınması.
4.	**Konum Bilgileri**	Bulunulan coğrafi ortamın ve bulunulan konumun sürekli takibi.
5.	**Kısa Mesaj Takibi**	Telefona gelen ve telefondan gönderilen mesajların takibi.
6.	**İnternet Bağlantı Bilgileri**	Tüm internet adreslerinin kullanıcı adı ve şifreleriyle takibi.
7.	**Dosya Bilgileri**	Telefonda bulunan video, fotoğraf gibi tüm dosyaların hedefe yönlendirilmesi.
8.	**Sosyal Medya Takibi**	Tüm yazışma ve paylaşılan bilgilerin takibi. E-posta dâhil.
9.	**Uygulama Bilgileri**	Telefona yüklenen tüm uygulamaların takibi veya engellenmesi.
10.	**Rehber ve Takvim Bilgileri**	Telefon rehberine yeni kayıtların takibi. Telefon takviminde bulunan önemli tarihlerin takibi.
11.	**Kısa Mesaj ile Kontrol**	Telefonu kilitleme, kilidi açma vb. işlemlerde kısa mesaj ile telefonun kontrolünün ele geçirilmesi.
12.	**Uzaktan Program Kaldırma**	Casus yazılım ihtiyacının ortadan kalkması durumunda uzak mesafeden telefondaki uygulamanın kaldırılması.

Kaynak: Bilgi Teknolojileri ve İletişimi Kurumu, Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT) Akıllı Telefonlarda Güvenlik, Yararlanarak Hazırlanmıştır. 2014: 14-15 https://bid.usak.edu.tr/

Casus yazılımların özellikle çocukları ve gençleri olumsuz etkilediği bilinir. Çocuklar ve gençler bilgisayarlarda ve internet üzerinde gezinirken kendilerine ve ailelerine verecekleri zararları düşünmemektedirler. Örneğin; indirilen bir oyun programında, casus yazılımlar gibi kötücül yazılımlar bilgisayarlara bulaşabilmektedir. İnternet üzerinde çocukların dikkatini çekebilecek yöntemlerle bulaşan bu tür zararlı yazılımlar, çeşitli tekniklerle kullanıcılara ve bilgisayarlara zarar verir. Bu noktada çocuklar ve gençler internet kullanırken çeşitli risk ve güvenlik tehditleriyle karşı karşıya kalmaktadırlar. Konu göz ardı edilemeyecek kadar önemlidir. Bu noktada çocukların aşırı bilgisayar kullanımlarının önüne geçilmesi üzerinde durulması gereken en önemli konudur. Bir ebeveyn ya da eğitimcinin görevi çocuğa sadece bilgisayar ve internet ortamına erişimi tanıtmak değildir. Çocuklar ev dışında nasıl başıboş bırakılmıyorsa internet ortamında da başıboş bırakılmamalı, oluşabilecek tehditlere karşı gerekli tüm tedbirler alınmalıdır (Canbek ve Sağıroğlu, 2007: 33-34).

8.5. Tüketiciler için Akıllı Telefon Güvenlik İpuçları (Andorid - Apple IOS - Blackberry – Windows Phone):

Kullanıcıların günlük hayatlarında önemli bir yer tutan akıllı telefonlar, birçok güvenlik riski barındırmaktadır. Bir kaç basit tedbirle bu risklerin azaltılması mümkündür. Tablo 5 ile alınabilecek güvenlik tedbirleri anlatılmaktadır.

Tablo 5: Tüketiciler için Akıllı Telefon Güvenlik İpuçları (Android-Apple IOS-Blackberry- Windows Phone)

NO	İPUCU	AÇIKLAMA
1.	**Ekran Koruyucu Şifre:**	Telefonun çalınması ya da kaybolması durumunda telefonun kullanımını engellemek için, şifre/PİN/ekran koruması yapılmalıdır.
2.	**Cihazın Temel Güvenlik Ayarları:**	Güvenlik ayarlarında değişiklik yapılmaması önerilmektedir. Telefonun fabrika ayarları değiştirildiğinde (rooting, jailbreak vb. işlemler) akıllı telefonlarda sunulan güvenlik özelliklerini zayıflatmaktadır.
3.	**Telefonun Yedeklenmesi ve Veri Güvenliği:**	Telefonda saklanan tüm verilerin (belgeler, rehber, fotoğraf vb.) yedeklenmesi tavsiye edilmektedir. Kişisel bilgisayarlarda, bulut ortamında veya harici depolama aygıtlarında saklanabilmektedir.
4.	**Uygulamaların Erişim Yetkilerinin Kontrolü:**	Akıllı telefonlarda bulunan ya da indirilen uygulamaların kişisel bilgilere erişim izni ve yetkisi hususunda çok dikkatli olunmalıdır.
5.	**Güvenilir Kaynaklardan Uygulama Yüklenmesi:**	Bir uygula indirilmeden önce yasal ve güvenilir olduğundan emin olunmalı ve mutlaka araştırma yapılmalıdır. Ayrıca indirilen uygulamaların işletim sisteminin resmi uygulama ortamından edinilmesi çok önemlidir.
6.	**Açık Wi-Fi Bağlantıları:**	Herkese açık, şifresiz ağ hizmetini bedava veren kişi tarafından, ortam dinlenebilmektedir. Bu sebeple halka açık ağ kullanımı yerine, güvenilir operatörlere ait güvenli bir Wi-Fi kullanılmalı veya kablosuz mobil bağlantı tercih edilmelidir.
7.	**Uzaktan Erişim ile Silmeyi Etkinleştirecek Güvenlik Uygulamaları:**	Akıllı telefonlarda uygulama olarak kullanılabilecek ya da varsayılan olarak kullanılan en önemli güvenlik özelliğidir. Telefonun GPS'si (konum bilgisi sağlayıcısı) kapalı dahi olsa telefondaki tüm verilere uzaktan erişebilme ve veri silme imkânı sağlamaktadır. Bu tür uygulamalar ayrıca telefon kaybedildiğinde, telefonun kolay bulunmasına yardımcı olmaktadır.
8.	**Telefon Verilerinin Silinmesi:**	Telefon satılmak istendiğinde kişisel veriler (mesajlar, fotoğraflar, uygulamalar, arama geçmişi vb.) mutlaka silinmeli ve fabrika ayarları sıfırlanmalıdır.
9.	**Çalınan Telefonun Bildirilmesi:**	Telefon kaybolduğunda veya çalındığında hattın kapanması için ilgili işletmeye başvurulmalıdır. Ayrıca ülkemizde Bilgi Teknolojileri İletişimi Kurumu, konuyla ilgili yetkili kurumdur. www.btk.gov.tr adresinden konu yetkililere iletilebilir.
10.	**Uygulama Marketinde Kredi Kartı Kullanımı:**	Yalnızca ücretsiz uygulamalar kullanılıyorsa, telefonun uygulama marketinde kullanıcı bilgisi oluşturulurken talep dahi edilse kredi kartı bilgileri girilmemelidir. Uygulama satın alındığı durumlarda düşük limitli sanal kartlar kullanılmalı ayrıca kredi kartı ekstresi takip edilmelidir.
11.	**Telefondaki Verilerin Şifrelenmesi:**	Telefonun veri şifreleme özelliği varsa mutlaka kullanılmalıdır. Bu özellik yoksa veri şifreleyen uygulamaların kullanılması tavsiye edilmektedir. Telefonun çalınması veya kaybolması durumunda veriler ilgili şahıs tarafından kullanılamayacaktır.
12.	**Akıllı Telefon Güvenliği (ANDROID):**	Detaylı bilgi için bakınız. https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-android.pdf .
13.	**Akıllı Telefon Güvenliği (IOS):**	Detaylı bilgi için bakınız. https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-ios.pdf
14.	**Akıllı Telefon Güvenliği (BLACKBERRY):**	Detaylı bilgi için bakınız. https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-bbery.pdf

NO	İPUCU	AÇIKLAMA
15.	**Akıllı Telefon Güvenliği (WINDOWS PHONE):**	Detaylı bilgi için bakınız. https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-wind.pdf

Kaynak: Bilgi Teknolojileri ve İletişimi Kurumu, Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT) Akıllı Telefonlarda Güvenlik, Yararlanarak Hazırlanmıştır. 2014: 16-18 (https://bid.usak.edu.tr/, 2018)

8.6. Kurum ve Kuruluşlar Siber Saldırı Kurbanı Olmamak için Ne Yapmalıdır?

Kurumda münferit olarak görülebilecek birbirleriyle ilgili olmayan siber saldırılarda son zamanlarda bir artış varsa bu durum önemsenmelidir. Birbiri ile bağlantılı görünmeyen ve kritik seviyesi düşük olarak tanımlanan siber saldırılar, organize bir siber saldırının ilk aşaması olabilmektedir. Bu sebeple küçük çapta olan tüm saldırılar dahi dikkate alınmalıdır. Kurumdaki bilişim sistemi bileşenlerinin normal zamanlardaki kullanım ve performans durumları izlenmelidir. Ağ trafiğindeki normal olmayan bir artışın ya da sunucu sistemlerindeki beklenmedik performans değişimlerinin sebepleri araştırılmalıdır. Çünkü bu değişimlerin sebebi bir siber saldırı ön hazırlığının bilgi toplama faaliyetleri olarak değerlendirilebilmektedir. Kurum bilişim sistemlerinde, kaydı alınması mümkün olan tüm bileşenler merkezi bir kayıt yönetimi yazılımı üzerinde kaydedilmelidir. Bu yazılımın kayıt ilişkilendirme özelliği varsa sistemlerin tüm çalışma rutininin dışına çıkan tüm olaylar için ilişkilendirme kuralları oluşturulmalı ve bir siber saldırı esnasında ilgili personele otomatik uyarı mesajları iletilmelidir.

İşletim sisteminin donanım, yazılım, uygulama gibi ürünlerde üreticiler tarafından yayımlanmış en güncel güvenlik yama ve güncellemelere sahip olduğu kontrol edilmelidir. Kurumda kritik bilişim sistemi bileşenleri belirli periyotlarda yedeklenmeli, yedekli çalışma kontrol testleri yapılmalı ve veri yedeklerinden geri dönüş tatbikatları gerçekleştirilmelidir. Siber saldırı istihbaratı alındığı durumlarda bilişim sistemleri erişim parolaları yenilenmeli, güçlü ve tahmin edilemeyecek parolalar belirlenmeli, yönetim araçlarında parolaları kriptolama teknikleri kullanılmalıdır. Kurumdan ayrılan kişilerin sisteme erişim hesapları ivedilikle engellenmelidir. Kurumda güncellenmeyen, güvenlik kontrollerinden geçirilmeyen sistemler kullanılmamalıdır. Kurumların büyük çoğunluğu hizmet dışı bırakma saldırılarına uğrar. Kurumda hizmet dışı bırakma saldırılarını engelleme teknolojileri

kullanılmalı, özellikle siber saldırı istihbaratı alındığı zamanlarda sistemler izleme kipinden sürekli koruma kipine getirilmelidir.

Son olarak; siber saldırı öncesi saldırı anı ve saldırı sonrasında kurum personelinin görev ve sorumluluklarını anlatan acil durum iletişim planları hazırlanmalı USOM (Ulusal Siber Olaylara Müdahale Merkezi), Sektörel SOME (Siber Olaylara Müdahale Ekipleri) ve güvenilir siber güvenlik bilgi kaynaklarından gelen bilgilendirme ve öneriler dikkate alınarak siber saldırılara karşı hazırlıklı olunmalıdır (http://www.havelsan.com.tr, 2018) Ancak alınan tüm tedbirlere rağmen özellikle çokuluslu şirketlere karşı gerçekleştirilen saldırıların tespit edilmesi zor olabilmektedir.

Ayrıca kurumsal siber tehditlerin başka bir unsuru insandır ve insan konusunun sadece teknik yaklaşımlarla ele alınması bazı saldırılar için doğru bir tespit değildir. Bu tehdit türü içsel tehdit olarak adlandırılır. Kurum içerisinde çalışan bir siber fail, örgütün bir parçasıdır ve bu durumdan yararlanarak kurumun kendisine olan güvenini kötüye kullanabilmektedir. İçeriden gelen tehditler konusunda çok az şey bilinir. Çünkü içeriden gelen tehditlerin kamuoyunda bilinmesi şirket itibarı için utanç vericidir. Bu sebeple içeriden gelen tehditler üzerinde çok az geçerli ölçüm ve raporlama bulunmaktadır. Bu tür saldırılara karşı durabilmek için kurum içerisinde, içeriden alınan saldırı ifadesi mutlaka tanımlanarak güvenlik uzmanlarına ve ilgili profesyonellere iletilmelidir. Ayrıca konu hakkındaki bilgi alışverişi, kamuoyu dışında yapılmalıdır. İçeriden gelen tehditlerin güvenilir bir şekilde ölçülebilmesi için elde edilen veriler, güvenlik araştırması topluluğunda toplanmalı ve paylaşılmalıdır.

Özetle endüstriler ile güvenlik araştırmacıları arasında işbirliği gereklidir. Çünkü içeriden gelen tehditleri tespit etmek veya engellemek için teknik kontroller geliştirmek zordur. Bu sebeple içeriden yasal erişim kullanılmaktadır. Fakat bu noktada da erişimin sınırlandırılması gibi tedbirler kötü niyetli çalışanlar üzerinde olumsuz etki bırakabilmektedir. Bu sebeple endüstrilerin içeriden saldırıya uğradığı vakaları ancak güvenlik araştırmacılarının analiz etme yetkinliği bulunmaktadır (Salvatore J.Stolfo ve diğerleri, 2008: 10-15).

ÜÇÜNCÜ BÖLÜM

DİJİTAL VATANDAŞLIK VE ONLİNE ALIŞVERİŞ

1. DİJİTAL VATANDAŞLIK KAVRAMI VE AVRUPA İLE ABD'DE DİJİTALLEŞME ÇALIŞMALARI

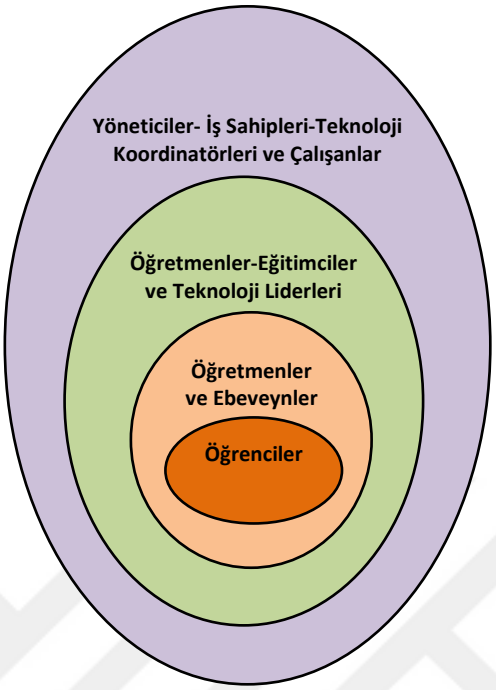
Popüler basında giderek yaygınlaşan dijital vatandaşlık kavramı, teknolojinin yanlış kullanımı ya da kötüye kullanımının artmasıyla beraber; makaleler, yazılı ve görsel basındaki metinler ve haberler ile adından sıkça bahsedilen bir kavram olmuştur. Dijital vatandaşlıkta amaç toplumun ve toplumu oluşturan bireylerin yenidünya düzeninde gelişen teknolojiye uygun davranış modeli kazanmasıdır. Dijital teknolojilere uygun davranış modellerinin geliştirilmesi çağımızda toplumun bütünlüğü için bir önceliktir. Kısa bir anlatımla dijital vatandaşlık kavramı, hayatımıza giren dijital araçları doğru kullanmasını bilen, kişi haklarına online platformlarda saygı duyan ve bu platformlarda sorumluluk ve güvenlik bilincine uygun hareket eden vatandaşlar olarak tanımlanmaktadır. Dijital vatandaşlık kavramı temelinde dokuz kavramı barındırır. Bu kavramlar; dijital erişim, dijital ticaret, dijital iletişim, dijital okuryazarlık, sayısal görgü kuralları (dijital teknoloji tarafından beklenen uygun davranış standartları), sayısal hukuk (teknolojiyi yönetenlerin yasal hak ve kısıtlamaları), dijital hak ve sorumluluklar, dijital sağlık ve dijital güvenlik olarak tanımlanmaktadır (Ribble ve Bailey, 2007: 9-10).

Dijital erişim ve dijital güvenlik kavramlarına yaklaşım ülkeler açısından farklılık göstermektedir. Örneğin 2010 yılında Almanya'nın Berlin kentinde 250.000'den fazla Alman vatandaşı Google Street'in tanıtımına karşı çıkmıştır. Google'dan evlerinin resimlerinin görüntülenmesini istemeyen vatandaşlar, konuyu gizlilik sorunu olarak değerlendirmiş ve kamuoyunu kullanarak bu uygulamanın kısıtlanmasını talep etmişlerdir (Delgado,2016: 18). Bu bağlamda dijital vatandaşlık kavramı, geniş kapsamlı politik katılım çalışmalarıyla birlikte ortaya çıkan sosyal hareketleri de teşvik etmektedir. Politik katılımı canlandıran çağdaş dijital

kampanyalar ile birlikte bu katılımı canlandırmak için kullanılan e-dilekçeler, sosyal medya paylaşımları, yazılı ve görsel medyada bilimsel tartışma vb. programlara dijital sistemlerden erişim, bireysel ve kültürel düzeyde toplumlarda dijital katılımı günden güne geliştirmektedir. Dijital katılımı harekete geçirebilmek için konuyla ilgili hikâye alıcısının duygusal olarak ele geçirilmesi önemliyken, dayanışma oluşturulması için konuyla ilgili paylaşılan bilginin birlik ve beraberlik duygusu içerisinde oluşturulması önemlidir. Çözümlemek için ise teknik iknadan ziyade ahlâki bir aciliyet ve sorun yaratılarak sosyal değişimi en hızlı şekilde sağlamak dijital bir kampanyanın başarılı sayılması için gerekli olan ana faktörlerdir (Vromen, 2017: 225-227). Dijital dünyada çevrimiçi ağlarda, çevrimiçi haberlerden bilgi edinmede kitlesel seçim insanların bilgi düzeylerini analiz etmede önemli bir etkendir. Örneğin haber sektörü ve çevrimiçi haber tüketim süreçleri değerlendirildiğinde insanların politika hakkında ne bildikleri ve ne hissettikleri, toplumsal düzeyde patlama ve toplumsal parçalanma süreçlerinde politik ve sosyal grupların birbirleriyle etkileşiminde önemli bir role sahiptir. Bu değerlendirmeler altında dijital ortamlarda toplumsal parçalanmanın ve kutuplaşmanın nasıl yaratıldığı derinlemesine analiz edilebilmektedir (Tewksburg ve Rittenberg, 2012: 119).

Paylaşılan tüm bilgiler ışığında; dijital vatandaşlık konusu başta yöneticiler, teknoloji liderleri, öğretmenler ve öğrenciler tarafından dikkatle takip edilmeli ve önemsenmelidir. Dolayısıyla bu kişilerin öncelikli olarak bilinçlendirilmesi ve eğitilmesi ilk hedef olmalıdır. Dijital teknolojilerin sürekli değişen doğası gereği bir sonraki teknolojinin ne olacağı ve nasıl kullanılacağı, yeni teknolojilerin öğretilmesi ve öğrenilmesiyle birlikte tüm topluma dijital vatandaşlık kavramını tanıtacaktır. Bu teknolojileri keşfetmek için öncelikli çerçeveye sahip olması gereken kişiler; eğitimciler ve öğrencileridir. Dijital vatandaşlık eğitimleri toplumunun tamamını ilgilendiren bir konudur. Velileri dijital vatandaşlık hakkında eğitmek, öğrencilerin tutarlı bir davranış modeli geliştirmesinde en iyi rol model olacaktır. Diğer taraftan dijital teknolojilerin uygun ve etkin kullanımı işletmeler ve endüstrilere büyük fayda sağlayacaktır. Eğitimcilerin konuya öncülük ve liderlik etmeleri, toplumda üretken dijital vatandaşları artıracak dolayısıyla ilerde oluşabilecek toplumsal ve ekonomik maliyetleri de engellemiş olacaktır. Dijital vatandaşlıkta ebeveynler kendi çocuklarının temel eğitimcileri olduklarından dijital vatandaşlığı anlama ve anlatmada temel çerçeve içine alınmıştır. Şekil 11 ile dijital vatandaşlığın

öğrenilmesi ve öğretilmesinde hedefte olan çerçeve kitle görselleştirilmiştir (Ribble ve Bailey, 2007: 129-130).



Şekil 11: Dijital Vatandaşlıkta Hedef Kitle

Kaynak: Ribble, M.; G. Bailey (2007). Digital Citizanship in Scholls, Washington, ABD, Book Publishing İste.Pp.130. Yararlanarak hazırlanmıştır.

Dijital vatandaşlığın gelişimiyle birlikte küçük yaşlardaki çocuklardan başlamak üzere yaratıcı düşünce, bilişim ve iletişim teknolojilerinde inovasyonun uluslararası düzeyde gerçekleşebilmesi için ISTE organizasyonu kurulmuştur. Bu organizasyon dünyanın dört bir yanında bulunan eğitimcilerin, eğitimdeki zor problemlerin üstesinden gelmelerine ve teknolojiyi en doğru şekilde kullanmalarına yardımcı olmaktadır (https://www.iste.org/, 2018 bakınız). Dijital vatandaşlık için oluşturulan en önemli standart ISTE (The International Society for Technology in Education- Uluslararası Eğitim Teknolojileri Derneği) organizasyonuna aittir. ISTE, dünyanın her noktasında üyesi olan ve ilköğretim çağlarından başlanmak üzere teknoloji kullanımını tüm öğrencilere kavratmayı hedefleyen ve bu kapsamda eğitim ve öğretim faaliyetlerinin geliştirilmesine yardımcı olan bir organizasyondur. Bu amaçla ISTE, eğitimde NETS (The National Educational Technology Standards) standartlarını oluşturmuştur. NETS standartları; öğretmenler, öğrenciler, yöneticiler, bilgisayar eğitimcileri ve eğitim koçları için ayrı ayrı hazırlanmaktadır. NETS özetle dijital çağımızda tüm öğretme ve öğrenme kabiliyetlerinin geliştirilmesi ve tüm

dünyada tanınması için oluşturulmuş standartlar kümesidir (Çubukçu, Bayzan, 2013: 159).

Avrupa'da dijitalleşme çalışmaları incelendiğinde; Avrupa Birliği, planlamasını yapmış olduğu tek dijital ağ geçidi (SDG) uygulaması için gerekli olan işlevsel teknik ve birlikte çalışılabilirlik gereksinimleri 2018 yılı nihai raporunda açıklamıştır. Rapordaki çıktılar genel olarak değerlendirildiğinde bilgi teknolojileri mimarisinde kaydedilen ilerlemenin adım adım değerlendirmeye alındığı görülmektedir. (bknz.https://ec.europa.eu/docsroom/documents/33287, 2019). Avrupa Birliği en geç 2023 sonuna kadar tüm AB'ye üye olan ülkelerde, herhangi bir fiziki evrak olmadan bir araba ya da bir emekli maaşı ödeneği almak gibi birçok prosedürü tek dijital ağ geçidi üzerinden, çevrimiçi erişimle yapmayı planlamaktadır. (bknz.http://ec.europa.eu/growth/single-market/single-digital-gateway_en, 2019).

Amerika Birleşik Devletleri ise dünyanın her yerinde mevcut olan güvenlik standartlarını dijitalleştirmek ve yaymak için uluslararası alanda kamuya açık olan Public.Resource.Org. ile Birleşik Devletler Federal Hükümetinin çalışmalarının dijital hale getirilmesini amaçlanmaktadır. Organizasyon tarafından yürütülen büyük projeler arasında ABD hükümetinin kendi çalışmaları için lisanslama kuralları çok sayıda mahkeme kaydının paylaşılması, ABD hükümetinin ürettiği video ve çeşitli yerlerin yasaları yer almaktadır (bknz. https://law.resource.org/, 2019). Bu çalışma ile öğrenmek ve içselleştirmek vatandaşlar açısından kolaylaşmaktadır. Ayrıca public.resource.org ile FedFlix izlenebilmekte, ulusal arşivler dahil olmak üzere diğer devlet kurumlarıyla işbirliği içinde Ulusal Teknik Bilgi Servisi (NTIS) ile ortak girişimde bulunulmaktadır. (bknz. https://public.resource.org/, 2019). Uluslararası düzeyde özellikle bireysel girişimcilik ve ekonomik faaliyetler içinde dijital süreçler işlemektedir. Bir proje ve girişimi desteklemek için çok sayıda insandan, az miktarda para toplanarak alternatif bir finansman kaynağı yaratan ve dijital kitle fonlaması olarak tanımlanan "crowdfunding" ile 2015 yılında dünya genelinde 34 milyar ABD dolarının üzerinde bir gelir artışı sağlanmıştır. (https://en.wikipedia.org/wiki/Crowdfunding, 2019).

2. SOSYAL AĞLAR VE SOSYAL MEDYA

Sosyal ağlar; kitlelerle iletişim ve bağlantı kurmak için sistemlerde bulunması zorunlu profillerin paylaşılmasına imkân sağlayan, bir bağlantıyı paylaşan kullanıcıyla diğer kullanıcıların birbirine eklenmesi ve sistemde kayıtlı olan her bir kişinin, birbirini görmesine olanak sağlayan web tabanlı servis olarak tanımlanmaktadır. Sosyal ağlar sosyal medyanın ilgi çekerek ön plana çıkmasına sebep olur. Farklı içeriklere sahip olan ağlar, insanların saatlerce sanal ortamlarda vakit geçirmesine de ortam hazırlamaktadır. Yapılan bir araştırma da öğrencilerin %85,9'unun sosyal ağ kullanıcısı olduğu tespit edilmiştir (Vural, Bat: 2010: 3355,3371). Bugün dünyada 3 milyar 191 bin kişi sosyal medya kullanmaktadır. (https://www.sabah.com.tr, 2018). Küresel internet raporunun 2018 yılı Ekim ayı verilerine göre Türkiye'nin sosyal medya karnesi açıklanmıştır. Açıklanan raporda ülkemizdeki Facebook kullanıcı sayısının 43 milyon, Instagram kullanıcı sayısının 37 milyon, Twitter ve Snapchat kullanıcı sayısının 9 milyona yaklaştığı görülmektedir.(https://www.sabah.com.tr 2018). Günümüzde en iyi sosyal ağlardan biri olan Facebook, e-posta gönderme, anında mesajlaşma, müzik, video ve fotoğraf paylaşma hizmetlerinin yanında 300.000 den fazla uygulamaya erişim imkânı sağlamaktadır. Ayrıca kullanıcılar Facebook sitesinden ayrılmadan Amazon'dan alışveriş yapabilmekte kullandıkları diğer sosyal ağlar ve paylaşım siteleriyle bağlantı sağlayabilmektedirler (örneğin, Twitter ve Instagram arası bağlantı vb.).

Sosyal ağlarda gezinen dijital insanların, farklı bilgi gereksinimlerini karşılamak için ağlarda bilgi yöneticileri bulunur. Bu kişilere bilgi profesyonelleri denilmektedir (gerçek ya da sanal anlamda). Günümüzde bilgi profesyonellerinin sadece geleneksel bilgiyi düzenleme yeteneğine sahip olmaları yeterli değildir. Bu kişiler aynı zamanda insan düzenleme becerilerine de sahip olmalıdırlar. Şöyle ki Google ve Facebook'un misyonlarının karşılaştırılması ile aradaki fark açıklanabilmektedir. Google'ın misyonu "dünyanın bilgisini düzenlemektir" Facebook ise "dünyanın insanlarını düzenlemeyi" kendisine misyon olarak seçmiştir (Tonta, 2009: 748,763). Sosyal medya ağı kullanıcılarının belirli bir düzeyde okur-yazarlık seviyesine sahip olması zorunludur. Çünkü sosyal ağlarda gizlilik en önemli unsurdur. Gizliliğin önemsenmemesi ise yıkıcı sonuçlara neden olabilmektedir. Bu

yıkıcı sonuçlar aşırıya kaçma olarak adlandırılır. Bu noktada aşırıya kaçma eylemi, gençlerin bütün samimiyetleriyle paylaşılan her türlü bilgiyi en özel detaylarıyla ele vermelerinden kaynaklanmaktadır. Ayrıca sosyal medya kullanıcılarının, gizliliklerini tehlikeye atan özel paylaşımlarda bulunmaları durumunda oluşabilecek tüm olası olumsuz gelişmelere karşı sadece kendilerini değil tüm aile ve arkadaş çevrelerini de tehlikeye atmış olduklarının bilincin de olmalılardır. Üstelik sosyal medya da arkadaş çevresi genişledikçe riskte büyümektedir.

Günümüzde artık işverenler için iş başvurusunda bulunan kişilerin sosyal medya hesaplarını taramak bir eğilim haline gelmiştir. İşverenlerin, başvuru sahiplerinin sosyal medya hesaplarını incelemeleri neticesinde iş başvurusunda bulunan adayların yüzde 34'ünün sosyal medya hesabında bu adaylara iş teklif edilmesine engel olacak nitelikte içerik tespit edilmiştir. Bu içeriklerin geneli incelendiğinde uygun olmayan fotoğraf paylaşımları ön plana çıkmaktadır. Sosyal medya ve mesleki riskler konusu değerlendirmeye alındığında konunun yeteri kadar önemsenmediği dikkat çekmektedir. Günümüzde üniversitelerde sosyal medya ve iletişim gibi konuların üniversite müfredatlarına dâhil edilmesine özellikle dikkat edilmelidir. Örneğin; Lancashire Üniversitesinde öğrencilerin çevrimiçi kimliklerini yönetmelerine yardımcı olan "Siz Markasınız" başlıklı dersler verilmektedir. Özellikle çevrimiçi kaynakları kullanma ve yasal içeriğini anlama konusunda tüm öğrenciler için bilgi ve becerilerini artıracak ve uygunsuz çevrimiçi davranışlarda risk değerlendirmesi yapılabilecek ek derslere ihtiyaç duyulmaktadır. Özetle bireysel iletişim ve gelişimle birlikte vatandaşlar arasında doğru iletişim dengesini sağlamaya ayrıca dijital okuryazarlıkla birlikte gençliğin, iletişim becerilerinin geliştirilmesi üzerine odaklanılmalıdır (Gathegi, 2014: 101-106).

2.1. Sosyal Ağlarda Gizlilik ve Güvenlik

İnternetin geniş kitlelerce kullanımının yaygınlaşmasıyla birlikte sosyal ağ sitelerinin de kullanımı günden güne artmaktadır. İnsanlar arasındaki sosyal etkileşimi kolaylaştıran sosyal ağlar, çevrimiçi kullanıcıların arkadaşları, iş arkadaşları, meslektaşları, aile çevresi ve hatta tanımadıkları yabancı insanlarla paylaşım ve etkileşim içerisinde oldukları ağlardır. Dikkatli kullanılmadığı takdirde kişi güvenliğini ve mahremiyetini tehlikeye atan sosyal ağlar kişilere finansal açıdan da önemli zararlar verebilmektedir. Sosyal ağlarda kişisel verilerin korunmasına

yönelik artan risk güvenlik konusunda yeni öngörüler gerektirmektedir. Yapılan çalışmalar kişisel verilere yönelik artan riskin en önemli sebebinin farkındalık eksikliği olduğunu göstermektedir (Ahn, Shehab ve Sguicciarini, 2011: 10).

Sosyal ağları kişisel çıkarları uğrana istismar eden kişilerin sayıları her geçen gün artmaktadır. Bu istismarın en önemli sebebi ise bilişim korsanlarının çok istemelerine rağmen ulaşamadıkları bilgilerin, sosyal ağlarda kullanıcılar tarafından bizzat ifşa edilip kolaylıkla ele verilmesidir. Sosyal ağlarda alınması gereken güvenlik tedbirleri incelendiğinde konu; sosyal çözümler, teknik çözümler ve yasal çözümler olmak üzere üç başlık altında incelenmektedir (Yavanoğlu, Sağıroğlu ve Çolak, 2012: 19).

2.1.1. Sosyal Önlemler

Sosyal önlemler çocuklar ve yetişkinler için olmak üzere iki başlıkta toplanmıştır.

2.1.1.1. Çocuk Kullanıcılar için Önlemler: Çocuklar için ilk etapta yapılması gereken ailelerin çocuklarını sosyal ağ sitelerini kullanmaktan uzak tutmaları olacaktır. Bu platformlarda çocukların başına gelebilecek tehlikeleri önlemede birinci derecede aileler sorumludur. Çocukların sosyal ağlarda çok dikkatli olmaları, başlarına gelebilecek tehdit ve tehlikeler konusunda bilgilendirilmeleri farkındalık açısından önemlidir. Bununla birlikte çocukların çevrimiçi bulundukları ortamlar kontrol edilmeli, fotoğraflarda etiketleme yapılmamalı ve detay verilmemelidir. Çocukların okul, sınıf, kimlik, adres ve telefon bilgilerinin sosyal ağlarda paylaşılmadığından emin olunmalıdır. Son olarak çocuklara tanımadıkları insanlarla yazışmamaları konusunda mutlaka uyarılarda bulunulmalıdır. Türkiye'de internetten cinsel içerikli mesaj aldığını ve bundan rahatsızlık duyduğunu söyleyen çocukların sayısı %50 iken Avrupa'da benzer şekilde mesaj alan ve bundan rahatsızlık duyan çocukların oranı %25'tir (Çelen, Çelik ve Seferoğlu, 2011: 649).

2.1.1.2. Yetişkin Kullanıcılar için Önlemler: Sosyal ağlarda, sosyal mühendislik ataklarından korunmak için bilinmeyen yeni gruplar içine girilmemeli, sosyal ağlara katılma davetleri araştırma yapıldıktan sonra kabul edilmeli, arkadaş olarak kabul edilecek kişiler konusunda seçici olunmalıdır. Kimlik bilgileri hiçbir zaman paylaşılmamalı zorunlu ise üzerinde küçük değişiklikler yapılmalı, isim ve

soyadı yerine yakın çevrede kullanılan takma isimler kullanılmalıdır. Profil sayfalarında çalışılan kurumla ilgili kurumsal bilgiler paylaşılmamalıdır. Sosyal ağlarda benzer çalışma alanların da çalışmalar yapan kişilere yönelik gruplar ve topluluklar bulunmaktadır. Bu grup veya topluluklarda sosyal mühendislik faaliyetlerine karşı dikkatli olunmalıdır. Özellikle tatile çıkıldığını belirten anlık bir mesaj ya da bir fotoğraf paylaşımı yapılmamalıdır. Bu durum hırsızlara davetiye çıkarmaktan farksızdır. Coğrafi konumu gösteren mobil uygulamalardan kaçınılmalıdır. Çünkü bu tür bilgiler üçüncü kişiler tarafından görüntülenebildiğinden bilgisayar korsanları ya da organize suç örgütleri tarafından gerçekleştirilen saldırılarda kullanılabilmektedir. Aile bireyleriyle çekilen fotoğraflarda etiketleme yapmaktan kaçınılmalı ayrıca izinsiz fotoğraf etiketlemesi yapan kişiler uyarılmalıdır. Son olarak sosyal medya profillerinde ya da arkadaş sayfalarında kişisel bilgileri deşifre eden özel konularda yorum yazmaktan özenle kaçınılmalıdır. (Yavanoğlu, Sağıroğlu ve Çolak, 2012: 24-25).

2.1.2. Yasal Önlemler: Sosyal ağ sitelerine üye olunmadan gizlilik politikaları iyi okunmalı, kişisel bilgilerin hangi şartlarda 3. şahıslarla paylaşılacağı bilinciyle üyelik işlemlerine başlanılmalıdır. Sosyal ağ sitelerinin gizlilik politikalarına uyup uymadıkları kontrol edilmelidir. Tüm sosyal medya kullanıcıları kanuni haklarını bilmeli ayrıca kişisel verilerin korunması kanununa uygun olacak şekilde bilgi ve belge paylaşımı yapılmasına özen gösterilmelidir. Çocukların yaşlarına uygun ağları kullanmalarına dikkat edilmelidir (Yavanoğlu, Sağıroğlu ve Çolak, 2012: 24-25).

2.1.3.Teknolojik Önlemler: Sosyal ağ şifresinin 12 karakter kombinasyonundan oluşturulmasına dikkat edilmelidir. Ayrıca karakterlerin içinde büyük ve küçük harf, "+, -, *, !" gibi özel karakterler bulundurarak şifrelerin düzenli aralıklarla değiştirilmesine özen gösterilmelidir. Bilgisayar korsanları çevrimiçi ağlarda kendilerini sosyal ağ kullanıcılarının arkadaşıymış gibi göstererek hedeflerinde bulunan kişiye mail yoluyla tuzak kurabilmektedirler. Bu aldatmacaları engellemek için e-postaların eklentisinde bir dosya ya da bağlantı bulunuyorsa verilen linkin öncelikle tarayıcıya kopyalanarak taşınmasına ve sonrasında açılmasına dikkat edilmelidir. Üye olunan sosyal ağ sitesine kaydedilen e-posta adresinde, tüm haberleşme akışının taranabileceği unutulmamalıdır. Ayrıca kaydedilen mail adreslerinin reklam sitelerine satılabileceği bilinmelidir. Sahte

sitelere karşı güvende olmak için öncelikle adres satırına erişilmek istenen web sitesinin adresi kopyalanarak web sitesine giriş yapmaya çalışılmalıdır. Bu yolla kullanıcılar sahte web sitelerinden korunmuş olacaklardır. Kullanılan yazılımların ve işletim sistemlerinin güncellenmemesinden dolayı oluşan güvenlik açıklarına dikkat edilmeli, tüm bilgisayar yazılımları güncel tutulmalı, anti-viral ve güvenlik duvarı yazılımları mutlaka kullanılmalı, kötücül yazılım ile spam engelleyici filtreler tercih edilmelidir. Dikkat edilmesi gereken en önemli noktalardan bir diğeri üye olunan sitelerde 3.parti uygulamaların kişisel bilgilere erişmek amacıyla bilgisayarlara yazılım yükleme girişimleridir. Bu zararlı yazılımlar, bilgisayar kullanıcısının dikkatini çekecek video ve fotoğraf paylaşımlarıyla sosyal medya ağı profillerine erişmeye çalışmaktadırlar. Bu noktada öncelikle bu tarz bir uygulamaya izin verilmiş ise uygulama ayarları menüsünden sahte uygulamalar kaldırılmalıdır. Bu konuda yaşanan en büyük tehdit kullanıcı adına arkadaş profillerine gönderilen reklam mesajlarıdır (Yavanoğlu, Sağıroğlu ve Çolak, 2012: 24-25).

2.2. Sosyal Ağlarda Yapılan Bir Güvenlik Çalışmasının Sonuçları ve Öneriler

Bir üniversitede sosyal ağların kullanımını araştıran bir çalışma, birçok sorunun nereden kaynaklandığını açıklamaktadır. Çalışmada ortaya çıkarılan tespitler aşağıdaki gibidir (Yıldırım ve Varol, 2013: 10-11).

- Kullanıcılar günde en az 1-5 kere arası sosyal ağları kontrol etmektedir. Öyleyse sosyal ağlar insan hayatında çok önemli bir yere sahiptir.
- Sosyal ağların kullanımında, kullanıcılar PC'yi akıllı telefonlara göre daha güvenli bulmaktadırlar. Fakat kullanıcılar yinede sosyal ağlara akıllı telefonlar ile daha fazla bağlanmaktadırlar. Ayrıca kullanıcılar akıllı telefon güvenliği hakkında ne yapacaklarını bilmemektedirler. Bu nedenle İOS tabanlı IPhone ve IPad gibi cihazların safari ayarlarında "Dolandırıcılık Uyarısı ve Pencereleri Engelle " seçeneklerinin seçili (mavi) olmasına dikkat edilmelidir. Android cihazlarda ise GPS (Global konumlandırma sistemi) kullanılmadığında devre dışı bırakılmalı ve sosyal ağ uygulamalarının telefon rehberi taramasına izin verilmemelidir.

- Kullanıcıların büyük çoğunluğu sosyal ağları güvenli bulmamalarına rağmen anti virüs yazılımları kullanmamaya devam etmektedirler. Oysaki antivirüs uygulamaları, zararlı yazılım uygulamalarını ve spamları engellemektedir.
- Sosyal ağ kullanıcılarının çoğunluğu kişisel bilgilerini, sistemlere doğru olarak girmektedir. Oysaki sosyal ağlar, kişisel verileri korumada yetersizdir bu nedenle sosyal mühendislik saldırılarının yaşanabileceği unutulmamalıdır.
- Kullanıcıların yarısından fazlasının zararlı spam ya da uygulamaya maruz kaldığı görülmüştür. Kullanıcıların çoğunluğu emin olmadıkları uygulamaları açmadıkları halde zararlı yazılımlara engel olamamaktadırlar. Bunun nedeni ise güvenli sanılan uygulamaların aslında zararlı uygulamalar olmasıdır. Bu zararlı uygulamaların dağıtılmasına engel olabilmek için sosyal ağ hizmetlerinin, arkadaşların e-posta adres defterlerini taramasına izin verilmemelidir.
- 10 kullanıcıdan 2'si adına sahte hesap açıldığı ve izinleri dışında fotoğraflarının kullanıldığı tespit edilmiştir. Bu durumu engelleyebilmek için tanınmayan kişiler sosyal ağlarda arkadaş olarak eklenmemeli ve güvenli arkadaş listeleri oluşturulmalıdır.
- 10 kullanıcıdan 3'ü sosyal ağlarda rahatsız edici mesajlar almaktadır. Bu gibi durumlarda gerekli yerlere mutlaka bildirimlerde bulunulmalıdır. Çünkü siber zorbalar, zorbalıklarıyla sanal ortamlarda olduğu gibi gerçek hayatta da karşımıza çıkabilmektedir.
- Sosyal ağ kullanıcılarından 10 kişiden 2'sinin sosyal güvenlik ayarlarını yılda bir ya da hiç kontrol etmedikleri tespit edilmiştir. Oysa her paylaşımda belirli listelere izinler vermek için gizlilik ayarları kontrol edilmelidir. Çünkü sosyal ağ sitelerinin büyük çoğunluğu güvenlik ayarlarını sıklıkla değiştirmektedir.

Son olarak sosyal ağlarda iyi bilinen şirketlerin isimleri kullanılarak sahte ürün satışlarıyla e-dolandırıcılık yapıldığı unutulmamalıdır. Ayrıca kritik görevlerde bulunan veya bulunma potansiyeli bulunan kişiler sosyal medyayı kullanmamalıdır (Ceyhan, Demiryürek ve Kandemir, 2015: 4-8).

3. ONLİNE (ÇEVRİMİÇİ) ALIŞVERİŞİ ETKİLEYEN NEDENLER VE TÜRKİYE'DE E-TİCARETİN GELİŞİMİ İÇİN DEĞERLENDİRİLMESİ GEREKEN BAŞLIKLAR

Günümüzde insanoğlu teknoloji çağında yaşamaktadır. Bu sebeple dünya ülkeleri teknolojilerine yatırım yaparak gelişmeyi hedeflemektedirler. Her gün internete bağlanan kişi sayısının artmasıyla birlikte çevrimiçi ortamlarda geçirilen sürenin artması e-ticaretin geleceğini etkileyen en önemli iki unsur arasında yer almaktadır. Araştırmalar insanların geleneksel mağazalarda alışveriş yapmak yerine çevrimiçi sitelerde alışveriş yapmalarını hem daha az zaman alıcı hem de daha eğlenceli bulduklarını ortaya çıkarmıştır. Bu eğilimin sonucunda internette alışveriş her yıl muazzam olarak büyümektedir. E-ticaret sisteminin küresel tüketicilere 7 gün 24 saat hizmet sunması, tüketicileri kendisine çeken bir başka faktördür. Konu çevrimiçi satıcıların pazarlama politikaları çerçevesinde değerlendirildiğinde çevrimiçi alışverişte iki önemli unsur ortaya çıkmaktadır. Bu unsurların ilki çevrimiçi web sitelerinde tasarımın öneminin kavranması bir diğeri ise web sitesinin yerel ve kültürel konularda tüketicileri yansıtacak içeriğe sahip olmalarıdır (Rahman, 2018: 8-9).

Avrupa'da çevrimiçi işletmelerin pazarlamada başarılı olabilmeleri için 5C stratejisi kullanılmakta ve çevrimiçi satışta genel bir çerçeve oluşturulmaktadır. 5C stratejisinde çevrimiçi şirketlerin başarı faktörleri şu şekilde özetlenir:

- Sitenin içeriği müşterinin sitede geçirdiği zamanı %33 oranında artırmaktadır.
- Sitenin müşterine kolaylıkla sipariş verme olanağı sağlaması ticari ilişkilerini %33 oranında artırmaktadır.
- Sitenin müşterileri arasındaki fikir alışverişini desteklemesi başarıyı %11 oranında artırmaktadır.
- Sitenin danışmanlık hizmeti vermesi %11 oranında güveni ve yeterliliği artırmaktadır.
- Potansiyel müşterilere reklam ile ulaşma %11 oranında başarıyı artırmaktadır (Angelı ve Kundler, 2006: 623-624).

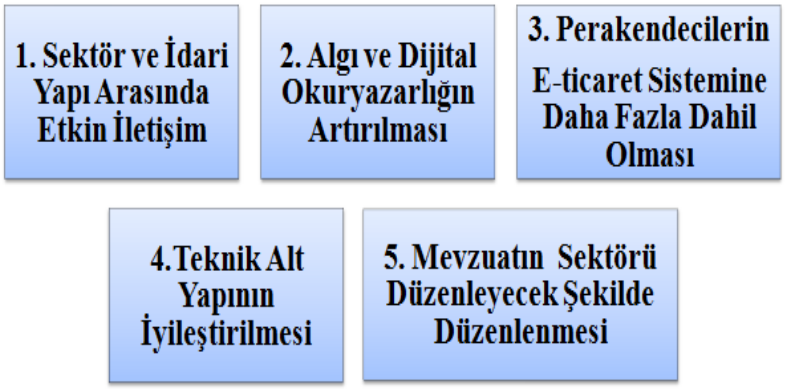
E-ticaret yoluyla uluslararası ticaret hacmi artmakta yüksek gelirli ekonomilerden yayılan bilgi aracılığıyla ithalatta bilgi ekonomisine açık olan ülkeler, artan ticaret hacminden pozitif yönde etkilenmektedirler. E-ticaret ayrıca hizmetler ticaretinde de önemli bir etkiye sahiptir. Doğrudan ya da dolaylı olarak yeni işler yaratmanın yanında iş kayıplarına neden olunması da mümkündür. Oluşacak yeni iş kolları arasında bilgi ve iletişim teknolojileri sektörü ivme kazanırken tüketici taleplerine bağlı olarak değişecek kar-zarar tabloları neticesinde e-ticarette net istihdam oranı değişecektir (Terzi, 2011: 752).

Günümüzde turizm ekonomisinin e-ticaret hacmine büyük etkisi bulunmaktadır. Turizmde elektronik ticarete duyulan güveni araştıran bir çalışmada tüketicilerin online alışveriş niyetlerinde, güven olgusunun satın almayı etkileyen bir sadakat göstergesi olduğu tespit edilmiştir. Turizmde e-ticaret siteleri yöneticileri kendilerini geliştirmeye, müşteri memnuniyetini ve güvenini kazanmaya dikkat etmelidir. Hala birçok tüketici tatil satın almak konusunda isteksiz davranmaktadır. Çünkü özellikle yüksek fiyatlı lüks ürünler ve hizmetler görünmeyecekleri için görünmez olan turizm ürünleri ve hizmetleri e-ticarette tüketicilere daha az güvenilir gelmektedir. Ülke ekonomisine yüksek katma değer sağlayacak olan turizm ürünleri ve hizmetleri, online ticarette şirket yöneticilerinin özenle üzerinde durması gereken bir konudur. Güney Kore'de yapılan bir araştırmada ortaya çıkan bulgular, online turizm pazarlamasında tüketici tarafından algılanan güvenliğin, talebi etkilemede en önemli unsur olduğu tespit edilmiştir (Ja Kim, Chung ve Ki Lee, 2011: 264).

Dünya genelinde olduğu gibi ülkemizde de e-ticaret hızla büyümektedir. Fakat bu büyüme ülkemizi uluslararası arenada beklenilen rekabetçi düzeye henüz taşıyamamıştır. Nedeni ise e-ticaretin hem arz hem de talep yönünde sisteme ilk kez dâhil edilecek üretici ve tüketicilerin teşvik edilmesi konusunda dönüşümü sağlayacak büyük adımların atılamamasıdır. Türkiye internet kullanıcı sayısı, ödeme ve lojistik alt yapısı ile e-ticaret pazarında dikkat çekici bir potansiyele sahiptir. Örneğin 2012 yılında % 45 olan internet kullanım oranının 2020 yılında %76 seviyesine çıkacağı öngörülmektedir. Dünyanın en kalabalık 19. ülkesi olan Türkiye, dünyada en çok internet kullanıcısı bulunan ülkeler arasında 17. sırada yer almaktadır. Ülkelerin online potansiyellerini gösteren en önemli göstergelerden bir tanesi de sosyal medya kullanımlarıdır. Türkiye 2016 yılında 33 milyon kullanıcısı ile dünyanın en büyük sosyal ağı Facebook'u en çok kullanan 10. ülke

konumundadır. Instagramda ise 16.3 milyon kullanıcısı ile ABD, Rusya ve Brezilyanın ardından 4. sırada yer almaktadır. Online potansiyeli gösteren bir başka unsur akıllı telefonlardır. 2021 yılında Türkiye nüfusunun %84'ünün akıllı telefon kullanıcısı olması beklenmektedir. Bu verilerin tamamı Türkiye'nin gelecekteki online potansiyelinin büyüklüğüne işaret etmektedir. Türkiye'deki tüketicilerin online alışveriş tutumları incelendiğinde online alışverişte en önemli motivasyon unsurunun ucuzluk olduğu, interneti kullanan bireylerin yalnızca üçte birinin online alışveriş yaptığı, ürün araştırmasının mobil telefonlarda, satın alma işleminin masa üstünde yapıldığı, ortalama sepet tutarının 279 TL olduğu tespit edilmiştir. Online alışverişte müşteri talepleri değerlendirildiğinde hızlı teslimat ve satış sonrası süreçlerin iyileştirilmesi ilk sıralarda yer alan talepler arasında bulunmaktadır. Türkiye'de son dönemde e-ticaret sektörü büyük bir gelişme göstermiş olsa da e-ticaretin altyapısal anlamda gelişimi için aşılması gereken bir takım sorunlar olduğu tespit edilmiştir.

Türkiye'de online ticaret sektörünün ivme kazanabilmesi için alınması gereken aksiyonlar Şekil 12 ile özetlenmektedir (Kantarcı ve diğerleri, 2017: 40-56).



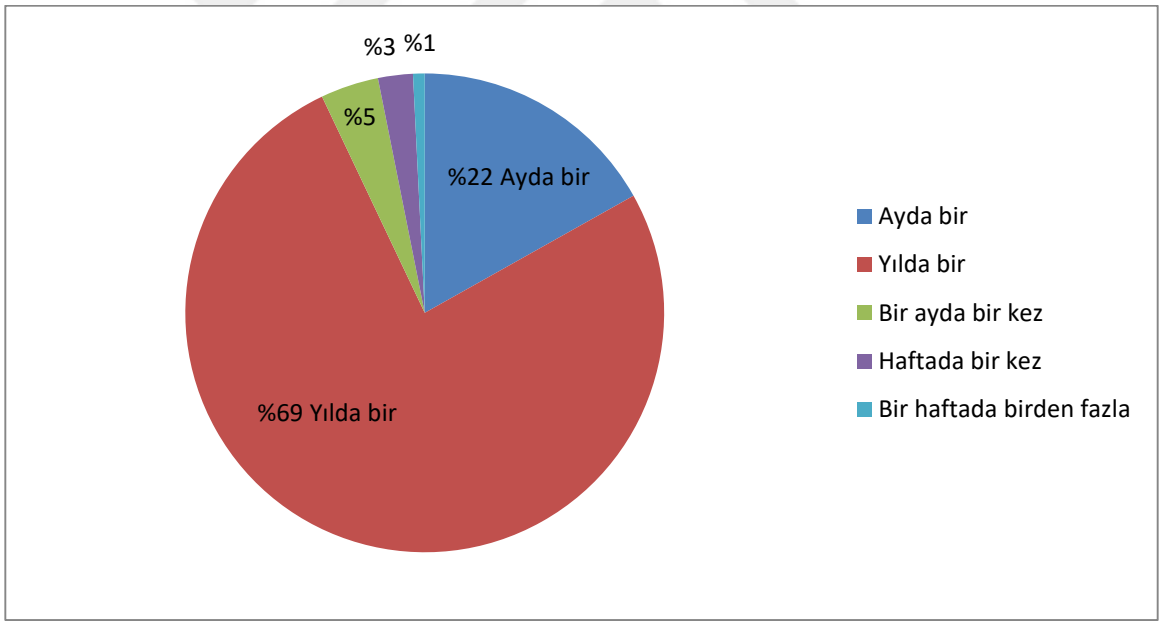
Şekil 12: Türkiye'de E-Ticaretin Büyümesi için Değerlendirilmesi Gereken Konular

Kaynak: Dijitalleşen Dünyada Ekonominin İtici Gücü: E-Ticaret. **TUSIAD Yayınları**, İstanbul.(2017).Sayfa,56 Yararlanarak hazırlanmıştır.

- Sektör ve idari yapı arasında etkin bir iletişim için iletişim ve koordinasyonda raporlama ve performans takibi yapılmalıdır.

- Algı ve dijital okuryazarlığın artırılması için internet kullanmayan tüketici ve işletmelerle birlikte internet kullanıcısı olmasına rağmen e-ticaret faaliyeti olmayan kitle sisteme dâhil edilmelidir.
- Perakendecilerin e-ticaret sistemine daha fazla dahil olması için mega ve büyük ölçekli perakendecilerle birlikte kobilerde sisteme dahil edilmelidir.
- Teknik alt yapının iyileştirilmesi için ödeme sistemleri, internet erişimi, lojistik ve operasyonel hizmetler iyileştirilmelidir.
- Mevzuatın sektörü destekleyecek şekilde düzenlenmesi için yeni e-ticaret kanunu ve farklı düzenleme alanlarıyla anlaşmazlıklar çözümlenmelidir.

2016 yılında Türkiye'de yapılan bir araştırma tüketicilerin online alışveriş yapma sıklığını araştırmıştır. Verilere göre katılımcıların %69'u yılda yalnızca bir kere online alışveriş yapmaktadır (El-Hassan, 2016: 439). Grafik 2 ile gösterilen veriler, Türkiye'de e-ticaretin büyümesi için değerlendirilmesi gereken konuları destekler niteliktedir.



Grafik 2: Türkiye'de Online Alışveriş Sıklığı

Kaynak: Mohamad El-Hassan (2016).Hizmet Sektöründe Online Alışveriş Davranışını Etkileyen Faktörler: Seyahat Sektörü (Türkiye ve Slovenya Karşılaştırması).Yayınlanmış Yüksek Lisans Tezi Mersin Üniversitesi S.B.E.Mersin, s.43.Yararlanarak Hazırlanmıştır.

4. ONLİNE TÜKETİCİ DAVRANIŞI VE ONLİNE ALIŞVERİŞTE GİZLİLİK İLE GÜVENLİK

Günümüzde şirketler rekabetçi bir ortamda faaliyette bulunmaktadır. Bu nedenle satıcılar müşteri ihtiyaçlarını en iyi şekilde anlamaya çalışarak müşterilerinin beklenti ve ihtiyaçlarına doğru cevap verebilmek adına çalışmalar yapmaktadır. Bu noktada satıcıların iki başarı faktörü ortaya çıkar. İlk faktör müşteri kazanmak, ikinci faktör müşteriyi elde tutabilmektir. Uzun zamandan beri çevrimiçi alışverişlerde tüketici davranışlarını anlamaya yönelik modeller geliştirilmeye çalışılmaktadır. Tüketici davranış modeli, satıcıların bir tüketicinin satın alma eylemini nasıl gerçekleştirdiklerini anlamalarına yardımcı olmak için tasarlanır.

Müşteri karar sürecini iyi analiz eden bir işletme, alıcıların kararını etkilemede sağlam adımlar atabilmektedir. Alıcıyı etkileme süreci öncelikli olarak ürün tasarımı ve reklam yoluyla başlar. Bu noktada tüketicileri iki gruba ayırmak mümkündür. İlk grupta bireysel tüketiciler, ikinci grupta hükümetler dâhil olmak üzere kâr amacı gütmeyen kuruluşlar yer almaktadır. Bu iki alıcı türü farklı satın alma davranış kalıplarına sahiptir. Bu sebeple farklı analiz edilir. Bireysel tüketici davranışları incelemeye alındığında, alıcının satın alma kararını etkileyen kişilik ve psikolojik değişkenlerin yanında, demografik faktörlerinde tüketici tercih ve davranışlarına etki ettiği görülmektedir. Çevrimiçi web sitelerinin izlediği başlıca demografik özellikler arasında; cinsiyet, yaş, medeni durum, eğitim düzeyi, etnik köken, meslek ve hane gelirine ilişkin bilgiler izlenmektedir. Çevrimiçi işletmelerde, satıcı işletmenin büyüklüğüyle ticari itibarı arasında doğru orantı bulunur. Örneğin, Amazon.com'un büyüklüğünden ileri gelen ticari itibarından dolayı müşterileri kendilerini daha fazla güvende hissetmektedir. Ticari işletmelerin çevrimiçi işlemlerinde; güvenlik koruması, ödeme mekanizması, bilgisayar ortamının tipi (mobil veya masaüstü), web sitesinin tasarımı, işlevselliği (navigasyon kolaylığı gibi) lojistlik desteği ve tüketici hizmetleri, satıcılar için müşteriyi etkilemede en önemli etkiye sahip konulardır. Tüm bu hizmetlerde dikkatli olunması gereken ana konu ise işlem sürecindeki tüketiciyi güvenlik ihlâlleri ve beklenmeyen teknik hatalardan korumaktır (Turban ve diğerleri, 2018: 362-364).

E-ticaret terimi elektronik ticaret deyiminden alınmıştır. Günümüzde mücevherlerden, kitaplara, mobilyalardan, filmlere kadar neredeyse her şey çevrimiçi

satın alınabilir duruma gelmiştir. Öyle ki online alışverişte açık arttırma çılgınlığı patlamıştır. İnternetten alışveriş müşteriye pek çok kolaylık sunar. Bilgisayardan ya da cep telefonundan yapılan alışverişlerde; araba kullanmak, park etmek, mağazada sıra beklemek gibi zaman alıcı aktiviteler olmadığından, geleneksel alışverişlere göre daha rahat bir alışveriş ortamı bulunmaktadır. Birden fazla mağazada aynı anda fiyat karşılaştırması yapılarak en iyi fiyat bulunabilmekte, dünyanın herhangi bir yerinde herhangi bir saatte alışveriş yapılabilmektedir. Ancak birçok kullanıcı internetten alışveriş yapma konusunda hâlâ çekimser davranmaktadır. Nedeni ise kredi kartı sahtekârlığına karşı vermek istemedikleri kredi kartı bilgileridir. Aslında birçok online alışveriş tehlikesi, geleneksel alışveriş tehlikesiyle aynıdır. Örneğin kredi kartı numarası web sitesi çalışanları tarafından çalınabilmektedir fakat geleneksel bir mağaza çalışanı tarafından da aynı bilgilerin çalınma ihtimâli vardır.

Çevrimiçi dünyada bir e-ticaret sitesi, birçok kart numarasını veri tabanında saklar. Bu veritabanları kredi kartı sahtekârlığında aktif olan suçlu bir hacker için mükemmel bir hedeftir. Bilgisayar korsanları şirket veritabanlarını hedefleyerek kart numaralarını elde ettikten sonra bu bilgileri karaborsada satabilir veya internette herkese açık olarak yayınlayıp ilgili şirkete şantaj yapabilmektedir. Aslında bilgisayar korsanlarının bu tür etkinlikleri çoğu insanın fark ettiğinden çok daha fazladır. Daha vahim olan bir konu ise bu tür saldırılara uğrayan şirketlerin, medyada haklarında olumsuz konuşmalar yapılması sebebiyle uğrayacakları itibar kaybı korkusuyla kanuni yollara başvurmamalarıdır.

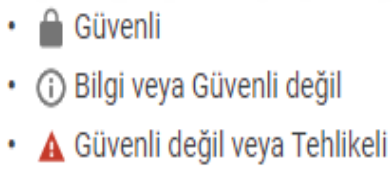
Bilgisayar korsanlarının denizaşırı ülkelerde bu tür dolandırıcılık eylemlerinde bulunmaları onları takip etmek ve kovuşturmak açısından zor ve imkânsız olabilir. Çevrimiçi kredi kartı sahteciliği ve dolandırıcılığı bir bütün olarak güven kaygılarını tartışmasız yeni bir seviyeye taşımıştır. İnternet genelinde birçok e-ticaret sitesi, kendilerini ve müşterilerini tüm bu risklerden koruyabilmek için güvenlik seviyelerini arttırmaya yönelik çalışmalar yapmaktadır. Konu tüketici açısından değerlendirildiğinde, tüketicilerin çoğunlukla online alışveriş yapma tutumlarında büyük bir kararlılık görülmektedir. Çünkü online alışveriş tüketiciye zamandan ve paradan tasarruf sağlamaktadır. Bununla birlikte tüketicilerin anlaması gereken en önemli konu online alışverişte güvenliklerini nasıl sağlayacaklarını bilmeleridir. Tüketicilerin yeterli bilgi birikimine ulaşmaları, sahip olacakları yüksek

bilinç düzeyleri, tüketici güvenliğini gerçek anlamda destekleyecektir (Bahadur, Chan ve Weber, 2002: 262-264).

İnternette tüketicileri en çok korkutan konu bilgilerinin gizliliğinin tehlikede olmasıdır. Bu nedenle pek çok tüketici internetten alışveriş yapmaktan vazgeçmektedir. Diğer taraftan web siteleri için kişisel bilgiler pazarlamanın araçları arasındadır ve ticari web sağlayıcıları tarafından bu bilgiler paylaşılmaktadır. Burada kişisel bilgilerin ticari web sitesi sağlayıcıları tarafından ikincil kullanımı, web sitesi sağlayıcılarıyla tüketiciler arasında ciddi bir çatışma nedeni olarak değerlendirilmektedir. İnternetin getirdiği veri madenciliği ve veri ambarı fırsatları çağımızda daha önce hiç olmadığı kadar istismar edilmektedir (Hoffman, Novak ve Peralta,1999: 83).

4.1. Bir Site Bağlantısının Güvenilirliğini Kontrol Etme

Bir web sitesi ziyaret edildiğinde site hakkındaki güvenlik bilgileri kontrol edilmelidir. Ziyaret edilen site güvenli veya gizli değilse web sitesi adresinin sol tarafında bulunan güvenlik durumu kontrol edilmelidir (https://support.google.com, 2018).



- Site Güvenli ise adres çubuğunda kilit işareti bulunur. Site üzerinden gönderilen ve alınan bilgiler gizli kalır. Sitede kilit işareti bulunsa bile gizli bilgiler paylaşılırken yinede dikkatli olunmalı ziyaret edilmek istenen site, adres çubuğundan yeni bir bağlantı açılarak kontrol edilmelidir.
- Adres çubuğunda Bilgi veya Güvenli Değil işareti bulunuyorsa site gizli bir bağlantı kullanmamaktadır. Yani birileri site üzerinden gönderilen bilgileri görebilmekte ve değiştirilebilmektedir. Böyle bir bağlantıyla karşılaşıldığında adres çubuğu seçilerek http:// kısmi silinmeli yerine https:// yazılmalıdır. Bu uygulamada işe yaramaz ise site sahibiyle iletişime geçilmeli verilerin güvenliğinin sağlanabilmesi için HTTPS bağlantısının sağlanması istenmelidir.

- Adres çubuğunda güvenli değil veya tehlikeli işareti bulunuyorsa bağlantının gizli olmadığı anlaşılmalıdır. Bu durumda siteyle, ağla veya bağlanılan cihazla ilgili bir sorun var demektir. HTTPS, bağlantı güvenliği demektir. Web siteleri kimliklerini tarayıcılara (örn, Google Chrome) kanıtlamak için sertifika kullanırlar. Fakat herkes istediği web sitesi olduğunu iddia ederek bir sertifika oluşturabilmektedir. Bu sebeple web sitelerinin güvenilir kuruluşlardan alınmış sertifikalara sahip olmaları gerekmektedir.

4.2. Web Sitelerinin Çerez Politikalarını Yönetme

Ziyaret edilen web siteleri tarafından oluşturulan dosyalara çerez denilmektedir. Çerezler kullanıcının göz atma bilgilerini kaydederek çevrimiçi deneyimlerini daha kolay hale getirmektedir. Çerezler sayesinde siteler kullanıcı oturumlarını açık tutabilmekte, site kullanıcısına tercihlerini hatırlatabilmekte ve kullanıcıya yerel olarak bulunduğu bölgeyle alakalı içerik sunabilmektedir. İki tür çerez bulunmaktadır (https://support.google.com, 2018).

- Birinci taraf çerezleri: Ziyaret edilen site tarafından oluşturulmakta ve site adres çubuğunda gösterilmektedir.
- Üçüncü taraf çerezleri: Diğer siteler tarafından oluşturulmaktadır. Bu siteler kullanıcı tarafından ziyaret edilen web sayfasında görülen reklam veya resim gibi içeriğin bir kısmına sahiptir.

Web siteleri tarafından kaydedilen çerezlere kullanıcı izin verebilmekte veya engelleyebilmektedir. Yalnız kullanıcıların, sitelerin çerezleri kaydetmesine izin vermediği durumlarda oturum açılması gerekiyorsa çoğu site çalışmamaktadır. Tüm kullanıcılar tüm çerezleri veya belirli çerezleri silme ve çerez ayarlarını değiştirerek belirli bir site için çerezlere izin verme veya onları engelleme hakkına sahiptir.

4.3. Tüketiciler için Online Alışverişte Güvenlik İpuçları

İnternet üzerinden elektronik alışveriş yapan tüketicilerin, site güvenliğinden emin olmaları için yapmaları gereken bazı güvenlik kontrolleri bulunmaktadır. Bu güvenlik kontrolleri şu şekilde sıralanabilir: (Çetin ve Irmak, 2014: 279-281, Crowder ve Crowder, 2000: 73, Küçükyılmazlar, 2006: 10).

- İnternet üzerinden elektronik alışveriş yapılırken kredi kartı bilgilerinin, üçüncü şahıslar tarafından ele geçirilmesinin önlenmesi amacıyla bu bilgilerin şifrelenmesi anlamına gelen SSL (güvenli kilit sistemi) ve SET (güvenli elektronik işlemler) protokolleri kullanılarak alışveriş güvenliği sağlanmaktadır. SSL sertifikası bulunmadan hiçbir bankadan pos alma imkânı yoktur. Bu sebeple kullanıcı web sitesinin SSL ve SET sertifikasının olup olmadığını mutlaka kontrol etmelidir.
- Sitenin iletişim bilgilerinde telefon numarası, açık adres ve sitenin kimliğini belirten bilgilerin açık bir şekilde verilip verilmediği kontrol edilmelidir.
- Ödeme adımına geçildiğinde, site isminin yazıldığı URL bağlantısında "https://.www" yazılmasına dikkat edilmelidir.
- Sitedeki ürünlerin en son ne zaman güncellendiğine dikkat edilmelidir.
- Alışveriş öncesi müşteri hizmetlerine mail gönderilmeli, 3 gün içerisinde dönüş yapılmasına dikkat edilmelidir.
- Alışveriş yapılan siteyle ilgili arama motorlarında, blogların arşivlerinde ve şikâyet sitelerindeki yorumlara dikkat edilmeli, site içerisinde alınmak istenen ürünle ilgili müşteri yorumları okunmalıdır.
- Alışveriş rehberlerinde ve karşılaştırma sitelerinde sitenin puanlamasına ve alışverişin nasıl yapılması gerektiği konusunda bir açıklama bulunup bulunmadığına dikkat edilmelidir.
- Sitenin güvenlik sertifikasının geçerlilik süresi kontrol edilmelidir.
- Kullanılan ödeme sisteminin güvenilirliği kontrol edilmelidir.
- Sitenin sosyal medya sayfaları (Facebook vb.) kontrol edilerek güncelleme yapılıp yapılmadığı kontrol edilerek takipçi sayısına dikkat edilmelidir. Ayrıca yapılan yorumların olumlu olup olmadığı sorgulanmalıdır.
- Nadiren karşılaşılan bir durumda olsa bazı online alışveriş siteleri müşterilerine web sitesinden alışveriş yapabilmeleri için bir şifre gönderip

yeni bir kullanıcı adı ve yeni şifre oluşturulmasını talep etmektedirler. Şifreler genellikle 4 ila 10 karakter arasında sınırlandırılır. Tüketici bu gibi durumlarda asla kendi adını, çocuklarının adını veya eşinin adını şifre olarak kullanmamalıdır. Birbirini tamamlayan veya sıralı bir şekilde takip eden şifreler kesinlikle kullanılmamalıdır. Örneğin "1234" bir şifre değildir. Ya da kullanıcı adının sucuk, sosis, salam vb. seçildiği durumlarda şifre olarak yumurta seçilmemelidir. Ayrıca harf ve sayı her zaman bir arada ve aynı şifre ikinci kez kullanılmamalıdır.

5. E-TİCARET ÖDEMELERİNDE SATICI PERSPEKTİFİ VE DOLANDIRICILIK

İnternetin gelişimi çevrimiçi tüccarlar ve finans sektörü üzerinde derin etki yaratmıştır. İnternetin tüccarlara, yeni müşterilere erişimi kolaylaştırdığı tartışmasız kabul edilir. Fakat aynı zamanda savunmasızlıklarını da aynı oranda arttığı görülür. Çünkü çevrimiçi satışlarda silahla bir mağazaya girmeye gerek yoktur. Online ortamlarda dolandırıcılar, bir başkasının kimliğini çalıp, çalıntı kimliği kullanarak alışveriş yapabilmektedir. Bu anlamda internetin genel şeffaflığı bir suistimalcinin saldırıya geçme hızını da arttırmıştır. Bu sebeple çevrimiçi ortamlarda tüccarlar için güvenlik ve dolandırıcılık konuları her geçen gün daha karmaşık bir hâl almaktadır. İnternette yapılan işlemlerde, sistemin açıklarından istifade edilerek sahtekârlık ya da dolandırıcılık yapılması olayına "Fraud" denilmektedir (Demir, 2016: 117).

Online satıcılar için güvenlik sadece ödeme işlemlerinin güvenliğini sağlamaktan ibaret değildir. Satıcılar aynı zamanda bağlantı güvenliğinin, transfer güvenliğinin ve hassas tüketici verilerinin güvenliğinin sağlanmasından da sorumludur. Bu noktada güvenlik sorunu ve dolandırıcılık online satıcılar için sadece parasal kayıp olmanın çok daha ilerisinde bir konudur. Çünkü böyle bir skandal karşısında online satıcı, kısa ve uzun vadede öncelikli olarak marka değeri erozyonu yaşayacaktır. Bununla birlikte yine de online satıcı veya tüccarlar; tüm dolandırıcılıkların önüne geçebilmek için gerekli olan güvenlik maliyetlerine yönelik tavır alıp para kaybetmek istememektedirler. Örneğin tüccarlar genellikle kredi kartı sahtekârlığından korunmazlar. Satıcıların bu tutumları değerlendirmeye alındığında yaşanan marka değeri ve itibar kaybının ardından, üstüne para ödeyerek güvenlik maliyetlerini arttırmanın bir anlamı yoktur. Konuyla ilgili bazı istisnalar vardır.

Örneğin Visa ödemeler sistemi uygulamalarına ait "Verified by Visa" programı gibi bir programdan muzdarip olan çok sayıda başarılı hacker bulunmaktadır. Çevrimiçi satıcılar ödeme sayfalarında bu programlar gibi geçerli yetkilendirmeler alarak kredi kartı sahtekârlıklarına karşı korunabilmektedirler. (https://visa.com.tr/bireysel-kartlar/guvenli-internet-alisverisi/verified-by-visa, bkz. 2018). Bu tür güvenli uygulamalara bir başka örnek; Visa Checkout(https://www.visa.com.tr/bizimle-isbirligi-yapin/payment-technology/visa-checkout.html, bkz. 2018) uygulamasıdır. Büyük marka değerlerine sahip satıcılar bu tür uygulamaları zaten kullanır. Fakat özellikle küçük ve orta ölçekli işletmeler, güvenlik konusunda daha istekli davranmalıdır. Online satıcılar ve finans kurumları için bir diğer zorluk, bir tüketicinin gerçekten söylediği kişi olup olmadığının tespit edilmesidir. Bu tespitin yapılması sadece dolandırıcılığı önleme meselesi değil aynı zamanda yasal bir zorunluluktur (Montague, 2011: 32-34).

Online satıcıların sahtekârlık önleme teknikleri arasında, adres doğrulama sistemleri (AVS) ve kart güvenlik kodu (CSC, CVV) programları yer almaktadır. Adres doğrulama sistemleri kredi kartıyla sağlanan bir araçtır. Bu kontrol sistemi, online satıcının isteği üzerine alıcının adresinin bankada kayıtlı olup olmadığını görmek için kullanılan kredi kartı üzerindeki yetkilendirmenin bir parçasıdır. Alıcının adresi, dosyadaki adrese göre banka tarafından kontrol edilir. Fakat AVS'nin güvenilirliği şüphelidir. Konuyla ilgili birçok geçerli sebep vardır. Örneğin tüketicinin bir online satıcıya verdiği fatura adresi farklı olabilmektedir. Ayrıca adres doğrulama sistemi olan AVS, sık seyahat eden tüketicilerin kayıtlarını güncel tutamaz bu nedenle bir aile üyesinin adresini kayıt adresi olarak kullanır.

Sonuç olarak AVS, hileli faaliyetler için iyi bir gösterge değildir ve yanlış uygulandığında online satıcının %5 ile %28 arasında yanılmasına sebep olur. Bununla birlikte AVS sadece bankalardan temin edilebilmektedir. Online satıcıların AVS hakkında konuşan yazılım veya ağ geçitleri temin etmeleri gerekmektedir. Aktarılan AVS uygulaması, Birleşik Krallıkta uygulamadadır. Amerika Birleşik Devletlerinde uygulamada farklılıklar görülür. Birleşik krallıkta AVS ve kart güvenlik kontrolü aynı talep kodu ve aynı cevap koduyla karşılanmaktayken ABD'de AVS ve kart güvenlik kodu ayrılmıştır. Satıcı yapmış olduğu ödeme karşılığında AVS'nin kullanımı ve uygulanmasıyla ilgili işlemciyle bağlantıya geçer. AVS

kontrolü genellikle yetkilendirme aramasının bir parçası olarak e-ticaret motoru üzerinden gerçek zamanlı olarak yapılır.

Özetle banka ile online siparişi alan satıcının AVS adresleri üzerinde tam bir eşleşme varsa daha az risk var demektir. Bu noktada online satıcılara, AVS ile birlikte Gelişmiş Adres Doğrulaması (AAV +) yapmaları tavsiye edilmektedir. Gelişmiş adres doğrulaması, verileri doğrulamak için geriye doğru arama yapmak anlamına gelmektedir. AVS'nin ötesine geçerek daha etkin bir kontrol sağlar (Montague, 2011:127-133). Kart güvenlik düzenleri içerisinde üç veya dört haneli bir sayı olarak yer alan CV, CVV2 numaraları ise kart güvenlik kontrollerini sağlamaya çalışır. Hileli girişimlerin sayısını azaltarak, kart sahtekârlıklarının önüne geçmeye çalışan bir uygulamadır. American Express kartları için kredi kartı numarasının üstünde ya da MasterCard ve Visa için arka yüzde bulunur. Amaç doğrulanan kartla birlikte tüketicinin de doğrulanmasıdır. Kart güvenlik kontrolünü çalıştırmak için ekstra bir maliyet yoktur (Montague, 2011: 137-138).

6. ÇEVRİMİÇİ HUKUKTA GÜVENCE VE SORUMLULUK

Günümüzde çeşitli güvenlik sorunlarıyla birlikte internet üzerinden ticarette hızla büyümeye devam etmektedir. Bununla birlikte ancak tüketicilerin güvenlik kaygılarını azaltan ve teknolojiyi yakından takip eden firmaların e-ticaret pazarında yer edinmeleri mümkün olmaktadır. E-ticaret pazarında en önemli konulardan biri ise tüketicilerin kişisel verilerinin korunması alanındaki kanuni düzenlemelerin yapılmasıdır. Türkiye'de kişisel verilerin korunması kanun tasarısı Türkiye Büyük Millet Meclisi Genel Kurulunda 2016 yılında kabul edilerek yasalaşmıştır. Yasayla birlikte tüm kurum ve kuruluşların, kişisel bilgilerin işlenerek kaydedilmesinden sorumlu olacak bir personel görevlendirmesi, yasayla getirilen kurallara uymayanlara ise yüksek para cezalarıyla birlikte 6 aydan 3 yıla kadar hapis cezası verilmesi hususunda yasal çerçeve belirlenmiştir (Angün, 2016: 65).

6.1. Kişisel Verilerin Korunması

Kişisel verilerin korunmasının tarihsel gelişimi incelendiğinde süreç ilk olarak 1948 Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesiyle başlamış 2011 yılında Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)'nün Gizliliğin korunması ve Sınır Ötesi Kişisel Veri Akışına İlişkin Rehberin (Guidelines on the Protection of

Privacy and Transborder Flows of Personel Data) hazırlanmasına kadar gelişimini tamamlamıştır. Kişisel verilere ilişkin son düzenleme ise 2016 yılında AB Komisyonu tarafından kabul edilen ve 2018 yılında yürürlüğe giren Veri Korunmasına İlişkin Genel Düzenlemelerdir (The General Data Protection Regulation).Türkiye'de ise kişisel verilerin korunmasına yönelik düzenlemelerin temelini öncelikli olarak anayasalar sonrasında uluslararası anlaşma ve sözleşmeler oluşturmaktadır. Ayrıca konuya ilişkin detayların düzenlenmesinde kanun, yönetmelik ve tebliğ gibi ikincil düzenlemelerde mevzuatta yer almaktadır.

Türkiye'de özellikle bankacılık sektöründe kişisel verilerin korunmasına yönelik çalışma bulunmaması, bankacılık sektöründe kişisel verilerin korunmasına yönelik çalışmaların araştırmacılar tarafından değerlendirilmesi gereken bir konu olduğunu göstermektedir. Türkiye'de bankaların Kişisel Verilerin Korunması Kanuna uyum sağlama yükümlülüğü bulunmaktadır. Fakat ülkeler arası kişisel verilerin tanımlanması ve sınıflandırılmasında farklılıklar bulunduğu tespit edilmiştir. Küreselleşme ve teknolojik gelişmelerin etkisiyle birlikte özellikle uluslararası düzeyde iletişim ve işbirliğinin artması sonucuna bağlı olarak yakın gelecekte kişisel verilerin tanımlanması, depolanması ve saklanması adına yeni gelişmelerin yaşanması beklenmektedir. Bu süreçte özellikle bankalar söz konusu süreci yakından takip etmelidir (Kartal, 2018: 5-15).Kişisel verileri koruma kanununda düzenlemeye alınan bir diğer konu ise "hassas veriler ve bu verilerin işlenmesi"dir. Bu amaçla Avrupa veri koruma kanunlarında, hangi verilerin hassas veri sayılacağı ve bunların hangi istisnai haller altında işleneceği belirlenerek özel bir rejime tabi tutulmaktadır. *Avrupa Birliği Veri Koruma Direktifi'nin 8. Maddesinin 1. Fıkrasında hassas veri türleri olarak; Irksal ve etnik köken, siyasi görüş, dini ve felsefi inanç, sendika üyeliği, sağlık durumu, mahkûmiyet ve suçlar gibi veriler kişilerin hassas verileri olarak kabul edilmiştir*.

Özellikle Avrupa Mahkemeleri ve veri koruma otoriteleri, hassas verileri işleyen şirketlerin amaçları hakkında veri sahiplerini ayrıntılı olarak bilgilendirmeleri konusunda sert davranmaktadırlar. 2000 tarihli Hollanda Veri Koruma Kanunda, hassas verilerin işlenebileceği durumlar ayrıntılı olarak belirtilmiştir. Ayrıca bazı ülkelerin mevzuatları, hassas verilerin işlenmesinden önce Ulusal Veri Koruma Otoritesinden izin alınmasını zorunlu kılmaktadır. Örneğin Danimarka'da hassas verilerin sisteme işlenmesinden önce Veri Koruma Otoritesinden ön izin

istenmektedir. Örneğin Fransız veri koruma otoritesi (CNIL) sağlıkla ilgili internet sitelerini denetlemiş fakat bu sitelerin, veri koruma mevzuatının gerekliliklerini yerine getirmediklerini tespit ederek konuya bazı ilkelerle açıklık getirilmiştir. Bu ilkeler şu şekilde özetlenmektedir. Belirlenebilir bir kişiyle ilgili bir sağlık verisi, veri sahibi rıza gösterse bile satılamaz ve satın alınamaz. Bireyin sağlıkla ilgili bir anket doldurması halinde bu veriler sigorta şirketlerine, bankalara ve işletmelere verilemez. Kamu otoriteleri bu verilerin gizliliğini güvence altına almak amacıyla sağlıkla ilgili internet siteleri üzerinde sıkı denetimler gerçekleştirmelidir. Günümüzde bilim ve teknolojinin ilerlemesi sonucunda biometrik sistemlerin kullanımının artması ve DNA veritabanlarının oluşumu vb. gelişmeler ülkeleri hassas veri türlerini yeniden gözden geçirmeye ve kişisel verileri koruma kanunlarını güncellemeye mecbur bırakmaktadır (Kaya, 2011: 317-332).

6.2. Türkiye'de Kişisel Verilerin Korunması Kanunundan Doğan Tüketici Hakları Nelerdir?

6698 Kanun numaralı 24/03/2016 tarihinde kabul edilerek yasalaşan 07/04/2016 tarihinde Resmi Gazetede yayımlanan; Kişisel Verilerin Korunması Kanunu kapsamında vatandaşlar kişisel verilerin;

a) İşlenip işlenmediğini öğrenme,

b) Kişisel veri işlenmişse, buna ilişkin bilgi talep etme,

c) İşlenme amacını ve amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde ve yurt dışında kişisel verilerin aktarıldığı 3. kişileri bilme,

d) Kişisel veri eksik ve yanlış işlenmişse düzeltilmesini isteme,

e) KVKK (kişisel verilerin korunması kanunu)'nun 7. Maddesinde öngörülen şartlar çerçevesinde silinmesini ve yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi nedeniyle kişinin kendisi aleyhine ortaya çıkan bir sonuca itiraz etme,

ğ) KVKK' ya aykırı olarak kişisel verilerin işlenmesi sebebiyle zarara uğranılan durumlarda zararın giderilmesini talep etme haklarına sahiptirler (http://www.mevzuat.gov.tr, 2019).

Türkiye'de kişisel verilerin korunmasına yönelik yasal mevzuat çalışmalarında Avrupa Birliği Veri Koruma 95/46/EC Direktifinden esinlenilmiştir. Bu direktif Türkiye'nin kişisel veri politikalarının oluşturulmasında itici bir faktör olmuştur. AB'ye tam üyelik çerçevesinde açılan birçok fasıl, veri güvenliğine ilişkin yükümlülük ve hakları içermektedir. Konu bu yönden değerlendirmeye alındığında Türkiye'de kamu güvenliği ve düzeninin sağlanmasına yönelik politikaların uygulanmasında kişisel verilerin korunmasına yönelik güvenlik ve özgürlük dengesinin gözetilmesi çok önemlidir (Kutlu ve Kahraman, 2017: 59).

6.3. Avrupa'da Çevrimiçi Koruma ve Gizlilik

Birleşik Krallıkta elektronik ortamda düzenleme yapmak üzere tasarlanmış AB mevzuatı paketinin bir parçası olan AB'deki iletişim ağları ve hizmetleri, Gizlilik ve Elektronik İletişim (AB Direktifi) 2003 yılında uygulamaya alınmıştır. 2003 düzenlemeleri ile veri koruma mevzuatı çerçevesi; telekomünikasyon, yeni teknolojiler ve gelişen teknolojilerle birlikte kişisel verilerin işlenmesini içeren alanlara odaklanmıştır. 2003 yönetmenliği ve direktifi arka planda Avrupa mevzuatından türetilmiştir. Amaç üye devletlerin elektronik iletişim sektöründeki yasalarını uyumlaştırmaktır. Bu iletişim yasasını AB gurubunun büyük bir bölümü uygulamaya almıştır. Örneğin, doğrudan pazarlama hizmetinde bulunan bir şirketin, tüketicinin kişisel verilerinin (cep telefonu numarası vb) nasıl işleneceği adil ve yasal kullanım hakları bu yasa ile denetim altına alınmıştır. Düzenlemeler spam e-postaları engellemek ve işletmelerin elektronik pazarlarda mal ve hizmetlerini etkin bir şekilde tanıtılabilmesi için etkin bir şekilde kullanılmaktadır. 2003 Elektronik posta yönetmeliği özellikle işletmelerin nasıl çalıştığını düzenleyen hükümleri içermektedir. Elektronik yollarla gönderilen pazarlama mesajlarına ilişkin e-posta mesajları, Birleşik Krallıkta pazarlamacılar üzerinde önemli bir etkiye sahiptir. Ayrıca çerezlerin kullanımı ve konum verileri üzerinde etkin bir denetim mevcuttur.

Avrupa Doğrudan Pazarlama Federasyonu'nun (FEDMA) baskısı sonucunda 2003 yönetmenliğinde son kullanıcı çerez kullanım fonksiyonları belirlenmiştir. 2003 Yönetmeliğinde bir diğer önemli düzenleme konum verilerinin işlenmesiyle ilgilidir.

Müşterilerinin konumlarının, seyahat yönlerinin ve lokasyon verilerinin kaydedildiği durumlarda kişilere lokasyon bazlı faydalı bir içerik sunulabilmektedir. Fakat yine de konum verilerinin işlenmesindeki amaç ve süre ile verilerin üçüncü bir tarafa aktarılıp aktarılmayacağı konusunda düzenlemelere gidilmiştir (Brown, 2005: 71-77).

6.4 Ulusal ve Uluslararası Çevrimiçi Ticarette Tüketici Şikayet Merkezleri

Ulusal alanda Gümrük ve Ticaret Bakanlığınca 2015 tarihinde, Ticari İletişim ve Ticari Elektronik iletiler hakkında resmi gazetede yayınlanan yönetmelikle birlikte, elektronik iletişim araçlarıyla yapılan ticari iletişime dair bilgi verme yükümlülüklerine ve ticari elektronik iletilerde uyulması gereken hususlara ilişkin usul ve esaslar düzenlenmiştir. Bu yönetmelikte gerçek ve tüzel kişilerin mal ve hizmetlerini tanıtmak, pazarlamak ya da işletmesini tanıtmak veya bunları başkaları adına yapmak amacıyla elektronik iletişim araçlarıyla yapılan her türlü ticari iletişimi kapsamaktadır. 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanuna Dayanılarak hazırlanan bu yönetmelikle şikâyet başvuruları, elektronik ortamda e-Devlet kapısı veya Bakanlığın internet sitesi üzerinden veya yazılı olarak şikâyetçinin ikametgahının bulunduğu yerdeki il müdürlüğüne yapılmaktadır (http://www.resmigazete.gov.tr, 2018). Ayrıca T.C. Ticaret Bakanlığı Ticari Elektronik İleti Şikâyet Sistemi ile e-Devlet üzerinden şikâyette bulunulabilmektedir https://tiss.gtb.gov.tr/, bkz. 2018).

Uluslararası alanda ise Uluslararası Tüketicinin Korunması ve Uygulama Ağı'nın bir girişimi olan (www.econsumer.gov, 2018) sitesi aracılığıyla çevrimiçi uluslararası dolandırıcılık bildirimlerinde bulunulmaktadır. Sitenin tüketici şikâyetlerine konu olan ülkelerin dağılımı incelendiğinde; 1 Temmuz- 30 Eylül, 2018 tarihleri arasında tüketicinin bulunduğu ülkeye göre şikâyetlerde 3.491 tüketici şikâyetiyle ABD ilk sırada, 485 şikâyetle Fransa 2. sırada, 430 şikâyetle Hindistan 3. sırada, Türkiye ise 92 şikâyetle 9. sırada yer almaktadır. Şirketin bulunduğu ülkeye göre tüketici şikâyetleri sıralandığında ise 1.451 şirket şikâyetiyle Çin ilk sırada, 1.362 şirket şikâyetiyle ABD ikinci sırada, 655 şirket şikâyetiyle Birleşik Krallık üçüncü sırada yer almaktadır (https://www.econsumer.gov/tr/ComplaintTrend#crnt, 2018).

Econsumer.gov üzerinden uluslararası dolandırıcılık vakaları için bildirimde bulunulabilmektedir. Bugün 36 ülkede bulunan tüketicilerin korunması, internet dolandırıcılığının önlenmesi ve sınır ötesi e-ticaret şikâyetlerini alan ve paylaşan site, tüketicinin güven düzeyini artırmak amacıyla kurulmuş olup Birleşik Devletler Federal Ticaret Komisyonu tarafından Tüketici İzleme Ağı platformu üzerinden hizmet sunmaktadır. (https://www.econsumer.gov/tr/AboutUs#crnt, 2018). Sınır ötesi çevrimiçi alışverişlerde yasal çözüm yolları, ülkelere göre farklılık göstermektedir. Bu nedenle sınır ötesi çevrimiçi alışverişlerde uyuşmazlık ve sorun yaşandığı durumlarda, site herhangi bir yasal yaptırımda bulunmadan şikâyetin hızlı ve ucuz bir yolla çözüme kavuşturulabileceğini iddia etmektedir. Web sitesi aracılığıyla atılabilecek adımlar şu şekilde sıralanmaktadır;

- Alternatif uyuşmazlık çözümü,
- Tüketici eğitimi,
- Satıcıyla iletişim kurabilmek,
- Ödeme kartı korumaları,
- Güven damgası
- Emanet hizmetlerinden faydalanabilmek

(https://www.econsumer.gov/tr/OtherSteps/OtherSteps/17#crnt, 2018).

6.5. Tüketici Mahremiyetinin Korunması

Tüketici mahremiyetinin koruması hususunda hangi aktörlerin sorumlu görüldüğü ve uygulanabilecek stratejiler yapılan literatür taramalarıyla belirlenmiştir. Tüketici mahremiyetinin korumasına yönelik yapılmış olan 32 adet bilimsel araştırmanın içerik analizinde en büyük sorumluluğun işletmelere düştüğüne dair yaygın bir kanı bulunmaktadır. Bununla birlikte ekosistem içerisindeki tüm aktörler değerlendirmeye alındığında tüketici mahremiyetinde sorumluluğun; devlet, tüketiciler, endüstri, çalışanlar, taraf kurumlar, eğitim verenler ve aileler tarafından korunması gerektiğine dair görüş birliği bulunmaktadır. Diğer taraftan tüketici mahremiyeti nasıl korunmalıdır? Sorusuna yanıt arandığında yapılan çalışmaların büyük çoğunluğunda ilk sırada işletme standartları yer almaktadır. Tüketici mahremiyetini koruma yöntemleri arasında işletme standartlarını takip eden koruma yöntemleri arasında; yasal yollar, tüketici eğitimi, endüstri standartları, iletişim ve

diğer önlemler bulunmaktadır. Özetle tüketicilerin kişisel verilerinde mahremiyet endişelerinin giderilmesinde en büyük görevin işletmelere düştüğü görülmektedir. Bu noktada işletme politikalarının yasalara uygun, açık ve anlaşılır olması tüketici hassasiyetinin belirlenmesinde kilit unsurlardır. Tüketicilerin büyük çoğunluğu ise konu hakkındaki düzenlemelerin devlet tarafından yapılması gerektiğini düşünmektedir. Konuyla ilgili her ne kadar çalışmalar yürütülmekte olsa da uygulamada yaşanan problemlerin daha kolay aşılabilmesi için yasa koyucuların yanında, konuya taraf olan kurum ve kuruluşların konuyla ilgili çabalarını artırarak daha aktif rol alması büyük önem arz etmektedir. Ayrıca tüketici mahremiyetinin korunmasında en önemli unsurun yine tüketicinin kendisi olduğu bilinmelidir. Bu nedenle tüketicilerin kişisel verilerin korunmasına yönelik bilgilendirilmesi ve farkındalık çalışmalarının artırılması tüm tarafları tetikleyici bir etki yaratacaktır (Aydın ve Marangoz, 2018: 481-483).

6.6. Türk Ceza Kanununda Bilişim Suçları

Türk Ceza Kanunu'nda, bilişim suçu kavramı ilk kez 765 sayılı Türk Ceza Kanunu'nda değişiklik ve ekleme yapan 06.06.1991 tarih ve 3756 sayılı kanunla literatüre girmiştir. Sonraki yıllarda yapılan düzenlemeler 765 sayılı Türk Ceza Kanunu'nu tamamen ortadan kaldıran ve 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı yeni Türk Ceza Kanunu'ndaki hükümler uygulanmaya başlayıncaya kadar yürürlükte kalmaya devam etmiştir. Günümüzde şu anda halen 5237 sayılı Türk Ceza Kanunu'ndaki düzenlemeler geçerli olmakla birlikte uygulama alanında bazı durumlarda yetersiz kaldığı düşünülmekte olsa dahi kısmen oturmuş durumdadır. (Aktaran: Akarslan, 2011: 18) Bilişim Suçları Türk Ceza Kanunu'nun ikinci kitabının "Topluma Karşı Suçlar" başlıklı üçüncü kısmında ve "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde 243, 244, 245 ve 246. maddelerinde düzenlenmiştir(http://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm, 2019).

Türk Ceza Kanununun 243'üncü maddesinin birinci fıkrasında "*bir bilişim sisteminin bütününe ya da bir kısmına, hukuka aykırı olarak girme ve orada kalmaya devam etme*" tanımlaması yapılmıştır. Aynı maddenin üçüncü fıkrasına geçildiğinde ise "*bu saldırı nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi"* durumunda cezanın artırılması gerektiği yazılmıştır. Bir internet sitesine ücret vermeksizin ulaşılması, ücretsiz üyelik istenen bir alana ise üyelik olmaksızın

girilmesi veya bir internet sitesinin yönetim paneline yetkisiz ulaşılması ve benzeri faaliyetlerde bu madde kapsamında değerlendirmeye alınmaktadır. Türk Ceza Kanununun 244'üncü maddesinin birinci fıkrasında, "*bir bilişim sisteminin işleyişini engelleme veya bozma*" ve ikinci fıkrasında "*bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilemez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme"* eylemleri düzenlenmiştir. 244. Madde, 243. Maddeye göre daha ağır cezai sorumluluk içermektedir. Bu bağlamda DOS/DDOS saldırıları incelendiğinde, erişebilirlilik ihlalinin çok sık yaşandığı görülmektedir. Bu saldırılarda site sayfalarına mesajlar bırakılarak değişiklik yapılması ise veri bütünlüğünün ihlali anlamına gelmektedir. İnternet sitelerine yapılan saldırı sonrasında, kişilere ait kayıtlar, yazışmalar, fotoğraflar, sosyal paylaşımları içeren her türlü video ve benzeri kayıtlar gibi özel hayatın gizliliğinin ihlali durumunda ise TCK'nın 134. Maddesi olan *"özel hayatın gizliliğini ihlal suçu*" düzenlenmiştir. Burada dikkat edilmesi gereken en önemli nokta verinin elde edilmesinin suçun oluşması için yeterli olduğudur. Bununla birlikte verinin 3.kişilerce ifşa edilmesi durumunda ise cezada artırıma gidilmektedir.(Çakır, Yalçın ve Kılıç, 2015: 163).

Özetle, Türk Ceza Kanunu Madde 243'e göre hukuka aykırı olarak bilişim sistemine girme suçunun cezası şudur;

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranında indirilir.

(3) *Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur*.
(http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, 2019: 9024).

Türk Ceza Kanunu Madde 244'e göre sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun cezası şudur;

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başla bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fillerin bir banka veya kredi kurumuna ya da bir kamu kurum ve kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) *Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur*

(http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, 2019: 9024).

Türk Ceza Kanunu Madde 245'e göre banka veya kredi kartlarının kötüye kullanılması suçunun cezası şudur;

(1) Bir başkasına ait banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya bir başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır ceza gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya alt soyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) *Birinci fıkra kapsamına giren fiillerle ilgili olarak bu kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.* (http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, 2019: 9024, 9024-1).

Türk Ceza Kanunu Madde 245'e göre yasak cihaz ve program kullanımına yönelik ceza düzenlemesinde; "*Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır*" hükmü yer almaktadır. (http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, 2019: 9024-1,)

Ülkemizde bilişim suçlarıyla ya da bir diğer adıyla siber suçlarla mücadelede yaşanan başlıca güçlükler değerlendirmeye alındığında ana başlıklar; yasal boşlukların bulunması, usule ilişkin mevzuatın yetersizliği, siber ortamda kolluk kuvvetlerinin yetkilerinin belirsizliği, teknik uzman eksikliği, siber ortamda yargılama yetkilerinin belirsizliği, siber saldırganların iadesinde yaşanan güçlükler olarak sıralanmaktadır (Ünver, Canbay ve Mirzaoğlu, 2009: 27-29).

7. İLGİLİ LİTERATÜR ÇALIŞMALARI

Sosyal mühendislik, siber güvenlik ve online alışveriş ile ilgili literatür çalışmaları Tablo 6 ile görselleştirilmiştir.

Tablo 6. İlgili Literatür Çalışmaları

Çalışmanın Başlıkları	Araştırmacıların İsimleri ve Çalışmanın Tarihi	Örneklem	Araştırmanın Sonuçları
1.Türkiye'de Siber Güvenlik Bilinci ve Sosyal Mühendislik Ataklarına Karşı Savunma Önlemlerinin Geliştirilmesi.	MEHMET ALİ BARIŞKAN (2017)	-19 sorunun sorulduğu 18-23 yaş arası bireylere uygulanan genel bilgi anketinde, katılımcıların sosyal mühendislik saldırılarına karşı açıklık durumları sorgulanmıştır.	-Katılımcıların çoğunluğunun, siber güvenlikte giriş seviyesinde bilgiye sahip olduğu tespit edilmiştir. Ayrıca sosyal mühendislik ataklarından çok az kişinin haberdar olduğu sonucuna ulaşılmıştır.
2.İnsan Zafiyetlerini İstismar Ederek Yapılan Sosyal Mühendislik Saldırılarının, Siber Güvenlik İle İlişkilendirilmesi: Türkiye Örneği	ADEM TOSUN (2015)	-Sosyal mühendislik saldırı türlerine karşı farkındalık düzeyinin belirlenmesi amacıyla gerçekleştirilen çalışmada, Türkiye'nin farklı bölgelerinde yaşayan 3994 kişiye sosyal mühendislik saldırı tekniklerinden olan kimlik avı tekniğiyle beraber kişisel iletişim kurma ve davranış teknikleriyle ustaca gerçekleştirilen sosyal mühendislik saldırılarında bulunulmuştur.	Saldırgan, saldırı tekniğini kurbanına göre uyguladığında yani doğru zamanda doğru yerde, kişiye göre değişen doğru saldırı tekniğiyle %59,5 başarılı olacaktır. Araştırmada ortaya çıkan en başarılı saldırı tekniği temastır. Diğer tekniklerin başarı sırası sırasıyla; dilek, yem ve kimlik avıdır. Saldırı esnasında kullanılan kişisel iletişim tekniği saldırının başarıyla sonuçlanmasına neden olmuştur. Yani bir sosyal mühendis tuzak kurup beklemek yerine saldırının kontrolünü ele geçirmek istemektedir. Bu nedenle, insanoğlunun korku, dikkatsizlik, yardım ve konfor bölgesi gibi zafiyetleri kullanılmıştır. Çalışmada korku zafiyeti baskın çıkmıştır.
3.The Use of Usable Security and Security Education to Fight Phishing Attacks	SUNİL CHAUDHARY (2016) UNIVERSITY OF TAMPARE	Likert ölçekli yapılan değerlendirme anketi ile yazar, bilgi güvenliğinde, öğretme ve öğrenmede yaşanan problemlere ilişkin bilgi güvenliği müfredatının geliştirilmesine hizmet edecek pilot bir anket kullanmıştır. Katılımcılar bilgisayar dalında yüksek lisans öğrencileridir Güvenlikte öğretme ve öğrenme yöntem ve materyallerin özellikleri değerlendirmeye alınmıştır.	Öğrencilerde kavram yanılgıları bulunmaktadır. Saldırganlar tarafından sömürülebilirler. Güvenlikte becerilerini ve yetkinliklerini geliştirmek için güncel bir güvenlik müfredatı kullanılmalıdır. Müfredatın değişen ve gelişen teknolojilere karşı esnek olması gerekir. Güvenlik müfredatı tasarımında kültürel boyutun dikkate alınması gerekir. Güvenlik müfredatı tasarımında kişilik özellikleri ve cinsiyette önemlidir. Bu öğrencilerdeki zayıflığı ortaya çıkartacaktır.
4. Hacking the Human Operating the Human Operating System: The Role Of Social Engineerng within Cybersecurity	SAMANİ R. AND MCFARLANDC (2014)	Sosyal mühendislik saldırılarının yaşam döngüsü üzerine model çalışılmıştır. Araştırmada yaşam döngüsü 4 aşamaya bölünmüştür. Araştırma, kanca, oyun ve çıkış.	Anlatılan döngü çerçevesinde sosyal mühendislik saldırılarının her geçen gün daha karmaşık hale geldiği savunulmuştur.
5.Web Security	SUHEİL SHAHYAR (2005) VERİSİGN UK	Kimlik avı saldırı modeli oluşturulmuştur. Kimlik avı saldırısında 3 temel aşama tespit edilmiştir. Hazırlık, saldırı ve veri kurtarma.	Veri sahtekarlığı ve güvenlik saldırıları arasındaki iki veri analizinde yüzde 47 korelasyon bulunmuştur. Çoğu web satıcısı sınırlı miktarda istihbarat almaktadır. Saldırganlar kimlik hırsızlığını bir meslek hale getirmişlerdir. Bu meslekten her geçen gün daha fazla kazanç sağlayacaklardır.

Çalışmanın Başlıkları	Araştırmacıların İsimleri ve Çalışmanın Tarihi	Örneklem	Araştırmanın Sonuçları
6.Explore Awareness of Information Security Insights from Cognitive Neuromechanism	YONGHUİ DAİ, DONGMEİ HAN, TİALİN HAN, XİNGYUN DAİ (2015)	İnsanların bilgi güvenliği konusunda farkındalıklarını ve bilişlerini objektif değerlendirmek için çevrimiçi finansal ödemelerde elektrofizyolojik sinyallerin analizine ilişkin analize dayalı deneysel bir çalışma yürütülmüştür. 12 sağlıklı yetişkin üzerinde çalışılmıştır. Bu yetişkinlerin 4'ü bilgi güvenli eğitimi almış, 8'i herhangi bir eğitim almamıştır. İnsanların bilgi güvenliği bilincini araştırmak için yapılan denemede 9 deney sahnesi tasarlanmıştır. Testte deneklere bilgi güvenliği sahtekârlığı ile ilgili resimleri ve duydukları sözleri not alarak seçim yapmaları istenmiştir. Cep telefonlarına sahtekârlık metin mesajları ve çevrimiçi ödemelerde kullanılan sahtekârlık mesajları atılmıştır.	Elektroensefalogram (EEG) sinyalinin ve beta ritimlerinin, insanların çevrimiçi finansal ödemede, potansiyel riskleri algıladıklarını tespit etmek için bir işaret olarak değerlendirilebileceğini ve bu sinyallerin, bilgi güvenliği bilincindeki, bilişsel risk derecesine duyarlı olduğu tespit edilmiştir. Özetle EEG sinyalleri ile bilgi güvenliği farkındalığı ve bilişinin tanımlanması için gizli sorularla deneklerin reaksiyonu test edilmiştir. EEG sinyalleri insanların nesnel değerlendirilmesi için iyi bir yöntem sunmuştur.
7. Bilişim Öğrencilerinin Siber, Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği	ÖMER SIDDIK BUDAK(2015)	-Mesleki ve teknik liselerdeki bilgisayar ve bilişimle iç içe olan öğrencilerin siber suç farkındalığı araştırılmıştır. Evreni, Erzurum'da mesleki ve teknik liselerin bilişim öğrencileri oluşturmuştur.	Öğrencilerin internette saldırıya uğrama durumları ile siber suçları algılama ve aldıkları önlemler arasında anlamlı bir farklılık tespit edilmemiş, Siber saldırıların yapılması siber farkındalığı etkilememiştir.
8.Çevrimiçi (Online) Alışverişte Farklı Toplumların Riskleri Algılamasına Dair bir çalışma.	SERDAR ANGÜN (2016)	- Sosyal medya ve e-posta üzerinden, Türkiye ve ABD vatandaşlarına toplamda 512 anket doldurulmuştur.	-Türkiye ve ABD'deki kullanıcılar arasında tüketicilerin internet üzerinden alışverişte algıladıkları riskler değerlendirmeye alındığında büyük bir farklılık bulunmadığı ortaya çıkmıştır. ABD'deki kullanıcılar sanal kart kullanımını Türkiye'deki kullanıcılara göre daha riskli bulmaktadır. Türkiye'deki kullanıcılar sanal kartı, kredi kartına göre daha yüksek bir oranla güvenle kullanmaktadırlar.
9. Lise Öğrencilerinin Siber Duyarlılık, İnternet Bağımlılığı Ve Sosyal Değerlerinin İncelenmesi.	İSA KILINÇ (2012)	-Aralarında, Anadolu Lisesi, imam hatip lisesi ve meslek lisesi öğrencilerinin yer aldığı 774 öğrenciye anket yapılmıştır.	-İnternet bağımlılığı ve siber zorbalığa ilişkin duyarlılık arasında, anlamlı olabilecek düzeyde bir ilişki tespit edilememiştir. Siber duyarlılık puanı yüksek olan öğrencilerin, sosyal değerler puanı ve sosyal değerlerin alt boyutlarından olan sorumluluk, dostluk ve saygı puanı yüksek çıkmıştır.
10.Hizmet Sektöründe Online Alışveriş Davranışını Etkileyen Faktörler	MOHAMAD, EL-HASSAN (2016)	-Toplamda 301 Anket formu değerlendirmeye alınmıştır. Maribor Üniversitesinden (Slovenya) 101 Anket, Mersin Üniversitesinden 200 Anket.	-İki ülke arasında tüketici niyetlerinin veya alışveriş planlarının şekillenmesinde belirleyici bir etkiye sahip olan faktörlerin; güvenlik, güven ve kullanım kolaylığı olduğu tespit edilmiştir.

DÖRDÜNCÜ BÖLÜM

YÖNTEM VE UYGULAMA

1. ARAŞTIRMANIN ÖNEMİ VE AMACI

Günümüz teknolojisinde elektronik platformlardan sunulan mal ve hizmetlerin (internet bankacılığı, e-ticaret, e-fatura, e-bilet, e-devlet vs.) sayısı her geçen gün artmakta ve bu platformları kullanarak bilgi edinen veya alışveriş yapan tüketicilerin sayısı günden güne çoğalmaktadır. Bu durum beraberinde online platformlarda ulusal ve uluslararası düzeyde hizmet veren kurumların artmasına ve kötü niyetli saldırganların bu platformlara illegal erişim isteklerinin günden güne çoğalmasına neden olmaktadır (Gülmüş M, 2010: 3). İnternet yoluyla ticaretin başladığı zamanlardan günümüze kadar güvenlik sorunu tüketicilerin davranışlarında belirgin değişikliğe neden olmuştur. E-ticaret sitelerinde yaşanan güvenlik ihlâlleri nedeniyle tüketicilerin mali ve son derece hassas kişisel bilgileri manipüle edilir hale gelmiştir (Suh ve Han, 2003: 155). Online ticaretin gelişimiyle birlikte sahte banka web sitelerinin oluşturulması neticesinde birçok kişi mağdur edilmiştir. PandaLaps'ın 2010 raporu ile her hafta 57 bin sahte web sitesinin oluşturulduğu ortaya çıkarılmıştır (Aksoy ve Sever, 2012: 155,156).

Gelişen teknoloji ve ticaretle birlikle hayatımıza giren dijital araçları doğru kullanılmasını bilen kişi haklarına ve umumi ahlâk kurallarına dijital veya online platformlarda saygı duyan aynı zamanda bu araçları güvenlik ve sorumluluk bilinciyle doğru kullanmasını bilen kişilere dijital vatandaş denilmektedir. Özetle dijital vatandaşlık, teknolojiyi kullanan vatandaşların sorumluluk bilincine uygun davranış şekli olarak tanımlanmaktadır (Mosseberger, Tolbert ve McNeal, 2007: 1-19). Ticari risklerin en önemli başlığını dijital vatandaşların kişisel verilerinin istismar edilmesi sonucu oluşan sosyal mühendislik bir diğer adıyla kimlik hırsızlığı oluşturmaktadır. Sosyal mühendislik; online ve sosyal ağlarda kullanılan; şifreler, parolalar, e-postalar aracılığıyla kişisel bilgilerin başkaları tarafından illegal çıkar sağlanması amacıyla istismar edildiği dolandırıcılık yöntemidir (Çubukçu, A, Bayzan Ş, 2013: 154). Sosyal mühendislik saldırıları gizli olan kişisel bilgilere meşru erişim imkânı sağlamaktadır (Barışkan, 2017: 1). Bu saldırıların gün geçtikçe artmasının bir başka nedeni online ağların gizlilik politikalarında kullanılan güvenlik politikaları

bilgilerinin kullanıcılara anlaşılır bir şekilde aktarılmamasıdır (Yavanoğlu, U, Sağıroğlu, Ş, Çolak, İ, 2012: 26).

Çoğu insan online ağlarda hak ihlâllerinin teknik yollardan olduğunu düşünmektedir. Oysa teknik önlemlerle asla engellenemeyecek sosyal mühendislik saldırıları, online sistemleri istismar etmenin en iyi yollarından biridir (Tosun, A, 2015: 5). Çağımızın internet olanakları ile insanların yaşam standartları ve alışveriş alışkanlıkları değişmiştir. Dolayısıyla internet insan ihtiyaçlarını daha hızlı, ucuz ve pratik olarak karşılayan bir araç haline gelmiştir. Fakat siber suçlular, online sistemlerde çeşitli siber saldırı ve sosyal mühendislik aldatmaca yöntemleri ile tüketicilere çeşitli tuzaklar kurup kullanıcıların kritik önem düzeyine sahip kişisel bilgilerini ele geçirerek tüketicileri dolandırıcı sitelere yönlendirebilmektedirler (Şahinaslan ve diğerleri, 2013: 2).

Bilişim suçlarının büyük bir çoğunluğu insanlar üzerinden gerçekleşen aldatmaca yani sosyal mühendislik saldırıları ile siber saldırıların birlikte kullanılması sonucu ortaya çıkmaktadır. Bu saldırıları etkisiz hale getirebilmek insan faktörü üzerinde güvenli davranış bilincine ve farkındalığa dayanmaktadır (Şahinaslan, 2013: 7-78). Bilişim suçlarına yönelik atılacak en etkili adım ise online platformlarda alışveriş yapan tüketicilerin bilinçlendirilmesidir.

Bu noktada sorulması gereken araştırma soruları şunlardır;

1. Genç tüketicilerin siber güvenlik ile sosyal mühendislik farkındalıkları online alışveriş niyetlerini etkiler mi?
2. Genç tüketicilerin siber güvenlik farkındalıkları ile sosyal mühendislik farkındalıkları arasında anlamlı bir ilişki var mı?

Bu çalışmanın üç amacı bulunmaktadır. Birinci amaç; online ağlarda gerekli olan güvenlik bilgilerinin tüketicilere ve ticari işletmelere açık ve anlaşılır bir şekilde aktarılması ile güvenli toplumların oluşturulmasına katkı sağlamaktır. Bu doğrultuda online alışverişlerde tüketicilere ve ticari işletmelere, siber güvenlik ve sosyal mühendislik risklerini doğru yönetebilmeleri için gerekli olan taktikler ve tedbir amaçlı bilgiler aktarılmıştır. İkinci amaç; genç tüketicilerin siber güvenlik ile sosyal mühendislik farkındalıklarının online satın alma niyetleri üzerinde etkili olup olmadığının ortaya çıkarılmasıdır. Üçüncü amaç ise sosyal mühendislik ile siber güvenlik farkındalığı arasında anlamlı bir ilişki olup olmadığının belirlenmesidir.

2. ARAŞTIRMANIN VARSAYIMLARI VE SINIRLILIKLARI

Araştırmamızın bulguları Bandırma Onyedi Eylül Üniversitesindeki öğrencilerin konuyla ilgili; algı, bilinç, bilgi düzeyleri ve niyetlerini yansıtmaktadır. Araştırma anketinde yer alan soruların ve önermelerin ankete katılan öğrencilerin online alışveriş niyetlerinde, sosyal mühendislik ile siber güvenlik farkındalıklarını ortaya çıkarmak için yeterli olduğu varsayılmıştır. Araştırma verilerinin sadece anket yöntemiyle toplanmış olması araştırmada mülakat ve gözlem gibi tekniklerin kullanılmamış olması araştırmanın sınırlılıklarındandır. Ankette toplanan verilerin geçerliliği ve güvenilirliği anket tekniğinin özellikleri ile sınırlıdır. Ayrıca anket katılımcılarının sadece genç nüfusu temsil eden üniversite öğrencilerinden oluşması çalışmanın bir başka sınırlılığını oluşturmaktadır. Konuyla ilgili bundan sonra yapılacak çalışmalarda araştırmacılara yaş sınırının genişletilmesi ve orta yaş ile yaşlı nüfusu da kapsayacak şekilde çalışmalar yapmaları tavsiye edilir.

3. ARAŞTIRMANIN KATKILARI

Günümüzde yapılan ticari faaliyetlerin büyük bir çoğunluğunun dijital ortamlara kayması Türkiye'nin iç ve dış ticaret politikalarını sık aralıklarla güncellemesi gerektiği anlamına gelmektedir. Bugün yüksek oranda mobil cihaz kullanımı ve nesnelerin internetiyle birlikte internet kullanım oranlarının artması Türkiye'nin sahip olduğu yüksek genç nüfus oranı ile birlikte değerlendirildiğinde online ticaretin önümüzdeki yıllarda ülke ekonomisinde sağlayacağı itici gücün, ticari hayat üzerindeki etkisinin ne denli kuvvetli olacağı öngörülebilmektedir. Çağımızın gelişmiş ekonomileri, iç ve dış ticaret stratejilerini dijital ekonomilere dayandırmaya çalışmaktadır. Bu nedenle siber alana etki eden konularda yapılan tüm çalışmaların arttırılması ve teşvik edilmesi gerekmektedir. Bu tez çalışması, genç tüketicilerin online alışveriş niyetlerini, siber güvenlik farkındalıları ile sosyal mühendislik farkındalıklarını ortaya çıkarmıştır.

Yapılan çalışma; sosyal mühendislik, siber güvenlik ve online alışveriş kavramları ana başlıklar olmak üzere genel anlatımla online güvenlik ve online alışveriş disiplinlerinin birleştirilmesiyle ortaya çıkarılan orijinal bir çalışmadır. Online alışverişte güvenlik unsurlarını tek modelde açıklayan bu çalışma, çevrimiçi ortamlarda güvenli alışveriş yapabilmek için tüketiciyi bilinçlendirmektedir. Ayrıca çalışılan Yapısal Eşitlik Modelleme Analizi (YEM) ile oluşturulan Online Alışveriş

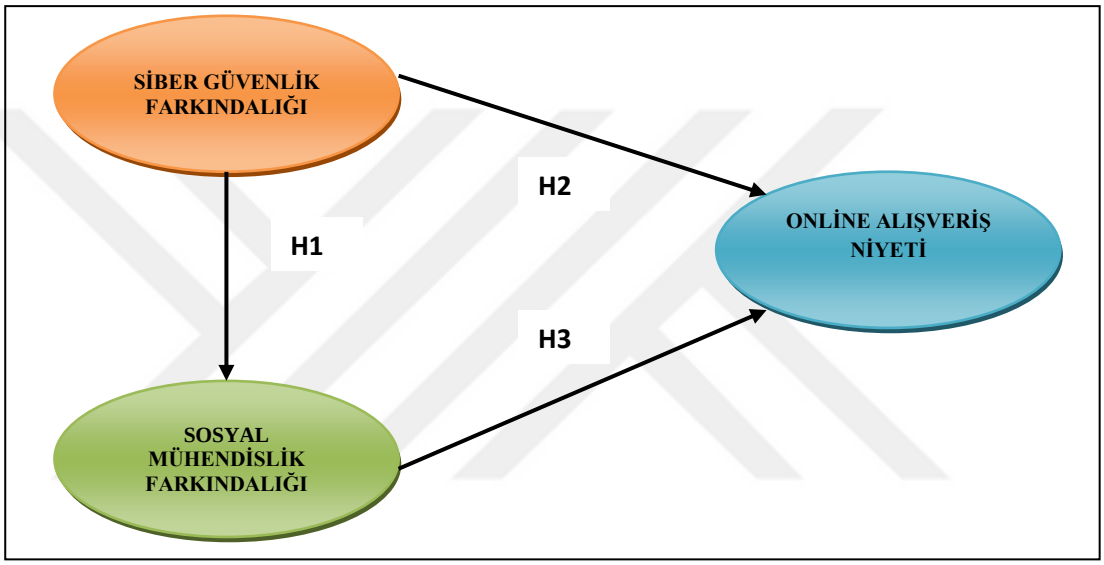
Güvenlik Modeli (OAGM) ile bundan sonra bu alanlarda yapılacak akademik çalışmalar için bir zemin oluşturmaktadır. Çalışma ilgili literatür ve internet araştırmaları neticesinde oluşturulan bilgilerle online tüketicilere ve ticari işletmelere siber güvenlik ve sosyal mühendislik ataklarıyla ilgili gerekli taktik ve tedbir amaçlı bilgileri aktararak tüketicileri ve ticari işletmeleri bilinçlendirmeye yönelik hazırlanmıştır. Çalışmada kurulan Online Alışveriş Güvenlik Modeli (OAGM) alanında çalışılmış ilk model olması sebebiyle özgündür. Bu model ile siber güvenlik ile sosyal mühendislik arasında daha önce tespit edilmeyen %65 oranında güçlü bir ilişki tespit edilmiştir. Türkiye'de özellikle sosyal mühendislik alanında yapılmış sınırlı sayıda çalışma bulunmaktadır. Aktarılan tüm bilgiler ışığında, bu çalışmanın ilgili alan yazına katkı sağlayacağı düşünülmüştür.

4. ARAŞTIRMANIN MODELİ VE HİPOTEZLERİ

Araştırmada; online alışveriş ile siber güvenlik ve sosyal mühendislik alanlarında yapılan literatür çalışmaları ayrı ayrı incelenmiştir. Şekil 13 ile gösterilen Online Alışveriş Güvenlik Modeli (OAGM) araştırmada ortaya çıkmış olan modeldir. Model online alışveriş niyeti ile siber güvenlik ve sosyal mühendislik farkındalığı değişkenlerinin kendi aralarında var olan ilişkisel bağlarını tespit ederek ortaya çıkaran orijinal bir modeldir.

Bazen bir araştırmada birden çok amaç bulunabilmektedir. Bu araştırma amacı bakımından tanımlayıcı ve açıklayıcı bir araştırmadır. Tanımlayıcı araştırmanın temel amacı; insanların, grupların, örgütlerin, olguların ve nesnelerin özelliklerini ortaya çıkarmak ve tanımlamaktır. Açıklayıcı araştırmada ise temel amaç değişkenler arasındaki nedensel ilişkileri ortaya çıkarmaktır (Gürbüz ve Şahin, 2016:103-104) Araştırma kullanılan araştırma yöntemi bakımından nicel araştırma desenleri çerçevesinde yer alan nedensel tarama araştırmaları kapsamında bulunmaktadır. Bir veya birden fazla bağımlı değişken üzerinde etkili olan bağımsız değişken veya değişkenlerin tespit edilmeye çalışıldığı tarama araştırmalarına nedensel tarama araştırmaları denilmektedir. Nedensel tarama desenleri çerçevesinde; yapısal eşitlik modelleri, çoklu doğrusal regresyon, lojistik regresyon vb. yapılabilecek analizler ile çalışma araştırılabilmektedir (Gürbüz ve Şahin, 2016: 110).

Araştırmanın uygulama bölümüne geçilmeden araştırma modelini ve amacını belirlemek amacıyla yapılan literatür taramaları neticesinde gerekli olan hipotezler hazırlanmış ve hazırlanan hipotezler ile Şekil 13 ile gösterilen araştırma modeli tasarlanmıştır. Sonrasında hipotezleri destekleyecek anket formunun oluşturulması için; sosyal mühendislik, siber güvenlik ve online alışveriş çalışmaları ile ilgili gerekli literatür tekrar taranarak ilgili konularda araştırma yapan araştırmacıların anket formlarından derleme yapılarak yeni bir anket formu oluşturulmuştur. Daha sonra oluşturulan anket formları üzerinden elde edilen veriler analiz edilmiştir.



Şekil 13 : Araştırma Modeli: Online Alışveriş Güvenlik Modeli (OAGM)

Araştırmaya temel oluşturacak hipotezler Tablo 7 ile gösterilmektedir. Literatürde yapılan siber güvenlik, sosyal mühendislik ve online alışveriş niyeti çalışmalarına yönelik; Barışkan, 2017; Tosun, 2015; Budak, 2015; Angün, 2016 ve Hassan, 2016 isimli araştırmacıların çalışmaları incelenmiş tespit edilen tüm bilgiler ışığında araştırmacıların yüksek lisans tezleri hipotezlerin geliştirilmesinde kullanılmıştır.

Tablo 7: Araştırma Hipotezleri

NO	HİPOTEZ	AÇIKLAMA
1.	**H1**	Genç tüketicilerin siber güvenlik farkındalıkları sosyal mühendislik farkındalıklarını pozitif yönde etkilemektedir.
2.	**H2**	Genç tüketicilerin siber güvenlik farkındalıkları online alışveriş niyetlerini pozitif yönde etkilemektedir.
3.	**H3**	Genç tüketicilerin sosyal mühendislik farkındalıkları online alışveriş niyetlerini pozitif yönde etkilemektedir.

5. ARAŞTIRMANIN EVRENİ VE ÖRNEKLEMİ

Araştırmanın ana kütlesini, Bandırma Onyedi Eylül Üniversitesinin merkez kampüsünde farklı bölümlerde öğrenim gören üniversite öğrencileri oluşturmaktadır. Örneklem teknikleri sınıflandırmasında kolayda örneklem tekniğinden yararlanılmıştır. Kolayda örneklemede; araştırmacı çalışması için ihtiyaç duyduğu büyüklükteki örnekleme ulaşıncaya kadar en kolay ve ulaşılabilir kaynaklardan veri toplamaktadır. "Bulduğunu örnekle" felsefesini güden kolayda örnekleme yönteminde araştırmacı örneklemeye girecek öğeleri ve birimlerini tanıdıklarından yakın çevresinden veya en kolay ulaşabileceği vasıtalardan yararlanarak örnekleme dâhil etmektedir (Gürbüz ve Şahin, 2016: 134).

Bir araştırmada ana kütlenin ve örneklem büyüklüğünün belirlenmesinde birtakım formüller kullanılmaktadır. Bunlar arasında en fazla kullanılan Cochran tarafından öne sürülen formüldür. Formülün temelinde üç önemli terim bulunur. Güven düzeyi (alfa) (t), kabul edilebilir hata toleransı (d) ve evren için kabul edilen standart sapma (s). Güven düzeyi araştırma evreninin, örneklem değerlerinin farklı zamanlarda tekrarlanması durumunda hangi güven düzeyinde temsil ettiğini gösterir. Genellikle %95 ve %99 olmak üzere iki güven düzeyi kullanılır. Güven düzeylerini 1'e tamamlayan fark ise yanılma olasılıklarını göstermektedir. Yanılma olasılıkları sırasıyla 0,05 ve 0,01'dir. Sosyal bilimler araştırmacıları çoğunlukla %95 güven düzeyinde çalışırlar. 0,005 güven düzeyine karşılık 1.96 "z" değeri, 0.001 güven düzeyine karşılık 2,58 "z" değeri kullanılmaktadır. Kabul edilebilir örneklem hatası, hata toleransıdır. Sosyal bilim araştırmalarında genellikle %5 lik hata toleransı kabul edilebilmektedir (Gürbüz ve Şahin. 2016: 130-131). Nicel değişkenli araştırmalar için örneklem hesaplama formülü denklem (1.a) ile gösterilmiştir.

Denklem (1.a): Nicel Değişkenli Araştırmalar İçin Örneklem Hesaplama Formülü

$$n = \frac{n_o}{1 + n_o/N}$$

N: Evren büyüklüğü

n: Örneklem büyüklüğü

t= Güven düzeyine karşılık gelen tablo z değeri (0.05 için 1.96, 0 .01 için 2.58 ve 0.01 için 3.28)

s= Evren için tahmin edilen standart sapma

d= Kabul edilebilir sapma toleransı

$$n_o = \frac{t^2 \times s^2}{d^2}$$

Kaynak: Bartlett, Körtlik ve Higgins 2001, s 46'dan uyarlanarak hazırlanmıştır.

Bandırma Onyedi Eylül Üniversitesinin merkez kampüsünde öğrenim gören öğrenciler çalışmanın ana kütlesini oluşturmaktadır. Üniversitede toplamda 11.650 öğrenci öğrenim görmektedir. Bu öğrencilerden yaklaşık olarak 7700 tanesi merkez kampüste eğitim-öğretim faaliyetlerine devam etmektedir. Bu öğrencilerin tamamı çalışmamızın ana kütlesine uyarlandığında, kabul edilebilir asgari örneklem büyüklüğüne, denklem (1.2a) ve denklem (1.2b) ile ulaşılmaktadır.

$$n_o = \frac{1{,}96^2 \times 0{,}5^2}{0{,}05^2} = 384{,}16 \qquad \textbf{(1.2a)}$$

$$n = \frac{384{,}16}{1 + 384{,}16/7700} = 365{,}93 \qquad \textbf{(1.2b)}$$

Görüldüğü gibi yaklaşık olarak 366 kişilik bir örneklem büyüklüğü araştırmamız için yeterli olmaktadır. Shirsavar, Gilaninia ve Almani (2012) ise çalışmalarında örneklem büyüklüğünü belirmeye yönelik farklı bir yaklaşım geliştirmişlerdir. Çalışmada ulaşılması gereken asgari örneklem sayısı denklem (1.3a) ile gösterildiği gibi formülize edilmiştir.

$$n = 5q \leq n \leq 15q \qquad \textbf{(1.3a)}$$

Formülde kullanılan q değeri ankette yer alan öğe sayısını göstermektedir. Çalışmada genel değerlendirme anketinde bulunan 20 adet tanımlayıcı soru hariç toplamda 19 adet likert ölçekli soru kullanılmıştır. Bu yaklaşıma göre ise ulaşılması gereken örneklem miktarı denklem (1.3b) ile gösterildiği gibi 95 ile 285 sayılarına eşit veya arasında olmalıdır.

$$(19\times5) = 95 \leq n \leq 285 = (19\times15) \qquad \textbf{(1.3b)}$$

Özetle örneklem hesaplamada aktarılan ilk formül araştırma evreninin büyüklüğüne göre ikinci formül ise ölçekte kullanılan soru sayısına göre oluşturulmaktadır. Araştırma kapsamında veri toplama işleminin yapılabilmesi için 15 Ocak 2019 tarihinde Bandırma Onyedi Eylül Üniversitesi Sosyal ve Beşeri Bilimler Etik Kuruluna başvurulmuş ve ilgili kurul tarafından 21.01.2019 tarihinde yapılacak olan çalışmanın uygun olduğuna karar verilmiştir (Bkz. Ek-2) İlgili etik kurul kararı ile birlikte 24.01.2019 tarihinde Bandırma Onyedi Eylül Üniversitesi Rektörlüğüne, uygulamanın Bandırma Onyedi Eylül Üniversitesi Öğrencileri üzerinde uygulanabilmesi için izin başvurusunda bulunulmuş ve rektörlüğün 06.02.2019 tarihli yazısı ile çalışmaya izin verilmiştir (Bkz. Ek-1). İlgili izinlerin alınması ile oluşturulan anket formu 18-21 Şubat 2019 tarihlerinde Bandırma Onyedi Eylül Üniversitesinin merkez kampüsünde bulunan fakültelerde öğrenim gören öğrencilere uygulanmıştır. Uygulama sonucu 693 adet anket geri dönmüştür. Yapılan inceleme sonucu 29 adet anket değerlendirmeye uygun bulunmamış ve örneklemden çıkarılmıştır. Kalan 664 kişi araştırmanın örneklemini oluşturmuştur.

6. VERİ TOPLAMA ARACI VE ANKET SORULARININ HAZIRLANMASI

Bu çalışmada olabildiğince fazla kişiye ulaşılmak istendiğinden anket tekniği kullanılmıştır. Araştırma anketinin oluşturulması için öncelikli olarak geçmiş yıllarda; sosyal mühendislik, siber güvenlik ve online alışveriş konularında yapılan çalışmalar incelenmiştir. Araştırma modeliyle aynı doğrultuda 12 araştırmacının çalışmalarında kullandıkları anketlerden derleme yapılarak toplamda 39 değişken ve sorudan oluşan iki bölümlük anket geliştirilmiştir. Anketin birinci bölümünde katılımcıların siber güvenlik ve sosyal mühendislik farkındalıkları ile online alışveriş niyetleri hakkındaki davranışlarını ölçmeye yönelik 19 değişkenden oluşan 5'li likert

ölçekli anket uygulanmıştır (1- Hiç Katılmıyorum, 2- Katılmıyorum, 3- Ne Katılıyorum Ne Katılmıyorum, 4- Katılıyorum, 5- Kesinlikle Katılıyorum). Ölçekte 8 değişken genç tüketicilerin siber güvenlik farkındalıklarını, 7 değişken genç tüketicilerin sosyal mühendislik farkındalıklarını, 4 değişken ise genç tüketicilerin online alışveriş niyetlerini ölçmeye yönelik hazırlanmıştır. Anketin ikinci bölümünde ise genç tüketicilerin sosyal mühendislik ve siber güvenlik riskleri ile ilgili genel bilgi, bilinç ve farkındalık düzeyleri ile online alışveriş niyetlerini ölçmeye yönelik 20 soruluk genel değerlendirme anketi uygulanmıştır. Ankette kullanılan ölçekler ve araştırmacıları Tablo 8 ile görselleştirilmiştir.

Tablo 8: Ankette Kullanılan Ölçekler ve Araştırmacıları

KAYNAK	**DEĞİŞKENLER**
1.Bölüm	**A. Siber Güvenlik Farkındalığı (Likert Ölçeği)**
Tuğba Kocadağ (2012)	**1**.Herkesin erişimine açık bilgisayarlarda herhangi bir şifre gerektiren işlem yapmamaya özen gösteririm. **2**. Bilinmeyen kişi ve adreslerden gelen mailleri herhangi bir güvenlik açığı oluşmaması için okumayarak kimlik avı ve dolandırıcılık ile ilgili yerlere şikâyet ederim. **3**.İhtiyaç duyduğumda ücretsiz yazılımları bilgisayarıma indirebilir veya kurabilirim.
Mustafa Öztürk (2015)	**4.** Web sitelerinin yardım güvenlik ve gizlilik gibi bölümleri olduğunu biliyorum ve kullanıyorum. **5.** İhbarda bulunacağım hat, web sitesi ve yasal kurumları bilirim. **8.**Bilgileri dijital ortamlarda nasıl güvende tutmam gerektiğini biliyorum.
Ömer Sıddık Budak (2015)	**6.** Bilgisayarımda lisansız yazılım kullanmaktan çekinmem. **7**. İnternet şifrelerimin güvenlik seviyelerini önemserim.
1.Bölüm	**B. Sosyal Mühendislik Farkındalığı (Likert Ölçeği)**
Taşkın Tanrıkulu, Hüseyin Kınay ve Osman Tolga Arıcak	**9**.İnternete girerken bilgilerimin başkaları tarafından çalınabileceğini göz önünde tutarım. **10.** Sosyal paylaşım sitelerinde (Facebook, Twitter vb.) özel bilgilerimin başkaları tarafından kötü amaçlı olarak kullanılabileceğini göz önünde bulundururum. **11.** Sanal ortamlardayken bir bilgisayar korsanının benim içinde tehlike oluşturabileceğini göz önünde bulundururum. **13.**internete girdiğimde internetin aynı zamanda başkalarına zarar verme amacıyla kullanılabileceğini aklımda tutarım
Mustafa Öztürk (2015)	**12.**İnternette tanımadığım insanlarla iletişim kurarım. **14**.Sosyal paylaşım sitelerinde bilgilerim herkese açıktır. 15.Yaptığım her şeyi sosyal medyada paylaşmayı severim (Facebook,Twitter, Instagram vb.)
KAYNAK	**DEĞİŞKENLER**
1. Bölüm	**C. Online Alışveriş Niyeti (Likert Ölçeği)**
Escobar, Rodriguez and Carvajal Trujillo (2013)	**16.**Gelecekte internet üzerinden alışveriş yapmaya devam etme niyetindeyim. **17.**Her zaman internet üzerinden alışveriş yapmak için çaba göstereceğim. **19.**İnternet üzerinden alışveriş yapmayı arkadaşlarıma tavsiye ederim.
Taylor and Todd (1995)	**18.**İnternet üzerinden alışveriş yapmak hayatımı daha cazip hale getirir.
2.Bölüm	**GENEL DEĞERLENDİRME ANKETİ** **(Siber Güvenlik-Sosyal Mühendislik-Online Alışveriş)**
Tez Yazarı	**1.**Cinsiyetiniz: Kadın ( ) Erkek ( ) **2.** Yaşınız: 18-25 ( ) 25-30 ( ) 30 ve üzeri ( ) **16.**İnternetten alışveriş yapıyorum Evet ( ) Hayır ( )
Mehmet Ali Barışkan (2017)	**Alınan Sorular: 4, 5, 6, 7, 8, 10, 11,12, 17 (Siber güvenlik ve sosyal mühendislik)** **4**.Bilgi güvenliği hakkında ne kadar bilgi sahibisiniz? Yeteri kadar biliyorum ( ) Çok az bir bilgim var ( ) Herhangi bir bilgim yok ( ) **5.**Bilgisayarınıza format attığınızda veya bir dosyayı sildiğinizde dosya kaybolur.

	Doğru ( ) Yanlış ( ) **6.**Flash diskten (USB/SD Card vb.)bir dosyayı sildiğinizde silinen dosya geri getirilemez. Doğru( ) Yanlış ( ) **7.**Bilgisayarınız saldırıya uğradığında neler yapmanız gerektiğini biliyor musunuz? Evet, ne yapmam gerektiğini biliyorum ( ) Hayır bilmiyorum ( ) **8.** Bilgisayarınızın saldırıya uğradığını veya virüs vb. zararlı yazılımların bulaştığını anlar mısınız? Evet, anlarım ( ) Hayır, anlayamam ( ) **10.** E-posta ile gelen ekleri açarken nasıl davranırsınız? Beklediğim kişiden geldiğine emin olurum ( ) Bildiğim yerden geldiyse güvenliğe dikkat etmem ( ) Dikkat etmem ( ) **11.** Oltalama (phishing) ataklarını duydunuz mu? Evet, duydum ( ) Hayır, duymadım ( ) **12.** Sosyal medya üzerinden (Facebook, Instagram, Twitter vb.) hiç kimseyi akrabanız olarak gösterdiniz mi? Gösterdiyseniz bu bilgi herkese açık mı? Evet, gösterdim. Bilgi herkese açık ( ) Evet ama sadece arkadaşlarım görüyor ( ) Hayır, göstermedim ( ) **17.**İnternette yaptığınız alışverişlerde 3D secure (Cep telefonuna doğrulama mesajı) kullanmaya dikkat ediyor musunuz? Evet ( ) Hayır ( )
Onur Dönmez (2015)	**Alınan Sorular: 3,9 (Siber güvenlik ve sosyal mühendislik)** **3**.Güvenli internet kullanımı konusunda bir eğitim aldınız mı? Evet ( ) Hayır ( ) **9.**Çevrenizde internet kaynaklı bir sorun (bilgi hırsızlığı, rahatsız edilme, e-dolandırıcılık yaşayan kimse oldu mu? Evet ( ) Hayır ( )
Emre Cihan Ateş (2016)	**Alınan Sorular:13, 14,15(Sosyal mühendislik)** **13.**Google'dan arandığında sosyal ağ profiliniz çıkıyor mu? Evet ( ) Hayır ( ) **14**.Tanımadığınız birini sosyal ağlarda arkadaş olarak eklediniz mi? Evet ( ) Hayır ( ) **15.**Sosyal ağda paylaştığınız verilerin, birileri tarafından kayıt altına alındığı bir durumla karşılaştınız mı? Evet ( ) Hayır ( )
Emre Çakmak (2011)	**Alınan Sorular:18,19, 20 (Online alışveriş)** **18.**İnternetten alışveriş yapma deneyiminiz ne kadardır. 1-5 kez ( ) 5-10 kez ( ) 10 ve üzeri ( ) Hiç ( ) **19.** İnternette bir kerede en fazla ne kadarlık alışveriş yapmayı düşünürsünüz? En fazla 100 TL ( ) 100-500 TL ( ) 500-1000 TL ( ) 1000 TL den fazla ( ) **20**.İnternet alışverişlerinizin önümüzdeki 5 yıl içerisinde tüm alışverişlerinizin yaklaşık ne kadarını oluşturacağını düşünüyorsunuz? %5 ten az ( ) % 5-10 arası ( ) %10-20 arası ( ) % 20'den fazla ( )

7. ARAŞTIRMANIN GÜVENİLİRLİĞİ

Likert ölçekli anketin birinci bölümünde uygulanan siber güvenlik farkındalığı başlığı altında yer alan 6 numaralı "Bilgisayarımda lisansız yazılım kullanmaktan çekinirim" faktörü ölçeğin güvenilirliğini düşürdüğü için anketten çıkarılmış ve değerlendirmeye alınmamıştır. 8 faktörden oluşan siber güvenlik farkındalığı bölümünün soruları, çıkarılan faktör ile toplamda 7'ye düşmüştür.

Faktör analizi sosyal bilimlerde yapı geçerliliğini test etmek için kullanılan bir analizdir. Faktör analizi ile ölçekte yer alan tüm boyutların güvenilirliğinin sayısal olarak bulunması gerektiğinden güvenilirlik analizi yapılır.

Güvenilirlik analizinde Alpha modeli kullanılmaktadır. Cronbach's Alpha sorular arası korelasyona bağlı uyum değerini gösterir. Cronbach's Alpha değerinin 0,70 ve üstünü göstermesi durumunda ölçeğin güvenilir olduğu kabul edilir. Fakat soru sayısı az olduğunda bu sınır 0,60 değeri ve üstü olarak kabul edilmektedir (Durmuş, Yurtkoru ve Çinko, 2016: 89). Bu doğrultuda ölçek güvenilirliğinin tespiti için Cronbach Alpha katsayısından yararlanılmasına karar verilmiştir. Alfa katsayısının yorumlanması genel olarak şu şekilde yapılmaktadır (Nakip, 2006: 146).

⟹ Katsayı 01-20 arası= Ölçeğe hiç güvenilmez,
⟹ Katsayı 21-40 arası= Ölçek güvenilmez,
⟹ Katsayı 41-60 arası= Ölçek nispeten güvenilir,
⟹ Katsayı 61-80 arası= Ölçek güvenilir,
⟹ Katsayı 81-100 arası= Ölçek çok güvenilir.

Paylaşılan tüm bilgiler ışığında, ölçeğin güvenilirlik analizleri Tablo 9 ile gösterilmektedir. Yapılan tüm güvenilirlik analizleri sonucunda ölçeğin güvenilir olduğu görülmüştür. İlk güvenilirlik analizinde siber güvenlik farkındalığı ölçeğinde bulunan 6. soru güvenilirliği düşürdüğü için değerlendirme dışı bırakılmıştır. Ankette yer alan tüm aralıklı/oransal sorulara ilişkin güvenilirlik değeri 0,798 olarak bulunmuştur.

Tablo 9: Ölçeğe İlişkin Güvenilirlik Analizi Sonuçları

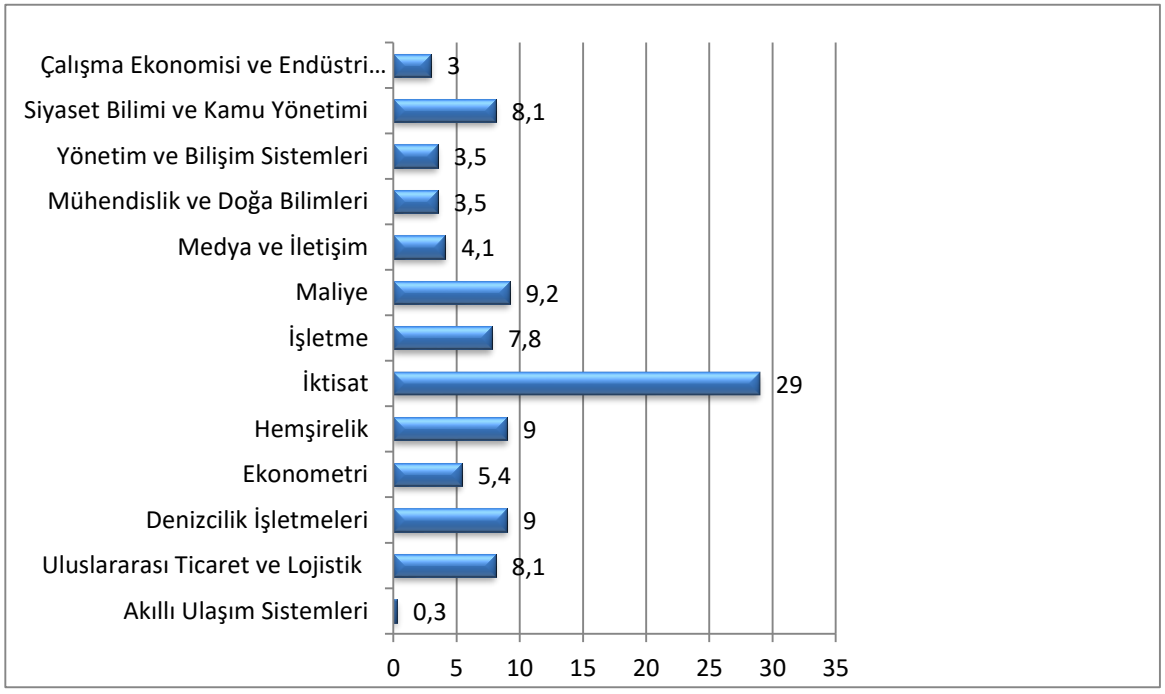
Boyut	İfade Sayısı	Alfa Katsayısı
Siber Güvenlik Farkındalığı	7	0,646
Sosyal Mühendislik Farkındalığı	7	0,776
Online Alışveriş Niyeti	4	0,880
SERVEQUAL TOPLAM	18	0,798

BEŞİNCİ BÖLÜM

BULGULAR VE ANALİZLER

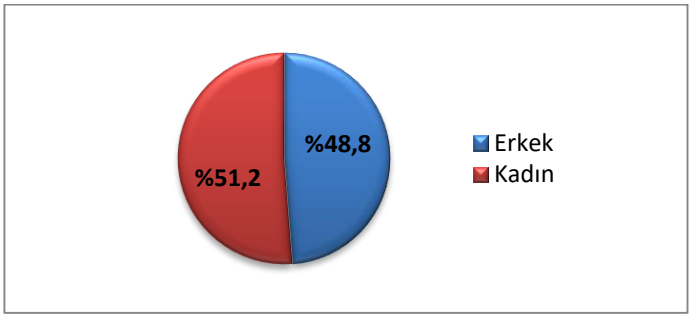
1. ÖRNEKLEME İLİŞKİN GENEL DEĞERLENDİRME ANKETİNİN SONUÇLARI VE TANIMLAYICI İSTATİSTİKLER (FREKANS DAĞILIMLARI)

Bandırma Onyedi Eylül Üniversitesinin farklı fakülte ve bölümlerinde eğitim gören (Bkz. Grafik 3) 664 lisans öğrencisine uygulanan anket çalışmasının ikinci bölümünde yer alan genel değerlendirme anketinden elde edilen verilerin istatistiksel frekans dağılımları ve sorulara verilen cevapların yüzdelik oranları soru numaralarını takiben aşağıda gösterilen grafikler yardımıyla açıklanmıştır. Veri analizlerinde SPSS versiyon 24 programından yararlanılmıştır. Anket katılımcılarının öğrenim gördükleri bölümlerin dağılımları ve oranları Grafik 3 ile gösterilmektedir.



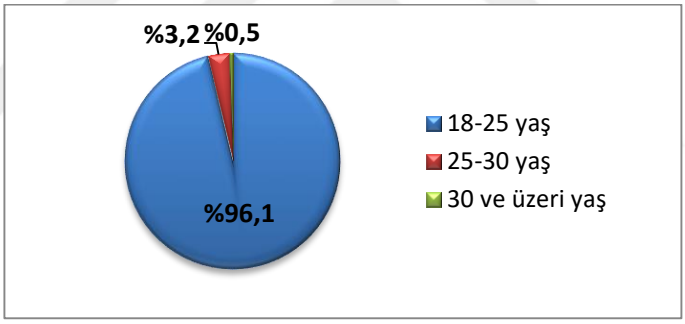
Grafik 3: Anket Katılımcılarının Öğrenim Gördükleri Bölümlerin Dağılımları ve Yüzdelik Oranları

1. Soru: Anket katılımcılarından 340 kişinin kadın, 324 kişinin erkek olduğu görülmektedir. Ankete katılımda cinsiyet dağılımı neredeyse eşittir. (Kadın %51,2 Erkek %48,8).



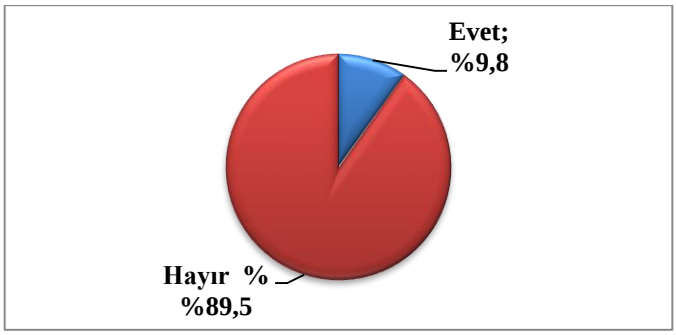
Grafik 4: Katılımcıların Cinsiyet Dağılım Oranları

2.Soru: Anket katılımcılarının %96,1'inin genç nüfusu temsil eden 18-25 yaş aralığında toplandığı görülmektedir. 21 kişi 25-30 yaş aralığında bulunmaktadır (%3,2). 3 kişi 30 ve üzeri yaş grubundadır (%0,5). 3 kişi ise soruya yanıt vermekten kaçınmıştır.



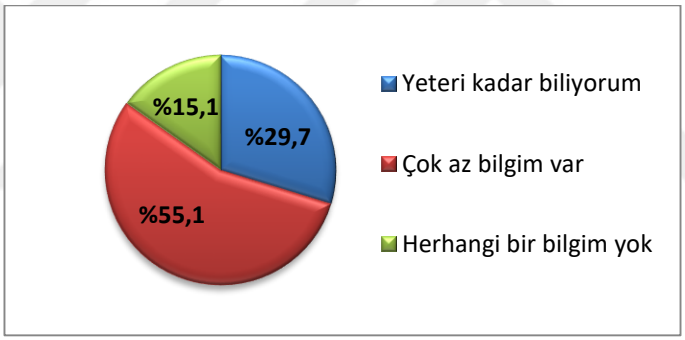
Grafik 5: Katılımcıların Yaş Dağılım Oranları

3. Soru: *"Güvenli internet kullanımı konusunda bir eğitim aldınız mı?"* sorusuna anket katılımcılarından yalnızca 65 kişinin evet yanıtını verdiği tespit edilmiştir (%9,8). 659 kişi soruyu hayır diyerek yanıtlamıştır. Yüzde %89,5 oranında kişinin soruya hayır şeklinde yanıt vermesi lisans öncesi eğitimde öğrencilerin güvenli internet kullanımı konusunda eğitim almadıklarını göstermektedir. 5 kişi ise soruya yanıt vermekten kaçınmıştır.



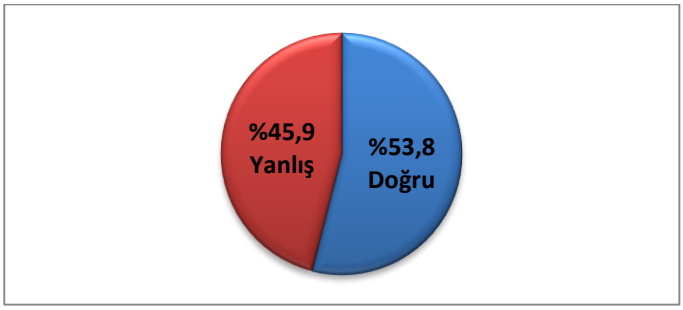
Grafik 6: Katılımcıların 3. Soruya Verdikleri Yanıtların Oranları

4. Soru: **"***Bilgi güvenliği hakkında ne kadar bilgi sahibisiniz?"* sorusuna anket katılımcılarından 197 kişi yeteri kadar biliyorum yanıtını vermiştir (%29,7). 366 kişi soruyu çok az bilgim var diyerek yanıtlamıştır (%55,1) 100 kişi ise herhangi bir bilgim yok diyerek hiçbir bilgisinin olmadığını ifade etmiştir (%15,1). Genel olarak katılımcıların yaklaşık %70'inin bilgi güvenliği hakkında bilgi sahibi olmadıkları ve çok az bilgi sahibi oldukları görülmektedir.



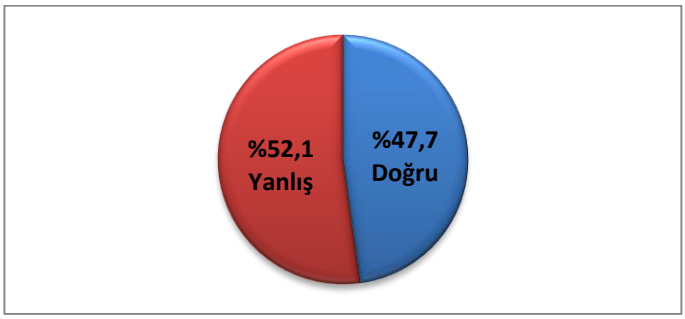
Grafik 7: Katılımcıların 4. Soruya Verdikleri Yanıtların Oranları

5. Soru: "*Bilgisayarınıza format attığınızda veya bir dosyayı sildiğinizde dosya kaybolur*" faktörüne anket katılımcılarından 357 kişi doğru (%53,8), 305 kişi ise yanlış yanıtını vermiştir (%45,9). Katılımcılardan 2 kişi soruyu yanıtlamamıştır.



Grafik 8: Katılımcıların 5. Soruya Verdikleri Yanıtların Oranları

6. Soru:“ *Flash diskten (usb/sd card vb) bir dosyayı sildiğinizde silinen dosya geri getirilemez”* faktörüne, anket katılımcılarından 317 kişi doğru (%47,7), 346 kişi (%52,1) ise yanlış yanıtını vermiştir. 1 kişi ise soruya yanıt vermekten kaçınmıştır.

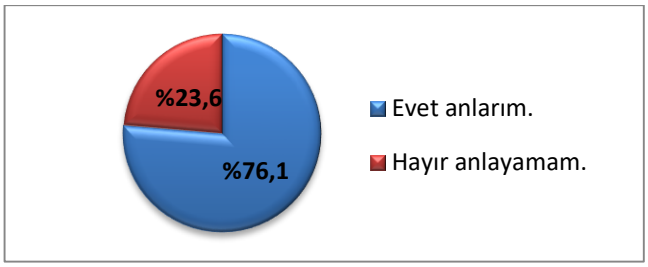


Grafik 9: Katılımcıların 6. Soruya Verdikleri Yanıtların Oranları

7. Soru: “*Bilgisayarınız saldırıya uğradığında neler yapmanız gerektiğini biliyor musunuz?”* sorusuna katılımcılardan 178 kişi (%26,8) evet ne yapmam gerektiğini biliyorum derken 485 kişi (%73) hayır bilmiyorum yanıtını vermiştir. 1 kişi ise yanıt vermekten kaçınmıştır.

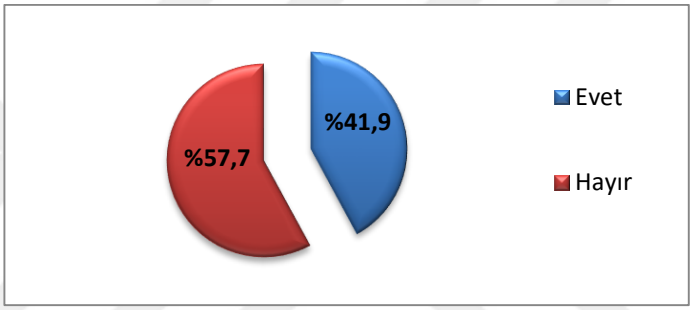
Grafik 10: Katılımcıların 7. Soruya Verdikleri Yanıtların Oranları

8. Soru: ***“****Bilgisayarınızın saldırıya uğradığını veya virüs vb. zararlı yazılımların bulaştığını anlar mısınız?”* sorusuna katılımcılardan 505 kişi evet anlarım yanıtını verirken (%76,1) 157 kişi hayır anlayamam yanıtını vermiştir (%23,6). 2 kişi ise yanıt vermekten kaçınmıştır.



Grafik 11: Katılımcılarım 8. Soruya Verdikleri Yanıtların Oranları

9.Soru: *"Çevrenizde internet kaynaklı bir sorun (bilgi hırsızlığı, rahatsız edilme, e-dolandırıcılık yaşayan kimse oldu mu ?"* sorusuna katılımcılardan 278 kişi evet yanıtını verirken (%41,9), 383 kişi hayır yanıtını vermiştir (%57,7). 3 kişi ise soruya yanıt vermekten kaçınmıştır.

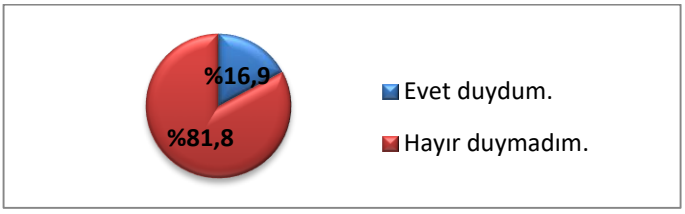


Grafik 12: Katılımcıların 9.Soruya Verdikleri Yanıtların Oranları

10.Soru: *"E- posta ile gelen ekleri açarken nasıl davranırsınız?"* sorusuna katılımcılardan 279 kişi (%42) beklediğim kişiden geldiğine emin olurum yanıtını, 245 kişi (%36,9) bildiğim yerden geldiyse dikkat etmem yanıtını, 139 kişi ise (%20,9) dikkat etmem yanıtını vermiştir. Bir kişi ise soruya yanıt vermekten kaçınmıştır.

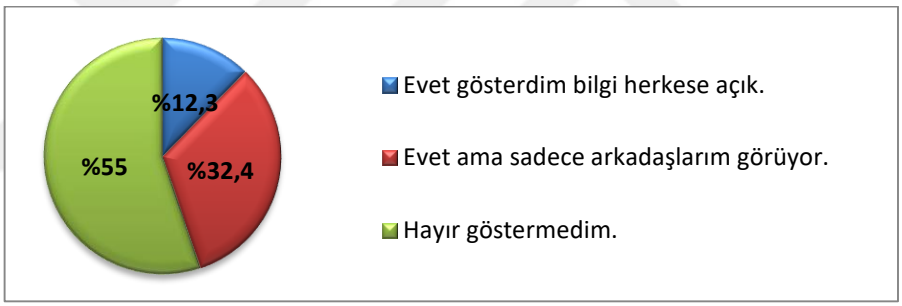
Grafik 13: Katılımcıların 10. Soruya Verdikleri Yanıtların Oranları

11. Soru: "*Oltalama (phishing) ataklarını duydunuz mu*?" sorusuna katılımcılardan 112 kişi (%16,9) evet duydum yanıtını, 543 kişi (%81,8) hayır duymadım yanıtını vermiştir. 9 kişi ise soruyu boş bırakmıştır.



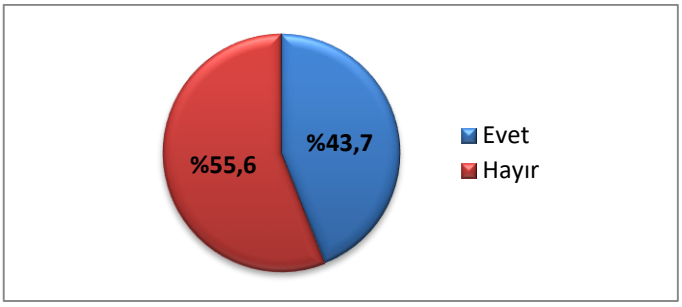
Grafik 14: Katılımcıların 11. Soruya Verdikleri Yanıtların Oranları

12. Soru: "*Sosyal medya üzerinden (Facebook, Instagram, Twitter vb.)hiç kimseyi akrabanız olarak gösterdiniz mi?" Gösterdiyseniz bu bilgi herkese açık mı?* sorusuna katılımcılardan 82 kişi (%12,3) evet gösterdim bilgi herkese açık, 215 kişi (%32,4) evet ama sadece arkadaşlarım görüyor, 365 kişi (%55) hayır göstermedim yanıtını vermiştir. 2 kişi ise soruya yanıt vermekten kaçınmıştır.



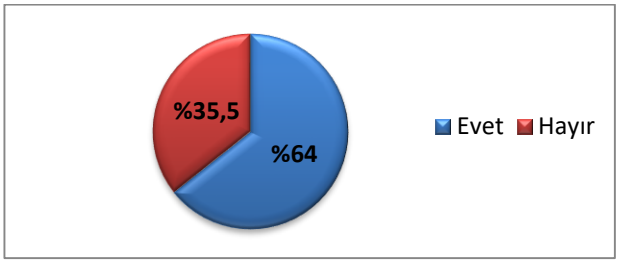
Grafik 15: Katılımcıların 12. Soruya Verdikleri Yanıtların Oranları

13. Soru: "*Google'dan arandığında sosyal ağ profiliniz çıkıyor mu?*" sorusuna katılımcılardan 290 kişi (%43,7) evet yanıtını vermiş, 369 kişi (%55,6) kişi ise hayır yanıtını vermiştir. 4 kişi yanıt vermekten kaçınmıştır.



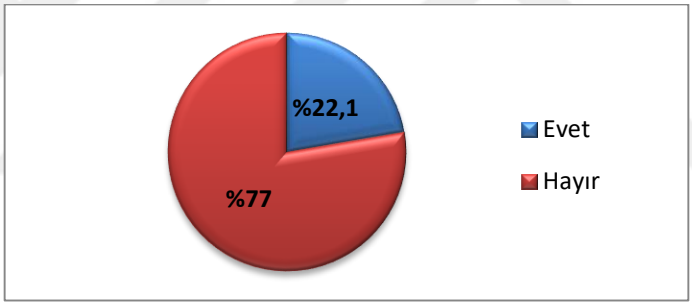
Grafik 16: Katılımcıların 13. Soruya Verdikleri Yanıtların Oranları

14. Soru: *"Tanımadığınız birini sosyal ağlarda arkadaş olarak eklediniz mi?"* sorusuna katılımcılardan 425 kişi (%64) evet yanıtını, 236 kişi(%35,5) hayır yanıtını vermiştir. 3 kişi ise yanıt vermekten kaçınmıştır.



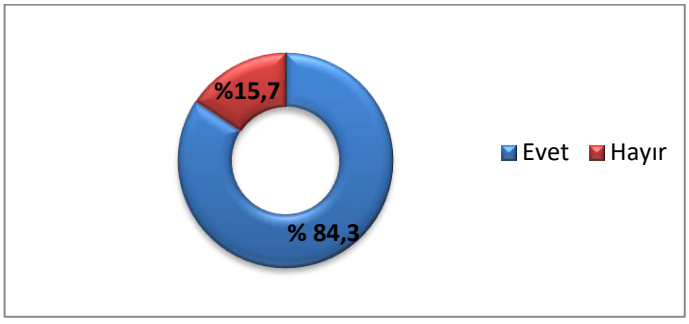
Grafik 17: Katılımcıların 14. Soruya Verdikleri Yanıtların Oranları

15. Soru: *"Sosyal ağda paylaştığınız verilerin, birileri tarafından kayıt altına alındığı bir durumla karşılaştınız mı?"* sorusuna katılımcılardan 147 kişi (% 22,1) evet yanıtını vermiş, 511 kişi (% 77) kişi hayır yanıtını vermiştir. 6 kişi ise yanıt vermekten kaçınmıştır.



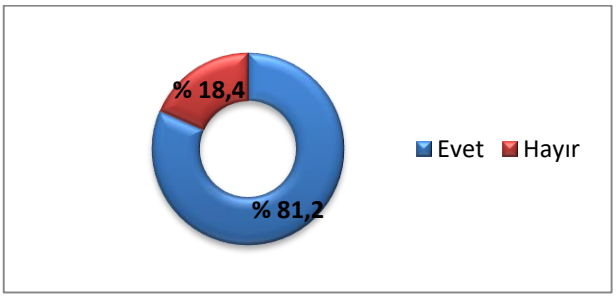
Grafik 18: Katılımcıların 15. Soruya Verdikleri Yanıtların Oranları

16. Soru: ***"İnternetten alışveriş yapıyorum"*** önermesine katılımcılardan 560 kişi (%84,3) evet yanıtını vermiş, 104 kişi (%15,7) kişi ise hayır yanıtını vermiştir.



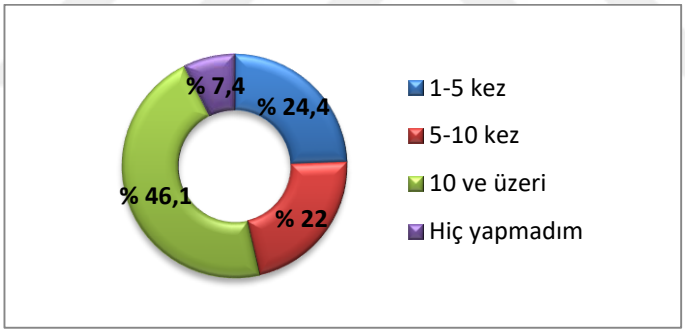
Grafik 19: Katılımcıların 16. Soruya Verdikleri Yanıtların Oranları

17. Soru: *"İnternette yaptığınız alışverişlerde 3D secure (cep telefonuna doğrulama mesajı) kullanmaya dikkat ediyormusunuz?"* sorusuna katılımcılardan 540 kişi (81,2) evet yanıtını verirken 122 kişi(%18,4) hayır yanıtını vermiştir.2 kişi yanıt vermekten kaçınmıştır.



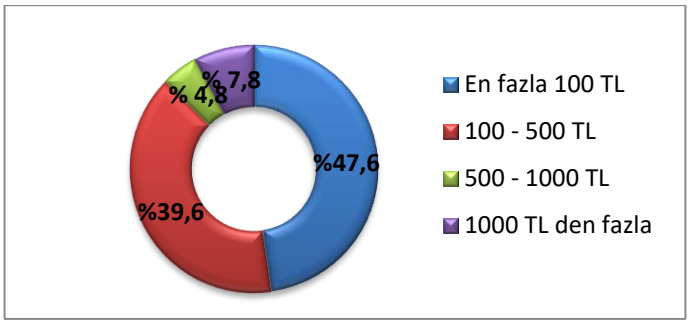
Grafik 20: Katılımcıların 17. Soruya Verdikleri Yanıtların Oranları

18. Soru:" *İnternette alışveriş yapma deneyiminiz ne kadardır?"* sorusuna katılımcılardan 163 kişi (% 24,4) 1-5 kez, 146 kişi (%22) 5-10 kez yanıtını, 306 kişi ise (%46,1) 10 ve üzeri yanıtını verirken 49 kişi (%7,4) kişi ise hiç alışveriş yapmadım yanıtını vermiştir.



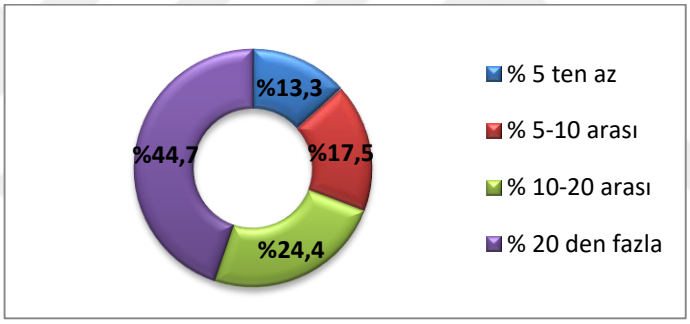
Grafik 21: Katılımcıların 18. Soruya Verdikleri Yanıtların Oranları

19. Soru: "*İnternette bir kerede en fazla ne kadarlık alışveriş yapmayı düşünürsünüz?"* sorusuna katılımcılardan 316 kişi (%47,6) en fazla 100 TL alışveriş yaparım yanıtını vermiş, 263 kişi (%39,6) en fazla 100-500 TL alışveriş yaparım yanıtını vermiş, 32 kişi (% 4,8) 500-1000 TL arası alışveriş yaparım demiş, 52 kişi ise (%7,8) 1000 TL'den fazla alışveriş yaparım yanıtını vermiştir. 1 kişi ise soruya yanıt vermemiştir.



Grafik 22: Katılımcıların 19. Soruya Verdikleri Yanıtların Oranları

20. Soru: *"İnternet alışverişlerinizin önümüzdeki 5 yıl içerisinde tüm alışverişlerinizin yaklaşık ne kadarını oluşturacağını düşünüyorsunuz?"* sorusuna katılımcılardan 88 kişi (%13,3) yüzde 5'den az yanıtını vermiş, 116 kişi (%17,5) yüzde 5 ile 10 arasında yanıtını vermiş, 162 kişi (%24,4) yüzde 10 ile 20 arasında yanıtını vermiş, 297 kişi ise (%44,7) yüzde 20'den fazla yanıtını vermiştir. 1 kişi ise yanıt vermekten kaçınmıştır.



Grafik 23: Katılımcıların 20. Soruya Verdikleri Yanıtların Oranları

2. GENEL DEĞERLENDİRME ANKETİNİN ANALİZİ VE YORUMLANMASI

Genel tanımlayıcı istatistiklerin değerlendirilmesi kapsamında yapılan değerlendirmeler Tablo 10 ile açıklanmıştır. Sonuç kısmında genel değerlendirme anketine verilen yanıtların yüzde oranları yazılmış değerlendirmeler kısmında sorulara verilen yanıtlar yorumlanarak tavsiyelerde bulunulmuş durum kısmında ise genel ortalamaya göre puanlama yapılmıştır. Sosyal mühendislik ve siber güvenlik sorularının değerlendirilmesinde durumun "Zayıf "olması genç tüketicinin yeterli düzeyde bilgiye sahip olmadığını, durumun "Orta" olması genç tüketicinin ortalama bir bilgiye sahip olduğunu durumun "İyi" olması ise genç tüketicinin yeterli düzeyde bilgiye sahip olduğunu ifade etmektedir. Online alışveriş niyetine göre yapılan durum değerlendirmesinde ise "Zayıf" genç tüketicinin online alışveriş niyetinin olmadığını, "Orta" genç tüketicinin ortalama düzeyde online alışveriş niyetinin bulunduğunu, "İyi" ise genç tüketicinin ortalamanın üstünde online alışveriş niyetinin bulunduğunu ifade etmektedir.

Tablo 10: Genel Değerlendirme Anketinin Analizi ve Yorumlanması

SONUÇ	DEĞERLENDİRMELER	DURUM
3.Güvenli internet kullanımı konusunda bir eğitim aldınız mı? Sorusuna **% 89, 5** oranında, hayır yanıtı verilmiştir. **4.** Bilgi güvenliği hakkında ne kadar bilgi sahibisiniz? Sorusuna toplamda **%70,2** oranında, çok az bilgim var ve herhangi bir bilgim yok yanıtı verilmiştir. **7.** Bilgisayarınız saldırıya uğradığında neler yapmanız gerektiğini biliyor musunuz? Sorusuna **%73** oranında, hayır bilmiyorum yanıtı verilmiştir. **11**. Oltalama (phishing) ataklarını duydunuz mu? Soruna sadece %16, 9 oranında evet yanıtı verilmiştir.% **81,8** oranında hayır yanıtı verilmiştir. **14.** Tanımadığınız birini sosyal ağlarda arkadaş olarak eklediniz mi? Sorusuna **% 64** oranında evet yanıtı verilmiş, %35, 5 oranında hayır yanıtı verilmiştir **10.**E-posta ile gelen ekleri açarken nasıl davranırsınız? Sorusuna %42 beklediğim kişiden geldiğine emin olurum demesine rağmen %36,9 oranında bildiğim yerden geldiyse dikkat etmem, %20,9 oranında dikkat etmem yanıtı vermiştir .	*3. 4. ve 7. sorulara verilen yanıtlara göre yüksek öğretim öğrencilerinin, bilgi güvenliği ve güvenli internet kullanımı konularında eğitimlere ihtiyaç duydukları görülmektedir. *Sosyal mühendislik saldırılarında oltalama (phishing) ataklarının yaygın olarak kullanıldığı bilinmektedir. 11. ve 14. Sorulara verilen yanıtlara göre, yüksek öğretim öğrencilerinin büyük çoğunluğu sosyal mühendislik saldırılarından haberdar değildir, bu sebeple sosyal mühendislik konusunda bilgi güvenliği eğitimlerinin altında bilinçlendirme çalışmaları yapılmalıdır. Yine büyük çoğunluğunun tanımadıkları kişileri sosyal ağlardan arkadaş olarak eklemeleri sosyal mühendislik saldırılarına açık olduklarını göstermektedir. * 10. soruya verilen yanıtlara göre, çoğunlukla e-postalar üzerinden gerçekleştirilen oltalama (phishing) saldırılarına karşı gerekli bilinç düzeyinin oluşmadığı görülmektedir. Çünkü katılımcıların yalnızca %42'si e-mailin beklediği kişiden geldiğine emin olmaktadır.	**ZAYIF**
SONUÇ	**DEĞERLENDİRMELER**	**DURUM**
9.Çevrenizde internet kaynaklı bir sorun (bilgi hırsızlığı, rahatsız edilme, e-dolandırıcılık yaşayan kimse oldu mu? Sorusuna %57,7 oranında hayır yanıtı verilmiş olmasına rağmen %41,9 oranında evet yanıtı verilmiştir. **12**.Sosyal medya üzerinden (Facebook, Instagram, Twitter vb.) hiç kimseyi akrabanız olarak gösterdiniz mi? Gösterdiyseniz bu bilgi herkese açık mı? "Evet" ve	* 9. Soruya verilen yanıtlara göre çevrimiçi ortamlarda her 10 kişiden 4 kişi, bilgi güvenliği hırsızlığı, rahatsız edilme ve e-dolandırıcılık ile dolandırılmaktadır. Bu yüksek bir orandır. Fakat katılımcıların yarısından fazlası hayır yanıtını verdiği için derecelendirmede orta düzey olarak değerlendirmeye alınmıştır. Bu sebeple dijital ortamlarda gerçekleşen rahatsız edilme ve	**ORTA**

"evet ama sadece arkadaşlarım görüyor" yanıtını verenlerin oranı toplamda %44.7'dir. %55 oranında ise "Hayır" göstermedim cevabı verilmiştir. **13.** Google 'dan arandığında sosyal ağ profiliniz çıkıyor mu? Sorusuna katılımcıların %43,7'si evet yanıtını vermiş, %55,6'sı ise hayır yanıtını vermiştir. **19.** İnternetten bir kerede en fazla ne kadarlık alışveriş yapmayı düşünürsünüz? Sorusuna %47,6 oranında en fazla 100 TL, %39,6 oranında 100-500 TL arasında yanıtı verilmiştir.	dolandırıcılık faaliyetlerine karşı gerekli tedbirler ve yasal yaptırımlar artırılarak gerekli bilinçlendirme çalışmaları yapılmalıdır. * 12. ve 13.sorularda sosyal ağlarda, akrabaların deşifre edilmemesi ve sosyal ağ profillerinin arama motorlarında gizlenmesi konusunda anket katılımcılarının yarısından fazlasının bilinçli olduğu görülmektedir. Fakat yinede sosyal medya kullanımı konusunda bilinçlendirme çalışmaları yapılmalıdır. * 19.soruda, katılımcıların internetten yaptıkları alışveriş tutarları değerlendirmeye alındığında yarıya yakın bir oranın 100 TL, yaklaşık %40'lık oranın ise 100-500 TL arasında harcama yaptığı görülmektedir. Bu oranlar öğrenci bütçesi düşünüldüğünde ortalama oranlardır.	**ORTA**
SONUÇ	**DEĞERLENDİRMELER**	**DURUM**
8. Bilgisayarınızın saldırıya uğradığını veya virüs vb. zararlı yazılımların bulaştığını anlar mısınız? Sorusuna %76,1 oranında evet anlarım yanıtı verilmiştir. **15.** Sosyal ağda paylaştığınız verilerin, birileri tarafından kayıt altına alındığı bir durumla karşılaştınız mı? Sorusuna %77 oranında hayır yanıtı, %22,1 oranında Evet yanıtı verilmiştir. **16.** "İnternet üzerinden alışveriş yapıyorum" Önermesine %84,3 oranında evet, %15,7 oranında hayır yanıtı verilmiştir. **17.** İnternette yaptığınız alışverişlerde 3D secure (cep telefonuna doğrulama mesajı) kullanmaya dikkat ediyor musunuz? Sorusuna %81,3 oranında evet yanıtı, %18,4 oranında hayır yanıtı verilmiştir. **18.** İnternetten alışveriş yapma deneyiminiz ne kadardır? Sorusuna %46,1 oranında 10 ve üzeri, %22 oranında 5-10 kez yanıtı verilerek %68,1 oranında 5 ve üzerinde alışveriş yapıldığı tespit edilmiştir. **20**. İnternet alışverişlerinizin önümüzdeki 5 yıl içerisinde tüm alışverişlerinizin yaklaşık ne kadarını oluşturacağını düşünüyorsunuz? sorusuna %44, 7 'si %20'den fazla yanıtını vermiş, %24,4 ü %10-20 arası yanıtını vermiştir.	*8. Soru değerlendirildiğinde katılımcıların büyük çoğunluğu bilgisayarlarına virüs vb. zararlı yazılım bulaştığını fark ettikleri görülmektedir. Fakat 7.soruya verilen yanıtlara göre katılımcılar, bilgisayarları saldırıya uğradığında neler yapmaları gerektiğini bilmemektedirler. Özetle katılımcılar saldırıyı fark etmekte fakat neler yapılması gerektiğini bilememektedirler. Saldırının fark edilmesi konusunda bir farkındalık vardır. 15. soruda katılımcıların büyük çoğunluğu sosyal ağlarda paylaştıkları verilerin birileri tarafından kayıt altına alındığı bir durumla henüz karşılaşmadığı görülmektedir. Bu sonuç şuanda internette bilgi hırsızlığının çok ilerlemediğini gösterse de %22 oranında katılımcının evet yanıtını vermesi, kişisel verilerin korunması konusunda bilinçlendirme eğitimlerine ihtiyaç olduğunu göstermektedir. * 16. 17. 18. ve 20. Sorular genel olarak değerlendirildiğinde, anket katılımcılarının neredeyse %85'nin internet üzerinden alışveriş yaptığı ve bu alışverişlerde %82 'ye yakın bir oranın 3D secure kullanımına dikkat ettiği görülmektedir. Bu oranlar ortalamanın çok üstünde kaldığından iyi olarak değerlendirmeye alınmıştır. Fakat katılımcıların, güvenli internet kullanımı, bilgi güvenliği ve sosyal mühendislik konularında eğitim almamış olmaları nedeniyle, bu kişilerin internet ortamında karşılaşabilecekleri olası bir siber veya bir sosyal mühendislik saldırısı karşısında online alışveriş niyetlerinde bir azalma olabileceği olasılığı değerlendirmeye alınmalıdır. 20. soruya verilen yanıtlara göre önümüzde ki 5 yıl içerisinde tüketicilerin %45'inin online alışverişlerine %20'den fazla bütçe ayıracağını göstermektedir.	**İYİ**

3. YAPISAL EŞİTLİK MODELLEMESİ (YEM) VE MODELLEMEYE İLİŞKİN TESTLERİN ANALİZLERİ

Yapısal eşitlik modeli sosyal bilimler alanında çalışmalar yapan bilim insanları tarafından sıklıkla kullanılan çok değişkenli ve çok kuvvetli bir analiz tekniğidir. Yapısal eşitlik modeli, istatistiksel bağımlılıkla açıklanabilen modellerde, hipotezlerin içinde bulunan değişkenlerin sebep sonuç ilişkisini açıklayarak teorik olan modellerin bir bütün halinde test edilmesine olanak sağlayan en etkili model test etme ve geliştirme yöntemlerinden biridir (Özkırış, 2010: 50). Özetle YEM, araştırmacı tarafından geliştirilmiş teorik hipotezleri sayısal veriler yardımıyla test etmektedir (Schumacker ve Lomax, 2004: 2). YEM analizi iki farklı istatistiksel parametre olarak kullanılan psikoloji ve psikonometri alanlarında gelişen faktörlerin melez, yani karma analizidir (Çokluk, Şekercioğlu ve Büyüköztürk, 2010: 253). Davranış bilimlerinde bilim insanları genellikle ölçülmesi mümkün olmayan teorik yapılar üzerinde çalışırlar. Bu yapılara gizil faktörler denilir. YEM, analizi diğer analizlerden farklı olarak gözlemlenen gizil eksojen ve gizil endojen değişkenleri üzerinde çalışır (Byrne, 2010: 4). Eksojen (Dışşal) olan gizil değişkenler YEM modellerinde bağımsız değişkenler ile kullanılan eş zamanlı değişkenlerdir. Endojen (İçsel) gizli değişkenler ise bağımlı değişkenler ile eş zamanlı olarak kullanılır ve modeldeki eksojen değişkenlerden doğrudan ya da dolaylı olarak etkilenir (Byrne, 2010: 5).

YEM'de ortaya çıkartılan modeller temelde üç stratejiye göre oluşturulur. Bu stratejiler; doğrulayıcı modelleme stratejisi, alternatif modeller stratejisi ve model geliştirme stratejisidir.

Doğrulayıcı modelleme stratejisi; araştırmacının çok net belirlediği bir model üzerinde topladığı verilerle bu modelin doğrulanıp doğrulanmadığını test etmektedir (Şimşek, 2007: 3).

Alternatif modeller stratejisi; değişkenlerin birbirleri ile aralarındaki ilişkileri açıklamada alternatif modeller arasından seçeceği modelin toplanılan veriler tarafından desteklenip desteklenmediğini test etmektedir.

Model geliştirme stratejisi; değişkenler arasındaki ilişkileri en iyi açıkladığı düşünülen modelin test edilmesi ve analiz sonuçlarına göre bu modelin geliştirilerek iyileştirilmesini amaçlamaktadır (Kayacan ve Gültekin, 2012: 7).

Yapısal Eşitlik Modellemesi iki parçadan oluşmaktadır. Bunlardan ilki gözlenen değişkenleri gizil değişkenlere bağlayarak uygulanan, "doğrulayıcı faktör analizi" kullanılan *"ölçme modeli*"dir. İkincisi ise gizil değişkenleri birbirlerine eşitlik sistemi ile eş zamanlı bağlayarak uygulamaya alınan "*yapısal model*"dir (Çokluk, Şekercioğlu ve Büyüköztürk, 2010: 261). Bu çalışmada doğrulayıcı faktör analizi ile kullanılan ölçme modeli kullanılmıştır.

4. İLK DFA (DOĞRULAYICI FAKTÖR ANALİZİ) SONUCU MODELDEN ÇIKARILAN DEĞİŞKENLER

Doğrulayıcı faktör analizi ile ölçme modeline geçildiğinde verilerde boş verilerin yer aldığı fark edilmiştir. Yapısal eşitlik boş veriyle çalışmamaktadır. Bu yüzden boş veriler SPSS paket programı yardımıyla EM (Expectation Maximization) algoritması kullanılarak doldurulmuş ilaveten hatalı girilen veriler düzeltilmiştir. Verilerin hem yapı geçerliliklerini test etmek hem de hipotez testleri öncesi modeli uygun bir yapıya sokabilmek için öncelikle doğrulayıcı faktör analizi yapılmıştır. Fakat bu analiz öncesi verilerin hem ifade bazında hem de çoklu bazda normallik değerleri incelenmiştir. Verilerin çoklu normal dağılım göstermediği (katsayı= 41.843) anlaşıldığından, analizlerde GLS (Generalized Least Square) tahmincisinin tercih edilmesine karar verilmiştir. Yapılan ilk DFA analizi sonucunda modelde yer alan 4 ifadeye ilişkin yük değerlerinin düşük olduğu ve yapı güvenilirliğini düşürdüğü anlaşılmış (Bkz, Tablo 11) bu değişkenler analizden çıkarılarak DFA analizi tekrar edilmiştir. Tablo 11'de ilk doğrulayıcı faktör analizinin sonuçları görülmektedir.

Tablo 11: İlk DFA (doğrulayıcı faktör analizi) Sonucu Modelden Çıkarılan Değişkenler

İfadeler	Katsayı
sgf3	,217
sgf2	,390
smf7	,246
Sgf 6	Güvenilirlikte Çıkarıldı
smf4	,268

5. İKİNCİ DFA (DOĞRULAYICI FAKTÖR ANALİZİ) SONUÇLARI

İlk doğrulayıcı faktör analizinden çıkarılan değişkenlerden sonra ikinci doğrulayıcı faktör analizine geçilmiştir. İkinci DFA analizi sonucunda tüm ifadelere ilişkin yük değerlerinin 0,4 ve üstünde olduğu anlaşılmıştır. Tablo 12'de ikinci DFA sonuçları görülmektedir. Ortaya çıkan sonuçla birlikte kurulan DFA modeline ilişkin uyum iyiliği değerlerinin ölçümüne geçilmiştir.

Tablo 12: İkinci DFA (doğrulayıcı faktör analizi) Sonuçları

İfadeler			Katsayı
sgf8	<---	SGF	,562
sgf7	<---	SGF	,603
sgf5	<---	SGF	,509
sgf4	<---	SGF	,508
sgf1	<---	SGF	,427
smf6	<---	SMF	,515
smf5	<---	SMF	,575
smf3	<---	SMF	,725
smf2	<---	SMF	,841
smf1	<---	SMF	,719
oan1	<---	OAN	,713
oan2	<---	OAN	,847
oan3	<---	OAN	,894
oan4	<---	OAN	,834

6. DOĞRULAYICI FAKTÖR ANALİZİ MODELİNE İLİŞKİN UYUM İYİLİĞİ DEĞERLERİ VE TESTLERİ

Yapısal Eşitlik Modellemesinde (YEM), model ve veriler arasındaki uygunluk farklı uyum endeksleri ile kontrol edilir (Yücenur, Demirel, Ceylan ve Demirel, 2011: 163). YEM, modelinde uyum iyiliği indeksleri ile teorik olarak belirlenen modelin araştırma sonrası elde edilen verilerle ne kadar iyi açıklandığı ispat edilir. Uyum iyiliği testleriyle modelin kabul veya reddedilmesine karar verilir. Fazla sayıda uyum iyiliği limit değerleri olmakla birlikte her uyum iyiliği indeksinde kritik limit değerleri bulunmaktadır. Uyum iyiliği indeksleri henüz gelişme aşamasında olduğundan bazı uyum iyiliği indekslerinin kritik limitlerin altında kalması normal kabul edilmektedir. (Özkırış, 2010: 51). Kullanılan uyum iyiliği indekslerinden en önemlileri aşağıda açıklanmıştır.

Ki-Kare (x^2): Bu değer modelin genel uyumunu değerlendirmektedir. Modelin iyi uyuma sahip olduğunu öne sürmek için bu değerin 0,05 düzeyinde anlamsız olması istenir. Fakat bu değer örneklem sayısına karşı çok duyarlıdır (Hooper, Coughlan ve Mullen, 2008: 53-54).

Yaklaşık Hataların Ortalama Kare Kökü (RMSEA): Model uyumu için kullanılan bir başka değerdir. Değerin 0 ile 0,05 arasında olması modelin iyi uyuma sahip olduğunu gösterir. Değerin 0,05 ile 0,08 arasında olması modelin kabul edilebilir bir uyuma sahip olduğunu gösterirken değerin 0,08 ile 0,10 arasında olması model uyumunun düşük olduğunu ifade etmektedir (Schermelleh –Engel, Moosbrugger ve Müller, 2003: 36).

Uyum İyiliği İndeksi (GFI): GFI modelin varyans ve kovaryans miktarının endeksidir. Örneklem hacmi yükseldikçe GFI değeri yükselir. Bu durum doğru sonuç alınmasını engelleyebilmektedir (Bayram, 2010: 74). GFI, 0 ile 1 arasında değer alır. Bu değerin 0,90'nın üzerinde olması iyi uyum olarak değerlendirilir (Schermelleh-Engel, Moosbrugger ve Müller, 2003: 36).

Düzeltilmiş Uyum İyiliği İndeksi (AGFI): İki ya da daha fazla modelin karşılaştırılmasında ya da bir modeli ve veri setini farklı kriterlere göre (örnek olarak kadın, erkek vb.) gruplandırmada kullanılır (Schumacker ve Lomax, 2004: 87).0 ile 1 arasında değer alır. 0,90 ve üzeri değerler iyi uyumu göstermektedir (Meydan ve Şeşen, 2011: 35).

Karekök Ortalama Artığı (RMR) ve Standardize Karekök Ortalama Artığı (SRMR): Örneklem kovaryans matrisi artıkları ile varsayılan kovaryans modeli arasındaki farkın karekökünden meydana gelir. İyi uyuma sahip bir modelde bu değerin 0,05'den düşük olması istenir (Hooper, Coughlan ve Mullen, 2008: 54-55).

Karşılaştırmalı Uyum İndeksi (CFI): Bu uyum kriteri 0 ile 1 arasında değer alır. 0,90 ve 0,94 arası değerler yeterli uyumu, 0,95 ve üzeri iyi uyumu göstermektedir (Byrne, 2010: 78).

Yapısal eşitlik modelinde kullanılan uyum iyiliği değerlerine ilişkin değerler Tablo 13 ile toplu olarak gösterilmiştir.

Tablo 13: Uyum İyiliği Değerleri

Uyum İyiliği	Değer	Model Uyumu
X^2/Df	288,972/74=3,905	Uyumlu
GFI	0,938	Uyumlu
AGFI	0,912	Uyumlu
RMR	0,999	Uyumlu Değil
RMSEA	0,066	Uyumlu
CFI	0,696	Uyumlu Değil

Tablo 13 ile gösterilen uyum iyiliği değerleri incelendiğinde, RMR ve CFI değerlerine göre model uyumunun düşük olduğu görülmektedir. Bununla birlikte yapıların x2/df, GFI, AGFI ve RMSEA değerlerine göre kabul edilebilir düzeyde uyum gösterdiği anlaşılmıştır. Yapılar uyum değerlerinin büyük çoğunda kabul edilebilir düzeyde uyum gösterdiği için modelin genel olarak uyumlu olduğuna karar verilmiş ve hipotez testlerine geçilmiştir.

7. HİPOTEZ TESTLERİNİN ANALİZLERİ VE SONUÇLARI

İlgili hipotezlerin test edilmesinde GLS tahmincisine dayanan Yapısal Eşitlik Modellemesinden yararlanılmıştır. Yapılan hipotez testleri neticesinde elde edilen sonuçlar Tablo 14 ile gösterilmektedir.

Tablo 14: Hipotez Testi Sonuçları

İlişki			Katsayı	Standart Hata	Anlamlılık (p)	R2 (Belirleme katsayısı)	SONUÇ
SMF	<--	SGF	,883	,093	,000	0,65 (%65)	DESTEKLENDİ
OAN	<--	SGF	,328	,158	,039	0,05 (%5)	DESTEKLENDİ
OAN	<--	SMF	-,058	,135	,666		DESTEKLENMEDİ

Yapılan testler sonucunda siber güvenlik farkındalığı değişkeninin hem sosyal mühendislik farkındalığı değişkeni üzerinde hem de online alışveriş niyeti değişkeni üzerinde pozitif yönlü ve anlamlı etki gösterdiği görülmüştür. Hipotez testleri sonucunda görüldüğü gibi bu değişkenler arasındaki değerler p<,05 koşulunu sağladığı için H1 ve H2 hipotezleri kabul edilmiştir. Genç tüketicilerin siber güvenlik farkındalığında meydana gelecek bir birimlik artış, genç tüketicilerin sosyal mühendislik farkındalığında 0,883 birim artış yaratmaktadır. Genç tüketicilerin siber

güvenlik farkındalığında meydana gelecek bir birimlik artış, genç tüketicilerin online alışveriş niyetlerinde 0,328 birim artış yaratmaktadır.

Özetle; "Genç tüketicilerin siber güvenlik farkındalıkları (SGF), sosyal mühendislik farkındalıklarını (SMF) pozitif yönde etkilemektedir" H1 hipotezi kabul edilmiştir. " Genç tüketicilerin siber güvenlik farkındalıkları (SGF) online alışveriş niyetlerini (OAN) pozitif yönde etkilemektedir" H2 hipotezi kabul edilmiştir. "Genç tüketicilerin sosyal mühendislik farkındalıkları (SMF) online alışveriş niyetlerini (OAN) pozitif yönde etkilemektedir" H3 hipotezi ret edilmiştir.

Genç tüketicilerin sosyal mühendislik farkındalıklarında meydana gelen değişimin %65'lik bir kısmı genç tüketicilerin siber güvenlik farkındalıklarında meydana gelen değişim tarafından açıklanmaktadır (R^2=0,65). Bununla birlikte genç tüketicilerin sosyal mühendislik farkındalıklarının, online alışveriş niyetleri üzerinde anlamlı bir etkisi bulunmamaktadır. Bu nedenle H3 hipotezi ret edilmiştir. Genç tüketicilerin online alışveriş niyetlerinde meydana gelen değişimin %5'lik bir kısmı, genç tüketicilerin siber güvenlik farkındalıkları tarafından açıklanmaktadır. (R^2=0,05). Bu düşük bir açıklama oranıdır. Ancak tüketicilerin online alışveriş niyetini etkileyen birçok faktör olduğu düşünüldüğünde bu sonucun kabul edilebilir olduğu rahatlıkla ifade edilebilir. Çünkü yapılan analizler online alışveriş niyetini etkileyen tüm faktörlerden sadece güvenlik faktörünü değerlendirmeye almıştır.

SONUÇ VE ÖNERİLER

Çağımızda bilgi güvenliğinin; teknoloji, ekonomi, finans, yönetim, sosyoloji, psikoloji, eğitim, sağlık ve ulusal güvenlik gibi birçok alanı etkileyen karmaşık ve sistematik bir sorun olduğu bilinmektedir. Bilgi güvenliğinin disiplinler üstü bir bilim dalı olduğunun bilinciyle yapılan bu çalışma ile online güvenliğinin sadece teknik bir konu olmadığı analizler sonucu oluşturulan Online Alışveriş Güvenlik Modeli (OAGM) ile ispatlanmıştır. Çalışma ile sosyal mühendislik, siber güvenlik ve online alışveriş konularının tek başlık altında işlenmesi ile siber alanda oluşan güvenlik zafiyetlerinin, online ticari hayat üzerindeki etkisi değerlendirmeye alınmıştır. Genç tüketicilerin sosyal mühendislik farkındalıkları ile siber güvenlik farkındalıklarının, online alışveriş niyetleri üzerindeki etkisini ölçen bu çalışmada; siber güvenliğin, sosyal mühendisliği %65 gibi güçlü bir oranda etkilediği bulgusuna ulaşılmıştır. Dolayısıyla "Genç tüketicilerin siber güvenlik farkındalıkları, sosyal mühendislik farkındalıklarını pozitif yönde etkilemektedir" H1 hipotezi kabul edilmiştir.

Çalışma sonucu göstermektedir ki aslında bilgi güvenliği farkındalığını etkileyen siber güvenlik ve sosyal mühendislik disiplinleri sanılanın aksine teknolojik gelişime paralel olarak ilerlememektedir. Örneğin; tüketiciler tarafından internet şifrelerinin güvenlik seviyelerinin önemsenmesi, ihbarda bulunulacak hat, web sitesi ve yasal kurumların bilinmesi, web sitelerinin yardım gizlilik ve güvenlik gibi bölümlerinin bilinmesi ve kullanılması, güvenilir olmayan ücretsiz yazılımların ve mobil cihazların kullanılmaması, ihtiyaç duyulduğunda güvenilir olan ücretsiz yazılımların kullanıcı tarafından bilgisayara indirilerek kurulabilmesi gibi genel bilgiler, bilgi güvenliği farkındalığı ile ilgili olası risklerin doğru değerlendirilmesiyle ilgilidir.

Daha öz bir ifadeyle; sosyal mühendislik farkındalığında meydana gelen değişimin %65'lik kısmının siber güvenlik farkındalığında meydana gelen değişim tarafından açıklanması, online ortamlarda gerçekleşen teknik güvenlik zafiyetlerinin siber güvenlik risklerini en fazla %35 oranında etkileyebileceği tespit edilmiştir. Siber güvenliğin tamamen teknik bir konu olmadığı teknolojik ve teknik zafiyetlerden bilinenin aksine yüksek oranda etkilenmediği tespit edilmiştir. Sadece

%35'lik oran teknik güvenlik zafiyetleri olarak bilinen yazılım ve donanımsal teknik risk faktörleriyle ilgili olup kalan %65'lik kısım güvenlik zincirinin en zayıf halkası olan insanın, insani zafiyetleri ve bilgi güvenliği farkındalığı ile ilgilidir. Kevin Mitnick'in ifade ettiği gibi; "Güvenlik bir teknoloji sorunu değildir, bir insan ve yönetim sorunudur" tanısı doğrulanmıştır.

Araştırmada kabul edilen ikinci hipotez "Genç tüketicilerin siber güvenlik farkındalıkları, online alışveriş niyetlerini pozitif yönde etkilemektedir" H2 hipotezidir. Genç tüketicilerin online alışveriş niyetlerinde meydana gelen değişimin %5'lik kısmı tüketicilerin siber güvenlik farkındalıkları tarafından açıklanabilmektedir. %5'lik kabul oranı düşük bir orandır. Bu durum iki şekilde açıklanabilir. Birincisi; genç tüketicilerin, online ortamlarda alışveriş yaparken siber güvenlik risklerini ihmâl etmelerinden kaynaklanmaktadır. Yani genç tüketiciler, online (çevrimiçi) ortamlarda karşılaşabilecekleri siber saldırı ve tehlikelerden ya haberdar değillerdir ya da benim başıma gelmez anlayışıyla umursamaz bir tavır sergilemektedirler. Dolayısıyla genel anlamda kabul edilebilir bir siber güvenlik farkındalığı yoktur denilebilir. İkincisi; tüketicilerin online alışveriş niyetlerini etkileyen birçok faktör bulunmaktadır. Konu literatürde "Teknoloji Kabul Modeli", (TKM) olarak çalışılmıştır.

TKM ilk olarak 1986 yılında Davis tarafından kullanılmıştır. Model e-ticaret web sitelerinin verimliliğinin değerlendirilmesinde tüketici niyetlerini açığa çıkartmaktadır (Davis, 1986; Davis, 1989; Lingyun and Dong, 2008; Klopping and Mckinney, 2004). Teknoloji Kabul Modeli, online kullanıcıların teknolojiyi nasıl benimsediklerini ve kullandıklarını modelleyen bilgi ve bilişim sistemleri teorisidir. Bilgi ve bilişim sistemleri üzerinde online kullanıcıların bu sistemleri kabul etmelerindeki faktörleri açıklayan ve yaygın olarak kullanılan modellerden biri olarak kabul edilmektedir (Lingyun and Dong, 2008; Suh and Han, 2002) Çelik (2009) tarafından referans alınarak genişletilen teknoloji kabul modeli ile yeni bir "Genişletilmiş Alışveriş Kabul Modeli" ortaya çıkmıştır. Geliştirilen bu modelde; "Algılanan Bilgi Kalitesi, Algılanan Servis Kalitesi, Algılanan Sistem Kalitesi, Algılanan Güven, Algılanan Kullanım Kolaylığı, Tutum, Online Alışveriş Niyeti ve Gerçek Davranış" alt başlıklarında likert ölçekli soru maddeleriyle ölçüm yapılmıştır (Çelik, 2009:2001,2004).

Özetle yukarıda açıklanan alt başlıkların tamamı değerlendirmeye alındığında tüketicilerin online alışveriş niyetlerindeki tutum ve davranış değişliği genel anlamda değerlendirilebilmektedir.

Bu çalışma genç tüketicilerin online alışverişlerinde yalnızca güvenlik faktörleri olarak tanımlanan; sosyal mühendislik ve siber güvenlik farkındalıklarına odaklandığından online alışveriş niyetini etkileyen diğer alt boyutlar ihmâl edilmiştir. Bu sebeple, "Genç tüketicilerin siber güvenlik farkındalıkları online alışveriş niyetlerini pozitif yönde etkiler " H2 hipotezinin kabul edilmesi, tüketicilerin online alışveriş niyetlerinde meydana gelen değişimlerin sadece %5'lik bir kısmının, genç tüketicilerin siber güvenlik farkındalıklarında meydana gelen değişim tarafından açıklanması yukarıda açıklanan diğer alt faktörlerin ihmâl edilmesi nedeniyle bu sonucunun kabul edilebilir olduğunu göstermektedir. Teknoloji Kabul Modelinde yer alan tüm faktörler değerlendirmeye alındığında aslında siber güvenlik farkındalığının, online alışveriş niyeti üzerinde %5'lik orandan çok daha yüksek oranda etkili olabileceği yorumu kolaylıkla yapılabilmektedir. Bununla birlikte yapısal eşitlik modellemesi ile ulaşılan sonuçlardan bir diğeri; genç tüketicilerin siber güvenlik farkındalığında meydana gelecek bir birimlik artışın genç tüketicilerin online alışveriş niyetlerini 0,328 birim arttırdığıdır.

Araştırma sonucunda ulaşılan bir başka bulgu, sosyal mühendisliğin, online alışveriş niyetini etkilemediğidir. Bu nedenle " Genç tüketicilerin sosyal mühendislik farkındalıkları, online alışveriş niyetlerini pozitif yönde etkilemektedir "H3 hipotezi reddedilmiştir.

Genel değerlendirme anketinin istatistiksel sonuçları değerlendirmeye alındığında aşağıdaki bulgulara ulaşılmıştır.

- ✓ Genç katılımcıların %89,5'i güvenli internet kullanımı konusunda eğitim almamıştır.
- ✓ Genç katılımcıların %70,2'sinin bilgi güvenliği hakkında bilgi sahibi olmadıkları ve çok az bilgi sahibi oldukları tespit edilmiştir.
- ✓ Genç katılımcıların %73'ü bilgisayarları saldırıya uğradığında neler yapılması gerektiğini bilmemektedir.
- ✓ Genç katılımcıların %81,8'i oltalama (phishing) ataklarından haberdar değildir.

- ✓ Genç katılımcıların %64'ü sosyal ağlarda tanımadıkları insanlarla arkadaşlık kurmaktadır.
- ✓ Genç katılımcıların %57,8'i E-posta ile gelen ekleri açarken dikkatli davranmamaktadır.
- ✓ Genç katılımcıların %47,7'si sosyal medya hesaplarında akrabalarını deşifre etmektedir.
- ✓ Genç katılımcıların %41,9'unun çevresinde, internet kaynaklı bilgi hırsızlığı, rahatsız edilme ve e-dolandırıcılık yaşayan bir kimse olmuştur.
- ✓ Genç katılımcıların %43,7'si arama motorlarında sosyal ağ profillerini gizlememektedir.
- ✓ Genç katılımcıların %22,1'i sosyal ağlarda paylaştıkları verilerin birileri tarafından kayıt altına alındığı bir durumla karşılaşmıştır.
- ✓ Genç katılımcıların %76,1'i bilgisayarının saldırıya uğradığını veya bilgisayarına virüs vb. zararlı yazılım bulaştığını fark etmektedir.
- ✓ Genç katılımcıların %81,3'ü internet alışverişlerinde 3D secure (cep telefonuna doğrulama mesajı) kullanmaktadır.
- ✓ Genç katılımcıların %47,6'sı internette bir kerede en fazla 100 TL alışveriş yapmaktadır.
- ✓ Genç katılımcıların %46,1'nin internetten alışveriş deneyimi 10 ve üzerindedir.
- ✓ Genç katılımcıların %47,7'si önümüzdeki 5 yıl içerisinde internet alışverişlerine %20'den fazla bütçe ayıracağını beyan etmiştir.

Genel değerlendirme anketinde üç adet önemli bulgu tespit edilmiştir. Bunlardan ilki; genç tüketicilerin büyük çoğunluğu, siber saldırılara ve sosyal mühendislik saldırılarına açıktırlar ve bilgi güvenliği eğitimlerine ihtiyaç duymaktadırlar. İkincisi; genç tüketicilerin, sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisi zayıftır. Üçüncüsü ise genç tüketicilerin %47,7'si önümüzdeki 5 yıl içerisinde online alışverişlere %20'den fazla bütçe ayıracaklardır. Elde edilen bulgulara dayanılarak; dijital vatandaşlığın geliştirilmesi kapsamında; bilgi güvenliği, bilgi okuryazarlığı, sağlık okuryazarlığı, finans okuryazarlığı, sosyal medya ağı okuryazarlığı ve dijital okuryazarlık

eğitimlerinin tüm üniversitelerde yaygınlaştırılması gerekmektedir. Dijital dönüşümün yaşandığı çağımızda ülke ekonomilerinin ve finansal piyasaların temel dinamikleri artık siber alana oturmaya başlamıştır. Bu nedenle siber alanda sağlam temeller atan ülkeler dünya ekonomisine yön veren ülkeler olacaktır. Bu noktada fırsatları değerlendirip zorlukları doğru yönetebilen ülkeler, maksimum verimlilik ve maliyet avantajları sağlayacak ve nihayetinde milli gelirlerini pozitif yönde etkileyerek ekonomilerini ileriye taşıyacaklardır.

Araştırma konusu genel olarak değerlendirildiğinde aşağıda akademiye ve sektöre yönelik yazılı olan önerilerin, ulusal ve uluslararası platformlar da Türkiye'de online ticaretin gelişimini destekleyeceği ve Türkiye'nin ekonomi politikaları üzerinde katma değer yaratacağı düşünülmüştür.

- Türkiye'de bireylerin bilgisayar ve internet kullanım oranları ile 4,5 G mobil telefon abone sayısındaki yüksek artış değerlendirildiğinde, elektronik ticaretin köklü değişimlere neden olacağı beklenmelidir. Bu nedenle dijitalleşen ticari hayata paralel olarak vatandaş profilleri de dijital vatandaşlık kavramına uygun ilerlemeli, dijital vatandaşlık konusunda çalışmalara hız verilmelidir.
- Sınır ötesi E-ticareti geliştirecek mevzuat eksikliği tamamlanmalıdır.
- Bir inşaat mühendisinin imzası olmadan bina yasal olarak inşa edilememektedir. Aynı durum bilgisayar ve yazılım mühendislerinin ortaya çıkaracakları projeler içinde geçerli olmalıdır. Bilişim alanında çalışan tüm mühendislerinin ortaya çıkaracakları projelerde imza yetkilerini kapsayan yetki ve sorumlulukları olmalıdır. Bilişim mühendislerinin imza yetkisi şartı hukuken getirilmelidir. Hiçbir eğitim almamış ya da yeterli düzeyde eğitim almamış kişilerin, web sitelerinin tasarımı ve yazılımının inşası konusunda yetkileri bulunmamalıdır. İmza yetkisi bilişim ve mühendislik faaliyetlerinde kamusal çıkarların denetlenmesi adına getirilmelidir. Çünkü çağımızda mühendislik faaliyetleri artık ekonomi politikalarının toplumsal zeminini oluşturmaktadır.
- Ticari işletmelerin bilgi işlem personelleri işin gerektirdiği nitelik ve yeterliliğe göre Mesleki Eğitim Kurumu tarafından mesleki yeterlilik belgesi ile yetkilendirilmeli veya Mesleki Yeterlilik Kurumunun üniversiteler

aracılığıyla belirli aralıklara verecekleri eğitimler ve değerlendirme sınavları ile bilgi işlem personelin kendilerini güncellemeleri sağlanmalıdır.

- İlköğretim seviyesinden başlamak üzere Milli Eğitim Bakanlığı'nın hazırlamış olduğu eğitim müfredatına dijital vatandaşlık dersi eklenmeli, çocuklara mutlaka dijital oyun dersleri verilmelidir. Mavi balina, momo vb. zararlı içeriği bulunan ve çocukları intihara sürükleyen oyunlara karşı çocuklar bilinçlendirilmelidir. Eğitimde tutarlı bir bilim ve teknoloji politikası olmadan dijital vatandaşlık kavramı benimsenmeyecektir.
- Ülkemizde ulusal veri koruma otoritesi Kişisel Verileri Koruma Kurumudur (KVKK). Veri gizliliğinde ulusal ve uluslararası standartların sağlanması amacıyla özellikle bankacılık, finans ve sağlık kuruluşları üzerinde sıkı denetimler gerçekleştirilmelidir.
- Ülkemizde bilişim ve bilgi teknolojileri sektöründe çalışan ve çalışacak olan tüm insan kaynağı kayıt altına alınmalıdır. Kayıt altına alma işleminde yapılacak yetkilendirme işlemi, üniversiteler aracılığıyla Yükseköğretim Kuruluna (YÖK), Yükseköğretim Kurulu aracılığıyla, Bilgi Teknolojileri ve İletişim Kurumuna (BTK) bildirilecek şekilde yapılanmalıdır. Kayıt altına alma işleminde ülke genelinde bilgisayar mühendisliği, yazılım mühendisliği, yönetim ve bilişim sistemleri, bilgi güvenliği, yazılım, kodlama, bilgisayar programcılığı vb. programlarda; ön lisans, lisans, yüksek lisans ve doktora eğitimi alan tüm bilişimcilerin imza yetkisini de kapsayacak şekilde sicil numarası ile işlem yapabilme yetkileri bulunmalıdır. Bu sicil numaraları ayrıca BTK' ya bildirilerek tüm bilişimci insan kaynağı kayıt altına alınmalıdır. Böylelikle online alışverişlerde sahte web sitelerinin oluşturulması neticesinde online dolandırıcılık engellenecek, bu sitelerin kimler tarafından oluşturulduğu kayıt altına alınmış olunacak ayrıca bu tür ticari işlemlerin tescillenmesi ile kayıt dışı ekonominin önüne geçilmiş olunacaktır. Ek olarak sicil numaraları ile Bilgi Teknolojileri ve İletişim Kurumu onayından geçen web sitelerinin yazılım ve tasarımcılarının sicil numaralarının web sitelerinin, gizlilik ve güvenlik bölümünde BTK' ya kayıtlı olduğuna dair vatandaşı bilgilendirecek ve güven uyandıracak bir işaret ya da ibare bulunmalıdır.

- Siber dolandırıcılıkların önüne geçebilmek amacıyla online tüketicileri korumaya yönelik online alışveriş sigortası getirilmelidir.
- Bilişim üzerine ihtisaslaşmış Bilişim İhtisas Mahkemeleri'nin kurulması için alt yapı çalışmalarına başlanılmalı ve zaman kaybedilmeden hayata geçirilmelidir. Hukuk fakültelerinin tamamında algoritma ve yazılım öğrenmeye dair dersler verilmeli, üniversitelerde Adli Bilişime yönelik programlar açılmalıdır. Gerekli hukuki alt yapı oluşturulmadığı takdirde tüm çalışmalar sonuçsuz kalacaktır.
- Finansal Bilgi Teknolojileri Araştırma Laboratuvarları kurulmalıdır. Bu laboratuvarlarda sermaye piyasalarına, bankacılık sektörüne ve sosyal güvenlik kurumlarına yönelik düzenlenebilecek olası siber saldırı faaliyetleri, bu faaliyetlerin etkileri ve sonuçları değerlendirmeye alınmalı ve neticede stratejik bilgi yönetimi ve bilişim sistemleri konularında Ar-Ge ve politika geliştirme çalışmalarına başlanılmalıdır.
- Teknolojik gelişim ve yenilenmeyle birlikte siber güvenlik uzmanlarına olan ihtiyaç artmaktadır. Bu noktada siber güvenlik açığının oluşmaması için yeterli düzeyde siber güvenlik uzmanı yetiştirilmelidir.

.

KAYNAKÇA

AHN, G. J., SHEHAB, M., & SQUİCCİARİNİ, A. (2011). **Security and privacy in social networks**. IEEE Internet Computing, *15*(3), 10-12.

AKARSLAN, H. (2011) Bilişim suçları, bilişim yoluyla işlenen suçlar ve adli bilişim ayrımı. Yayımlanmış Yüksek Lisans Tezi, **Polis Akademisi Güvenlik Bilimleri Enstitüsü** Ankara.

AKSOY, R. & SEVER, H. (2012). Elektronik pazarlarlarda güven problemi ve kriminal faaliyetler. *Ejovoc* **(Electronic Journal of Vocational Colleges),** *2*(1).

ALAGÖZ, A. & ALLAHVERDİ, M. (2011). **Kurumsal Bilgi Güvenliği Ve Muhasebe Bilgi Sistemi. Muhasebe ve Vergi Uygulamaları Dergisi** (MUVU)/Journal Of Accounting & Taxation Studies (JATS), 4(3).s.51

ALATAŞ, Ş, & ATAN, M. (2007). **Phishing: İnternet Denizinin Popüler Avlanma Yöntemi.** XII. Türkiye İnternet Konferansı" İnternet ve Toplum Bilgi Toplumuna Doğru.

ALEXANDER BROWN, Protecting Online Privacy, **The Secure Online Busıness handbook e-commerce, IT functionality& business continuity**, consultant editör: Jonathan Reuvid, thirt edition, Printed and bound in Great Britain by Cambridge University Press, Kogan Page Limited (2005).Pp.71-77.

ANDERSON, R., BARTON, C., BÖHME, R., CLAYTON, R., VAN EETEN, M. J., LEVİ, M., & SAVAGE, S. (2013**). Measuring the cost of cybercrime. In The economics of information security and privacy** (pp. 265-300). Springer, Berlin, Heidelberg.

ANGELI SUSANNE & KUNDLER WOLFGANG (2006).**Der Online Shop Handbuch für Existenzgründer**.2006 by Markt + Technik Verkag, ein Imprint der Pearson Education Deutschland GmbH, Printed in Germany. Pp.623-624.

ANGÜN, S.(2016).Çevrimiçi(Online) alışverişte farklı toplumların riskleri algılamasına dair bir çalışma. Yayınlanmış Yüksek Lisans Tezi. **Maltepe Üniversitesi, S.B.E**.İstanbul.

ARSLAN, M. E. **Siber Güvenlik Ve Siber Saldırı Türleri**..Sağlık Bilişim Enstitüsü, Gazi Üniversitesi, Ankara ss.3-10..

ATEŞ, E.C.(2016).Üniversite öğrencilerinin sosyal ağlara ilişkin tutumlarının suç ve suçla mücadele açısından değerlendirilmesi. Yayınlanmış Yüksek Lisans Tezi. **Ondokuz Mayıs Üniversitesi F.B.E**.Samsun.

BAĞCI, H . (2008). **Sosyal Mühendislik Ve Denetim**. Denetişim, (1), 42-51. "Çevrimiçi" http://dergipark.gov.tr/denetisim/issue/22499/240554 Erişim: 06.08.2018

BAHADUR. G,CHAN. C, WEBER (2002).**Privacy Defended Protecting Yourself Online**. First Printing:February 2002. Printed in the United States of America.Copyrigh 2002 by Que.Pp.262-264.

BARIŞKAN, M. A. (2017). Türkiye' de Siber Güvenlik Bilinci Ve Sosyal Mühendislik Ataklarına Karşı Savunma Önlemlerinin Geliştirilmesi. Yayınlanmış Yüksek Lisans Tezi, **İstanbul Üniversitesi, F.B.E** İstanbul. Ss.3-67

BARTLETT, J.E., KÖRTLİK, J.W. VE HİGGİNS, C.C. (2001). Organizationalresearch: Determinig appropriate sample size in survey research. **Information Technology, Learning, and Performance Journal**, 19(1), 43-50.

BAYRAM, N. (2010). "Yapısal Eşitlik Modellemesine Giriş: AMOS Uygulamaları". Ezgi Kitabevi, Bursa .

BERKAY, A. (2009**). Hack Teknikleri**. Yayınlanmamış Ders Notları. http://www. bilmuh. gyte. edu. tr/ispinar/BIL673 (15 Mayıs 2006).

BİLEN ADAM,(2017) "Çevrimiçi" https://www.youtube.com/watch?v=p7SC3ZlCxvg, IP Adresini Bulup Yer Tespiti Yapma, Erişim: 29.03.2019.

BUDAK, Ö.S.(2015).Bilişim öğrencilerinin siber suç farkındalığı: Erzurum ili mesleki ve teknik liseler örneği. Yayınlanmış Yüksek Lisans Tezi. **Atatürk Üniversitesi, E.B.E.** Erzurum.

BYRES, E., & LOWE, J. (2004, October). **The myths and facts behind cyber security risks for industrial control systems.** In Proceedings of the VDE Kongress (Vol. 116, pp. 213-218).

BYRNE, B. M. (2010). "**Structural Equation Modeling with AMOS: Basic Concepts, Applications and Programming**," Second Edition. Routledge Taylor and Francis Group; New York, U.S.A

CALDWELL, T. (2011). **Ethical hackers: putting on the white hat**. Network Security, *2011*(7), pp.10-13.

CAMPBELL, M. A. (2005). Cyber bullying: An old problem in a new guise? **Journal of Psychologists and Counsellors in Schools,** *15*(1), 68-76.

CANBEK, G.& SAĞIROĞLU, Ş. (2007). **Ç**ocukların ve gençlerin bilgisayar ve internet güvenliği**. Politeknik Dergisi,** *10*(1).

CANBEK, G., & SAĞIROĞLU, Ş. (2007**).** Bilgisayar Sistemlerine Yapılan Saldırılar Ve Türleri: Bir İnceleme. **Erciyes Üniversitesi Fen Bilimleri Enstitüsü, Fen Bilimleri Dergisi,** 23(1), ss.1-12.

CEYHAN, E. B. DEMİRYÜREK, E. & KANDEMİR, B. (2015). Sosyal ağlarda güncel güvenlik riskleri ve korunma yöntemleri. **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 1(1).**

CHAUDHARY, S.(2016). **The Use of Usable Security and Security Education to Fight Phishing Attacks**. Acta Universitatis Tamperensis 2238. Tampere University Press Tampere 2016. Pp,76-139

CYBERMAG, (2017)Siber Güvenlik Dergisi, "Siber Terörle Mücadelede Tehditler ve Önlemler**'' Bilgi Güvenliği Derneği**, **Siber Güvenlik Dergisi,** sayı, 14, s.19.

CYBERMAG, (2017)Siber Güvenlik Dergisi, "Sosyal Mühendislik Korunma Yolları" **Bilgi Güvenliği Derneği, Siber Güvenlik Dergisi,** sayı, 18, ss.21-23.

CYBERMAG, (2017)Siber Güvenlik Dergisi, "Türkiye'de ve Dünya'da Siber Savaşlar'' **Bilgi Güvenliği Derneği, Siber Güvenlik Dergisi,** sayı, 12, ss.20-23.

ÇAKIR, H. YALÇIN, N., & KILIÇ, M. S. (2017). İnternet Sitelerine Yapılan Siber Saldırılar: 2015 Yılı Türk Kamu Siteleri İncelemesi. **Güvenlik Stratejileri Dergisi**, *13*(25), 149-192.

ÇAKMAK, E.(2011).İnternet ortamında müşteri güveni. Yayınlanmış Yüksek Lisans Tezi. **Boğaziçi Üniversitesi. S.B.E**.İstanbul

ÇELEN, F. K. ÇELİK, A. & SEFEROĞLU, S. S. (2011). **Çocukların internet kullanımları ve onları bekleyen çevrim-içi riskler**. Akademik Bilişim, 2-4.

ÇELİK, H.E.(2009).Yapısal Eşitlik Modellemesi ve Bir Uygulama: Genişletilmiş Online Alışveriş Kabul Modeli. Yayınlanmış Doktora Tezi. **Eskişehir Osmangazi Üniversitesi, F.B.E.**

ÇELİKTAŞ, B (2016).Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme. Yayınlanmış Yüksek Lisans Tezi. **Karadeniz Teknik Üniversitesi, SBE**. Trabzon.

ÇETİN, H. & IRMAK, S. (2014). Elektronik Alışverişte Akademisyenlerin Güvenlik ve Risk Algılarının Belirlenmesi. Journal of Administrative Sciences **/Yönetim Bilimleri Dergisi,** *12*(24).

ÇOKLUK, Ö. ŞEKERCİOĞLU, G. VE BÜYÜKÖZTÜRK, Ş. (2010). "**Sosyal Bilimler İçin Çok Değişkenli İstatistik**: SPSS ve Lisrel Uygulamaları", Ankara. Pegem Yayınevi.

ÇUBUKCU, A. & BAYZAN, Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. **Middle Eastern & African Journal of Educational Research,** *5*, 148-174.

DAİ. Y, HAN. D, HAN. T, DAİ. X.(2015) Explore Awareness of Information Security: Insights from Cognitive Neuromechanism. PMC. US National Library of Medicine National.

DAVİD A.CROWDER & RHONDA CROWDER (2000). **CliffsNotes Shopping Online Safely**. CliffsNotes Shopping Online Safely Published by IDG Books Worldwide,INC.An International Data Group Company.Printed in the United States of America.s.73.

DAVİS, F.D. (1986) A technology acceptance model for empirically testing new end-user

information systems: theory and results, **PhD dissertation, Massachusetts Institute of Technology, Cambridge, MA.**

DAVİS, F.D. (1989), Perceived usefulness, perceived ease of use, and user acceptance of

information technology, **MIS Quarterly,** 13(3), 319-39.

DEİBERT, R. J., ROHOZİNSKİ, R., MANCHANDA, A., VİLLENEUVE, N., & WALTON, G. M. F. (2009). **Tracking ghostnet: Investigating a cyber espionage network.pp.5-6.**

DELGADO. A.(2016). **Technoscience and Citizenship: Ethics and Governance in the digital Society,** Volume 17, Bergen, Norveç, Springer p.18.

DEMİR, B.(2016). E-Ticarette Tüketicilerin Güvenlik ve Risk Algılarının Değerlendirilmesi Yayınlanmış Yüksek Lisans Tezi. **Yaşar Üniversitesi, S.B.E.** İzmir.

DEMİRAL FATİH,(2004), Deloitte, "**Bilgi Güvenliği Bilincinin Genele Yayılması**" ss.1,7," http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/50_45_1.pdf "Çevrimiçi" Erişim:24.07.2018

DURMUŞ. B, S.YURTKORU, M. ÇİNKO (2016).**Sosyal Bilimlerde SPSS'le Veri Analizi**, 6. Baskı, İstanbul, Beta Basım Yayım Dağıtım A.Ş.

DİJLE, H., & DOĞAN, N. (2011). Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı**. International Journal of InformaticsTechnologies**, *4*(2).ss.43-53.

DİLSİZ, R.(2012). Hack, Hacker ve Siber Kültür. **XVII. Türkiye'de İnternet Konferansı,** Anadolu Üniversitesi İletişim Bilimleri Fakültesi, Eskişehir.7-9 Kasım,2012,ss,135-136).

DÖNMEZ, O.(2015).Sınıf öğretmeni adaylarının çocukların karşılaştığı çevrimiçi risklere yönelik algılarının çeşitli değişkenler açısından incelenmesi. Yayınlanmış Doktora Tezi. **Anadolu Üniversitesi, E.B.E** Eskişehir.

ERİŞ, U. (2009). Türkiye' de Kırıcı(Hacker) Kültürü. Yayınlanmış Doktora Tezi, **Anadolu Üniversitesi, S.B.E.** Eskişehir. ss.1-11.

Erişim Tarihi:25.11.2018

EROL, S.E (2016). Siber Güvenlik Farkındalığı için Yetenek Tabanlı Dinamik Model Yayınlanmış Yüksek Lisans Tezi, **Gazi Üniversitesi, F.B.E.** Ankara. Ss.52-87.

ESCOBAR-RODRÍGUEZ, T.& CARVAJAL-TRUJİLLO, E. (2013). Online drivers of consumer purchase of website airline tickets. **Journal of Air Transport Management,** 32, 58–64.

FRİSCHMANN, B. (2014). **Human-focused Turing tests: A framework for judging nudging and techno-social engineering of human beings**.ss.2-3.

GÜLMÜŞ, M.(2010) Kurumsal Bilgi Güvenliği Yönetim Sistemleri Ve Güvenliği. Yayınlanmış Yüksel Lisans Tezi, **Yıldız Teknik Üniversitesi, F.B.E**. İstanbul. s.3.

GÜNDÜZ, M. Z. & RESUL, D. (2016). **Sosyal Mühendislik Yaygın Ataklar ve Güvenlik Önlemleri.** ISCTURKEY, *9*, 11-18.

HADNAGY, C.(2011) **Social Engineering The Art Of Human Hacking** United States of America**,** Richard Swadley.

HALİS, B. (2012). Tüketimin değişen yüzü: Elektronik ticaret uygulamaları ve sosyal paylaşım ağlarının rolü/The changing face of consumption: E-commerce applications and the role of social networks. **Journal of History Culture and Art Research**, *1*(4), 149-160.

HATHAWAY, O. A.CROOTOF, R. LEVİTZ, P., NİX, H., NOWLAN, A., PERDUE, W., & SPİEGEL, J. (2012). **The law of cyber-attack.** ***California Law Review***, pp.817-885.

HOFFMAN, D. L.NOVAK, T. P., & PERALTA, M. (1999). Building consumer trust online**. Communications of the ACM**, *42*(4), 80-85.

HOOPER, D. COUGHLAN, J., & MULLEN, M. R. (2008). "Structural Equation Modelling : Guidelines for Determining Model Fit", **The Electronic Journal of Business Research Methods Volume 6 Issue 1 pp. 53–60.**

IGURE, V. M., LAUGHTER, S. A., & WİLLİAMS, R. D. (2006). **Security issues in SCADA networks.** *Computers & Security*, *25*(7), 498-506.

IRMAK, E., & ERKEK, İ. **Endüstriyel Kontrol Sistemleri ve SCADA Uygulamalarının Siber Güvenliği**: Modbus TCP Protokolü Örneği. Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, 6(1), 1-16.

İPEK H. (2000). **Önemli Bir Sorun: Kara Para ve Kara Paranın Aklanması**. Beta Yayınları:İstanbul.

JAGATİC, T. ve :diğerleri (2007**). Social Phishing.** Communications of the ACM, *50*(10), 94-100

JOHN.N. GATHEGİ. Social Media Networking Literacy: Rebalancing Sharing, Privacy, and Legal Observance**, Information Leteracy, Lifelong Learning and Digital Citizenship in the 21st Century** Second European Conferance, ECIL, 2014, Dubrovnik, Croatia, October 20-23-2014. Pp.101.

KABAKUŞ, A. T., DOĞRU, İ. A., & ÇETİN, A. (2015). Android kötücül yazılım tespit ve koruma sistemleri. **Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi**, 31(1), 9-16.

KANTARCI, Ö. ÖZALP, M. SEZGİNSOY, C., ÖZAŞKINLI, O., & CAVLAK, C. (2017). Dijitalleşen Dünyada Ekonominin İtici Gücü: E-Ticaret. **TUSIAD Yayınları**, İstanbul.

KARA, M.(2013).Siber Saldırılar- Siber Savaşlar ve Etkileri**.** Yayınlanmış Yüksek Lisans Tezi, **İstanbul Bilgi Üniversitesi, S.B.E**. İstanbul. s-11.

KARTAL, M. T. (2018). Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme (Protection of Personal Data: A Conceptual Evaluation Upon Turkish Banking Sector).**Uluslararası Ekonomi ve Yenilik Dergisi**, 4 (1) 2018,1-18.

KAYA, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi. **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,** *69*(1-2), 317-334.

KAYACAN, B. VE GÜLTEKIN, Y.S. (2012). "Yapısal Eşitlik Modellemesinin (YEM) Ormancılıkta Sosyo-ekonomik Sorunların Çözümlenmesinde Kullanımı", I**II. Ormancılıkta Sosyo-Ekonomik Sorunlar Kongresi, İstanbul Üniversitesi, Orman Fakültesi 18-20 Ekim 2012.**

KILINÇ, İ.(2015).Lise öğrencilerinin siber duyarlılık, internet bağımlılığı ve sosyal değerlerinin incelenmesi**.** Yayınlanmış Yüksek Lisans Tezi. **Necmettin Erbakan Üniversitesi, E.B.E.** Konya

KİM, M. J. CHUNG, N., & LEE, C. K. (2011). The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. **Tourism Management,** *32*(2), 256-265.

KLOPPİNG, I. M. AND MCKİNNEY, E. (2004), Information Technology, **Learning, and Performance Journal**, 24(1), 35-47.

KOCADAĞ, T. (2012). Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi.

KORHAN, S. Siber Uzayda Aktör-Güç İlişkisi. **Cyberpolitik Journal**, *2*(4), 75-104.

KUTLU, Ö. &KAHRAMAN, S. (2017). Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi. **Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi,** *5*(4).

KÜÇÜK, S (2016). Siber Zorbalık Ölçeği Türkçe Uyarlaması. Yayınlanmış Yüksek Lisans Tezi, **İstanbul Üniversitesi, Adli Tıp Enstitüsü,** İstanbul. s.10.

KÜÇÜKYILMAZLAR, A. (2006). Elektronik Ticaret Rehberi**. İTO Yayınları** *:İstanbul.*

LONG, J.(2008) **"Chapter 5 Social Engineering" No Tech hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing,** Ed: Scott Pinzon, CISSP, 2008,ABD, Elsevier, Inc.112,113

LİNGYUN, Q. AND DONG, L.(2008), Applying TAM in B2C E-Commerce Research: An extended model, **Tsinghua Science & Technology**, 13(3), 265-272.

MAHMOOD, M. A., SİPONEN, M., STRAUB, D., RAO, H. R., & RAGHU, T. S. (2010). **Moving toward black hat research in information systems security: an editorial introduction to the special issue**. MIS quarterly, *34*(3), 431-433.

MANN, I.(2008) "**Hacking the Human Techniguesand Security Countermeasures**" Gover e-Book, s.177.

MARANGOZ, M.(2018).Tüketici Mahremiyetinin Korunması: Sorumlular Ve Yöntemler Üzerine Nitel Bir Araştırma. **Journal of Academic Researches and Studies,** *10*(19), 474-488.

MEYDAN, C.H VE ŞEŞEN, H (2011). **"Yapısal Eşitlik Modellemesi AMOS Uygulamarı**". Detay Yayıncılık, Ankara.

MITNICK. D. KEVIN and SİMON L.WİLLİAM (2017) **Aldatma Sanatı, Bilgi Güvenliğinde İnsan Faktörünün Kontrolü**. 8. Basım . ODTÜ Yayıncılık.

MOHAMAD EL-HASSAN (2016).Hizmet Sektöründe Online Alışveriş Davranışını Etkileyen Faktörler: Seyahat Sektörü (Türkiye ve Slovenya Karşılaştırması). Yayınlanmış Yüksek Lisans Tezi. **Mersin Üniversitesi S.B.E**.Mersin, 2016, s.43.

MONTAGUE, D.(2011).**Essentıals of Online Payment Security and Fraud Prevention.** Printed in the United States of America. Pulished by John Wiley&Sons, Inc.Hoboken, New Jersey Published Simultaneouslyin Canada.2011.Pp.32-34.

MOORE. A & EDWARDS.L.J.(2014) **CYBER SELF DEFENSE, Expert advice to Avoid Online, Predators, Identity Theft, and Cyberbullying,** Lyons Press, ss.160-166.

MOSSBERGER, K., TOLBERT, C. J., & MCNEAL, R. S. (2007). **Digital citizenship: The Internet, society, and participation**. MIt Press. The MIT Press Cambridge, Massachusetts London, England, Pp.1-19.

NAKİP, M. (2006). "**Pazarlama Araştırmaları: Teknikler ve (SPSS Destekli) Uygulamalar**"2. Baskı Ankara Seçkin Yayıncılık, ISBN: 975 02 0310 0

ÖĞÜN, M. N. & Adem, KAYA. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler**. Güvenlik Stratejileri Dergisi**, *18*(18).

ÖNDER, Ş. (2018). ISO 27001 Standardı Kapsamında Kurumsal Bilgi Güvenliği ve İşletme Performansı Arasındaki İlişki: BIST 100 Endeksinde Yer Alan İşletmeler Üzerine Bir Uygulama**. Ekonomik ve Sosyal Araştırmalar Dergisi**. ss.89-97.

ÖZKIRIŞ, B. (2010). "Tüketicinin İmajı İle Marka İmajı Arasındaki Uyumun, marka Sadakati Üzerine Etkileri", **Gebze Yüksek Teknoloji Enstitüsü, Sosyal Bilimler Enstitüsü**, İşletme Anabilim Dalı, Doktora Tezi, Gebze.

ÖZTÜRK, M.(2015).Ortaokul öğrencilerinin dijital vatandaşlık düzeyleri. Yayınlanmış Yüksek Lisans Tezi. **Kastamonu Üniversitesi, S.B.E.**Kastamonu.

RAHMAN, K. M. (2018). A **Narrative Literature Review and E-Commerce Website Research.** arXiv preprint arXiv:1806.07833.Pp.8-9.

RİBBLE, M.:G. BAİLEY (2007).**Digital Citizanship in Scholls, Washington**, ABD, Book Publishing İste.Pp.130

SAİT GÜRBÜZ, FARUK ŞAHİN, Sosyal Bilimlerde Araştırma Yöntemleri, Felsefe – Yöntem –Analiz, 3. Baskı, Seçkin Yayıncılık, 2016, Ss.103-140.

SALVATORE J.STOLFO Ve diğerleri (2008).**Insider Attack And Cyber Security Beyond The Hacker**. New York, ABD, Springer Science +Business Media, LLC. Pp.10-15.

SAMANİ, R. AND MCFARLAND, C. (2014). Hacking the Human Operating System: The Role of Social Engineering within Cybersecurity. Technical Report, Intel Security McAfee, July 2014.

SCHERMELLEH-ENGEL, K. MOOSBRUGGER, H. VE MÜLLER, H. (2003). "Evaluating the Fit of Structural Equation Models: Tests of Significance and Descriptive Goodness-of-Fit-Measures". **Methods of Psychological Research Online** *2003, Vol.8, No.2, pp. 23-74.*

SCHUMACKER, R. E AND LOMAX, R. G. (2004). "**A Beginner's Guide to Structural Equation Modeling, Second Edition**". Lawrence Erlbaum Associates. U.S.A

SHAFQAT, N. & MASOOD, A. (2016). Comparative analysis of various national cyber security strategies. **International Journal of Computer Science and Information Security,** 14(1), 129.

SHALHOUB, Z.K: AL QASİMİ, S.L(2010).**Cyber Law And Cyber Security İn Developing And Emerging Economies.** Edward Elgar Publishing, Inc.Pp.230-232).

SHİRSAVAR, H. A. GİLANİNİA, S. & ALMANİ, A. M. (2012). A study of factors influencing positive word of mouth in the Iranian banking industry. **Middle-East Journal of Scientific Research, 11(4), 454-460.**

SÖNMEZ, Ü.(2017) Bilişim Sistemleri Aracılığıyla Dolandırıcılık Suçu**. Dicle Üniversitesi Adalet Meslek Yüksekokulu Dicle Adalet Dergisi,** *1*(2), ss.48-50.

SUH, B.& HAN, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. **International Journal of Electronic Commerce**, 7(3), 155.

SUH, B. AND HAN, I.(2002), Effect of trust on customer acceptance of Internet banking, **Electronic Commerce Research and Applications**, 1(3-4), 247-263.

SHAHRYAR SUHEİL (2005), **The Secure Online Busıness handbook e-commerce, IT functionality& business continuity**, consultant editör: Jonathan Reuvid, thirt edition, Printed and bound in Great Britain by Cambridge University Press, Kogan Page Limited (2005).Pp.33-48.

ŞAHİNASLAN, Ö. ŞAHİNASLAN, D. E. BORANDAĞ, D. E. & ŞAHİNASLAN, D. M. (2013). Güvenli Bir Toplumun İçin Son Kullanıcı Siber Güvenliği.

ŞAHİNASLAN, Ö.(2013). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma. Yayımlanmış Doktora Tezi. **Trakya Üniversitesi, F.B.E**. Edirne. s.7-78.

ŞİMŞEK D. V. & ÇINAR, O.(2016). E-Ticaret ve Siber İşlemler. T.C.İSTANBUL TİCARET ÜNİVERSİTESİ. **Dış Ticaret Enstitüsü Tartışma Metinleri**. WPS NO/45/2016-06.Ss.1-19.

ŞİMŞEK, Ö. F (2007). "**Yapısal Eşitlik Modellemesine Giriş: Temel İlkeler ve LISREL Uygulamaları"**. Ankara. Ekinoks Yayınları,

TANRIKULU, T. KINAY, H. & ARICAK, O. T. (2011). "Siber Zorbalığa İlişkin Duyarlılık Ölçeği".İzmir XI. **Ulusal Psikolojik Danışma ve Rehberlik Kongresi Bildiri Özetleri Kitabı.**

TAT, M. (2007).Zihin dili programlaması (NPL)nin kişisel gelişim ve kişiler arası iletişim üzerindeki etkileri. Yayınlanmış Doktora Tezi. **Ege üniversitesi, S.B.E.** İzmir**.**

TAYLOR, S., & TODD, P. A. (1995). **Understanding İnformation Technology Usage: A Test Of Competing Models**. Information Systems Research, 6(2), 144-176.

TERZİ, N.(2011). The impact of e-commerce on international trade and employment. **Procedia-Social and Behavioral Science**s, 24, 745-753.

TEWKSBURG, D.AND RİTTENBERG, J.(2012). **News on the Internet Information and Citizenship in the 21st Century.**Published by Oxford Üniversity Press, Inc. New York, Ünited States of America. Pp.119.

TONTA, Y. (2009). **Dijital Yerliler, Sosyal Ağlar Ve Kütüphanelerin Geleceği.** Türk Kütüphaneciliği, 23(4), 742-768.

TOSUN, A (2015). İnsan Zafiyetlerini İstismar Ederek Yapılan Sosyal Mühendislik Saldırılarının Siber Güvenlik İle İlişkilendirilmesi: Türkiye Örneği. Yayınlanmış Yüksek Lisans Tezi. **Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü**. Ankara. ss.8-15

TURAN, M,&KÜLCÜ, Ö. (2013) Türk Ceza Kanunu Çerçevesinde Bilişim Suçlarına Dönük Yargıtay Kararlarının Analizi. ÜNAK 2013 Konferansı, 12.sayfa,14-23.

TURAK, Y.& BECENİ, A. Y. (2018**). Nesnelerin İnterneti ve Güvenliği.** s.3.

TURBAN, E. OUTLAND, J.KİNG, D.LEE J.K.LİANG T.P.(2018). **Electronic Commerce 2018 A Managerial and Social Networks Perspective** Ninth Edition,Cham, Switzerland,Springer International Publishing AG 2018, Pp, 362-364.

TÜRKMAN, S. (2014). Kore Savaşı Ve Türkiye'nin Nato'ya Girişi. **Türk Dünyası İncelemeleri Dergis**i,131-148

ÜNAL TATAR,(2011).“Sosyal Mühendislik Saldırıları”, **4. Ağ ve Bilgi Güvenliği Sempozyumu**, **Tübitak Bilgem**, Ankara, 25-26 Kasım 2011,s.11.

ÜNVER, M. CANBAY, C. & MİRZAOĞLU, A. G. (2009). Siber Güvenliğin Sağlanması: Türkiye’deki Mevcut Durum ve Alınması Gereken Tedbirler. **Bilgi Teknolojileri ve İletişim Kurumu** *(BTK), Ankara.*

VON SOLMS, R., & VAN NİEKERK, J. (2013). **From information security to cyber security. computers & security,** *38*,s. 97

VROMEN. A (2017).**Digital Citizenship And Political Engagement**. The Challenge From Online Campaigning and Advocacy Organisations, London, United Kingdom, Springer Nature,Pp.225-227.

VURAL, Y. & SAĞIROĞLU, Ş. (2011). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler**. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi**, 26(1). ss.97-102.

VURAL, Z. & BAT, M. (2010). Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim Fakültesine Yönelik Bir Araştırma. **Journal Of Yasar University**, *5*(20).

YALÇIN, N.& GÜRBÜZ, F. (2015**). Sosyal Ağlarda İşlenen Suçlar, Facebook Sosyal Ağı Örneği**. Akademik Bilişim Konferansi, ss2, 2015.

YANIK, A.(2014).Yeni Medya Kullanımımdaki Akış Deneyiminin Risk Algısı ve Online Turistik Satın Alma Niyetine Etkisi. Yayınlanmış Doktora Tezi. **Adnan Menderes Üniversitesi, S.B.E**.Aydın.

YAVANOĞLU, U. SAĞIROĞLU, Ş, & ÇOLAK, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. **Politeknik Dergisi**, *15*(1).

YAYLA, M. (2013). Hukuki Bir Terim Olarak Siber Savaş. **TBB Dergisi,** 104, 194-198.

YAZICI, A. (2008). Yeni Karapara Aklama Yöntemleri Olarak Akıllı Artlar Ve Internet. **Anadolu University Journal of Social Sciences, 8(2).**

YILDIRIM, N. & VAROL, A.(2013). Sosyal ağlarda güvenlik: Bitlis Eren ve Fırat Üniversitelerinde gerçekleştirilen bir alan çalışması. **Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 6(1).**

YILMAZ, O.(2017) Küreselleşme Sürecinde Dönüşen Güvenlik Algısı Ve Siber Güvenlik. **Cyberpolitik Journal**, *2*(4), s.24.

YÜCENUR G.N., ÇETİN DEMİREL N, CEYLAN C., DEMİREL T. (2011). "Hizmet Değerinin Müşterilerin Davranışsal Niyetleri Üzerindeki Etkisinin Yapısal Eşitlik Modeli ile Ölçülmesi**," Doğuş Üniversitesi Dergisi, Sayı: 12(1), ss. 156-168,**

ZEYDAN, Ö.(2006). **Kişisel bilgisayarlar ve internet güvenliği**. *XI*." Türkiye'de İnternet" Konferansı, 21-23.s.

ZORBA. M.E.(2013) **Sosyal Mühendislik Nedir ve Örnek Senaryolar**."Çevrimiçi" https://www.merdincz.com/Sosyal-Muhendislik-Ornek-Senaryolar/ Erişim:08.08.2018

İNTERNET KAYNAKLARI

http://ec.europa.eu/growth/single-market/single-digital-gateway_en Erişim Tarihi: 11.02.2019

http://www.bilgimikoruyorum.org.tr/?b321_sosyal_muhendislik_giris.Tehditler ve Korunma Yöntemleri: Sosyal Mühendislik. Tübitak Bilgem. Erişim Tarihi: 01.07.2018

http://www.econsumer.gov. Çevrimiçi Uluslararası Dolandırıcılık Bildiriminde Bulunma Sitesi. Erişim Tarihi:22.08.2018.

http://www.emo.org.tr/ekler/288230da37dbf3c_ek.pdf Erişim Tarihi: 25.07.2018

http://www.ensonhaber.com/pearl-harbor-saldirisi-nedir-2012-02-27.html. Keylogger Nedir, Erişim Tarihi: 19.08.2018

http://www.havelsan.com.tr/files/files/document/6092016095748459_havelsan-aylik-siber-guvenlik-bulteni-agustos-2016-sayisi.pdf Erişim Tarihi:19.11.2018

http://www.hgm.gov.tr/tr/haber/107 Erişim Tarihi: 08.11.2018.

http://www.milliyet.com.tr/6-trilyon-dolarlik-siber-risk-teknoloji-haber-2693138/Erişim Tarihi:22.11.2018

http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm Erişim Tarihi 08.11.2018

http://www.resmigazete.gov.tr/eskiler/2015/07/20150715-4.htm Erişim Tarihi: 26.12.2018.

http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf Erişim Tarihi: 08.11.2018

http://www.udhb.gov.tr/images/istatistik/2003-2017.pdf Erişim Tarihi: 08.11.2018.

http://www.wikizeroo.net/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvU0NBREE Scada, Erişim Tarihi:06.11.2018

https://bid.usak.edu.tr/upload/bid/p7eDmMI3d2_1418807372-USOM-SGFF-004-Akilli%20Telefonlar%20ve%20Guvenlik.pdf Erişim Tarihi 24.11.2018

https://ec.europa.eu/docsroom/documents/33287 Erişim Tarihi: 12.02.2019.

https://eksisozluk.com/shodan--269965 Erişim Tarihi: 30.11.2018

https://evidence2e-codex.eu/ Erişim Tarihi: 07.11.2018.

https://home.kpmg.com/tr/tr/home/media/press-releases/2017/08/bilgisayar-korsanlarinin-gozu-ceolarda.htm Bilgisayar Korsanlarının Gözü CEOLAR'da. Erişim Tarihi:10.07.2018

https://iplogger.org/ IP Adreslerine Ulaşma Sitesi. Erişim Tarihi:08.08.2018

https://law.resource.org/ Erişim Tarihi: 12.02.2019

https://public.resource.org/ Erişim Tarihi: 12.02.2019

https://support.google.com/chrome/answer/95617?visit_id=636698816329925449-528112417&p=ui_security_indicator&rd=1 Erişim Tarihi: 13.12.2018.

https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=tr&oco=1 Erişim Tarihi: 14.12.2018.

https://support.google.com/websearch/answer/106318?hl=tr Kimlik Avı Saldırılarını Önleme ve Bildirme. Erişim Tarihi:17.07.2018

https://tiss.gtb.gov.tr/ Erişim Tarihi: 26.12.2018.

https://tuketici.btk.gov.tr/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi Erişim Tarihi: 01.04.2019

https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-android.pdf . Erişim Tarihi: 26.11.2018

https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-ios.pdf Erişim Tarihi: 26.11.2018

https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-wind.pdf Erişim Tarihi: 26.11.2018

https://tuketici.btk.gov.tr/uploads/pages/tuketiciler-icin-akilli-telefon-guvenlik-ipuclari-guncellendi/smartphone-sec-bbery.pdf Erişim Tarihi: 26.11.2018

https://visa.com.tr/bireysel-kartlar/guvenli-internet-alisverisi/verified-by-visa/ Erişim Tarihi: 04.11.2018

https://www.btk.gov.tr/siber-guvenlik-kurulu Erişim Tarihi: 01.12.2018

https://www.btk.gov.tr/uploads/pages/bilgi-teknolojileri-ve-iletisim-kurumu-2016-faaliyet-raporu-yayimlandi/2016-faaliyet-raporu.pdf s.96.Erişim Tarihi:08.11.2018

https://www.cnnturk.com/ekonomi/dunya/alman-ordusu-siber-guvenlik-ajansi-kuruyor Erişim Tarihi 21.11.2018

https://www.econsumer.gov/tr/AboutUs#crnt Erişim Tarihi: 27.12.2018.

https://www.econsumer.gov/tr/ComplaintTrend#crnt Erişim Tarihi: 27.12.2018.

https://www.econsumer.gov/tr/OtherSteps/OtherSteps/17#crnt Erişim Tarihi: 27.12.2018.

https://www.enisa.europa.eu/about-enisa Erişim Tarihi: 07.11.2018.

https://www.findeks.com/findeks-hakkinda Findeks Kredi Kayıt Bürosu Hakkında, Erişim Tarihi: 20.08.2018.

https://www.ftc.gov/contact Federal Ticaret Komisyonu Sitesi. Erişim Tarihi: 08.07.2017

https://www.globalnet.com.tr/ssl-guvenlik-sertifikasi-almalisiniz-ama-neden.html Erişim Tarihi: 08.02.2019.

https://www.internetyardim.org.tr/ Erişim Tarihi:01.12.2018

https://www.interpol.int/ Erişim Tarihi: 07.11.2018.

https://www.interpol.int/Crime-areas/Cybercrime/Online-safety Erişim Tarihi: 19.11.2018.

https://www.iste.org/ Erişim Tarihi: 28.11.2018

https://www.itu.int/en/about/Pages/whatwedo.aspx Erişim Tarihi: 07.11.2018.

https://www.kaspersky.com/free-virus-scan Erişim Tarihi: 19.11.2018

https://www.kkb.com.tr/uyelik Kredi Kayıt Bürosu Kurumsal Üyelik, Erişim Tarihi: 20.08.2018.

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf Erişim Tarihi:16.12.2018.

https://www.nsa.gov/resources/students-educators/#cae Erişim Tarihi: 30.10.2018

https://www.sabah.com.tr/teknoloji/2018/03/19/dunyada-3-milyar-190-bin-kisi-sosyal-medya-kullaniyor Erişim Tarihi: 26.11.2018

https://www.sabah.com.tr/teknoloji/2018/10/20/turkiyenin-sosyal-medya-karnesi-aciklandi Erişim Tarihi: 26.11.2018

https://www.shodan.io/explore Erişim Tarihi: 30.11.2018

https://www.titanium-project.eu/ Erişim Tarihi: 07.11.2018.

https://www.trendmicro.com/tr_tr/forHome/products/housecall.htmlErişim Tarihi: 19.11.2018

https://www.trthaber.com/haber/dunya/abd-siber-guvenlik-icin-bagimsiz-komutanlik-kurdu-363976.html Erişim Tarihi:21.11.2018

https://www.turkhackteam.org/sosyal-muhendislik/1057188-bir-sosyal-muhendis-nasil-dusunur.html Bir Sosyal Mühendis Nasıl Düşünür? Erişim Tarihi: 20.07.2018

https://www.turkhackteam.org/sosyal-muhendislik/1507546-sosyal-muhendislikten-korunma-yollari-t3rmin4tor.html Sosyal Mühendislikten Korunma Yolları, 2018. Erişim Tarihi: 05.08.2018

https://www.turkiye.gov.tr/bilgi-teknolojileri-ve-iletisim-kurumuErişim Tarihi:09.11.2018

https://www.usgf.org.tr/federasyon/tuzuk/ Erişim Tarihi: 07.11.2018.

https://www.usom.gov.tr/index.html Ulusal Siber Olaylara Müdahale Merkezi Erişim Tarihi: 05.09.2018.

https://www.visa.com.tr/bizimle-isbirligi-yapin/payment-technology/visa-checkout.html Erişim Tarihi: 04.11.2018

https://www.whois.net/ Web sitesi adresi sorgulama**.** Erişim Tarihi: 09.11.2018

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf Erişim Tarihi: 17.03.2019

https://gazeteistanbul.com/galata-koprusunu-satan-efsanevi-dolandirici-sulun-osman/ Erişim Tarihi: 19.03.2019.

https://www.youtube.com/watch?v=xX04wGyHW6Q Erişim Tarihi: 19.03.2019

https://www.nato.int/nato-welcome/index.html Erişim Tarihi: 30.03.2019

https://www.ihbarweb.org.tr/ Erişim Tarihi: 30.03.2019

https://www.egm.gov.tr/sayfalar/ihbar.aspx Erişim Tarihi: 30.03.2019

https://www.kvkk.gov.tr/Icerik/4118/Videolar Erişim Tarihi: 01.04.2019

http://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm Erişim Tarihi: 24.05.2019

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf Erişim Tarihi: 24.05.2019

EKLER

EK: 1. Rektörlük Anket İzin Yazısı

EK:2. Etik Kurul Değerlendirme Formu

EK: 3.Onaylı Anket Formu

EK:1- Rektörlük Anket İzin Yazısı

Evrak Tarih ve Sayısı: 06/02/2019-E.1507

T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ REKTÖRLÜĞÜ
Genel Sekreterlik

BEL576MH

Sayı : 71646715-800-
Konu : Anket İzni Hk.

ÖMER SEYFETTİN UYGULAMALI BİLİMLER FAKÜLTESİ DEKANLIĞINA

İlgi : 24/01/2019 tarihli ve 1119 sayılı yazınız,

Fakülteniz öğretim elemanı Dr. Öğr. Üyesi Özer YILMAZ'ın danışmanlığını yürüttüğü Uluslararası Ticaret ve Lojistik Anabilim Dalı yüksek lisans öğrencisi Gülcihan AYDENER'in "Tüketicilerin Sosyal Mühendislik ile Siber Güvenlik Farkındalıklarının Online Alışveriş Niyetleri Üzerindeki Etkisinin Ölçülmesi" adlı yüksek lisans tezi kapsamındaki anket çalışmasını Üniversitemiz öğrencilerine uygulama isteği Rektörlüğümüzce uygun görülmüştür.

Bilgilerinizi ve gereğini rica ederim.

e-imzalıdır
Prof. Dr. Süleyman ÖZDEMİR
Rektör

EK:2. Etik Kurul Değerlendirme Formu

T.C. Bandırma Onyedi Eylül Üniversitesi Sosyal ve Beşeri Bilimler Etik Kurulu Değerlendirme Formu

Araştırmanın Başlığı:	Tüketicilerin Sosyal Mühendislik ile Siber Güvenlik Farkındalıklarının Online alışveriş Niyetleri Üzerindeki Etkisinin Ölçülmesi
Başvuru Formunun Etik Kurula geldiği tarih:	15/01/2019
Başvuru Formunun Etik Kurulda incelendiği tarih:	21/01/2019
Toplantı No. ve Karar tarihi:	2019/2 - 21/01/2019

SONUÇ

1.	■ Uygun	
2.	☐ Düzeltilmesi gereklidir: Etik sorun olabilecek sorular/maddeler, süreçler ya da unsurlar bulunmaktadır. Açıklama:	
3.	☐ Görevsizlik: Gerekçe, Görüş, Tavsiye ve Açıklamalar:	
4.	☐ Uygun değildir: Gerekçe, Görüş, Tavsiye ve Açıklamalar:	

Başvuru dosyasının incelenmesinde hazır bulunan ve araştırmayla doğrudan veya dolaylı olarak ilişkisi bulunmayan Etik Kurul başkan ve üyelerinin ad soyad ve imzaları

Prof. Dr. Gökhan ORHAN
Başkan

Prof. Dr. Burak DARICI
Üye

Doç. Dr. Tarhan OKAN
Üye

Dr. Öğr. Üyesi Ömür KIZILGÖL
Üye

Dr. Öğr. Üyesi Adnan UZUN
Üye

EK:3. Onaylı Anket Formu

Tüketicilerin Online Alışverişlerinde Sosyal Mühendislik ile Siber Güvenlik Farkındalığı Anketi: Değerli öğrenciler, bu araştırma ile tüketicilerin sosyal mühendislik ile siber güvenlik farkındalıklarının, Online alışveriş niyetleri üzerindeki etkisinin ölçülmesi, amaçlanmaktadır. Her bir soru için parantez içine X işareti koyunuz. Veriler yalnızca bilimsel amaçla kullanılır.

Öğrenci: Gülcihan AYDANER — Tez Danışmanı: Dr. Öğr. Üyesi Özer YILMAZ

1-Hiç Katılmıyorum
2-Katılmıyorum
3-Ne Katılıyorum Ne Katılmıyorum
4-Katılıyorum
5- Kesinlikle Katılıyorum

Size En Yakın Gelen Rakama X İşareti Koyunuz.

Katkılarınız için Teşekkür Ederiz.

	1. BÖLÜM A.SİBER GÜVENLİK FARKINDALIĞI					
1.	Herkesin erişimine açık bilgisayarlarda herhangi bir şifre gerektiren işlem yapmamaya özen gösteririm.	1	2	3	4	5
2.	Bilinmeyen kişi ve adreslerden gelen mailleri herhangi bir güvenlik açığı oluşmaması için okumayarak kimlik avı ve dolandırıcılık ile ilgili yerlere şikayet ederim.	1	2	3	4	5
3.	İhtiyaç duyduğumda ücretsiz yazılımları bilgisayarıma indirebilir veya kurabilirim.	1	2	3	4	5
4.	Web sitelerinin yardım güvenlik ve gizlilik gibi bölümleri olduğunu biliyorum ve kullanıyorum.	1	2	3	4	5
5.	İhbarda bulunacağım hat, web sitesi ve yasal kurumları bilirim.	1	2	3	4	5
6.	Bilgisayarımda lisansız yazılım kullanmaktan çekinirim.	1	2	3	4	5
7.	İnternet şifrelerimin güvenlik seviyelerini önemserim.	1	2	3	4	5
8.	Bilgileri dijital ortamlarda nasıl güvende tutmam gerektiğini biliyorum.	1	2	3	4	5
	B. SOSYAL MÜHENDİSLİK FARKINDALIĞI					
9.	İnternete girerken bilgilerimin başkaları tarafından çalınabileceğini göz önünde tutarım.	1	2	3	4	5
10.	Sosyal paylaşım sitelerinde(Facebook, Twitter vb.) özel bilgilerimin başkaları tarafından kötü amaçlı olarak kullanılabileceğini göz önünde bulundururum.	1	2	3	4	5
11.	Sanal ortamlardayken bir bilgisayar korsanının benim içinde tehlike oluşturabileceğini göz önünde bulundururum.	1	2	3	4	5
12.	İnternette tanımadığım insanlarla iletişim kurmam.	1	2	3	4	5
13.	İnternete girdiğimde internetin aynı zamanda başkalarına zarar verme amacıyla kullanılabileceğini aklımda tutarım.	1	2	3	4	5
14.	Sosyal paylaşım sitelerinde bilgilerim herkese açık değildir.	1	2	3	4	5
15.	Yaptığım her şeyi sosyal medyada paylaşmayı sevmem (facebook, twitter, instagram vb.)	1	2	3	4	5
	C. ONLİNE ALIŞVERİŞ NİYETİ					
16.	Gelecekte internet üzerinden alışveriş yapmaya devam etme niyetindeyim.	1	2	3	4	5
17.	Her zaman internet üzerinden alışveriş yapmak için çaba göstereceğim.	1	2	3	4	5
18.	İnternet üzerinden alışveriş yapmak hayatımı daha cazip hale getirir.	1	2	3	4	5
19.	İnternet üzerinden alışveriş yapmayı arkadaşlarıma tavsiye ederim.	1	2	3	4	5

ARKA SAYFAYA GEÇİNİZ.

2.BÖLÜM

Genel Değerlendirme Anketi (Siber Güvenlik-Sosyal Mühendislik-Online Alışveriş)

1. Cinsiyetiniz:	Kadın ( ) Erkek ( )
2. Yaşınız:	18-25 ( ) 25-30 ( ) 30 ve üzeri ( )
3. Güvenli internet kullanımı konusunda bir eğitim aldınız mı?	Evet ( ) Hayır ( )
4. Bilgi güvenliği hakkında ne kadar bilgi sahibisiniz?	Yeteri kadar biliyorum ( ) Çok az bir bilgim var ( ) Herhangi bir bilgim yok ( )
5. Bilgisayarınıza format attığınızda veya bir dosyayı sildiğinizde dosya kaybolur.	Doğru ( ) Yanlış ( )
6. Flash diskten (USB/SD Card vb.)bir dosyayı sildiğinizde silinen dosya geri getirilemez.	Doğru ( ) Yanlış ( )
7. Bilgisayarınız saldırıya uğradığında neler yapmanız gerektiğini biliyor musunuz?	Evet, ne yapmam gerektiğini biliyorum ( ) Hayır bilmiyorum ( )
8. Bilgisayarınızın saldırıya uğradığını veya virüs vb. zararlı yazılımların bulaştığını anlar mısınız?	Evet, anlarım ( ) Hayır, anlayamam ( )
9. Çevrenizde internet kaynaklı bir sorun (bilgi hırsızlığı, rahatsız edilme, e-dolandırıcılık yaşayan kimse oldu mu?	Evet ( ) Hayır ( )
10. E-posta ile gelen ekleri açarken nasıl davranırsınız?	Beklediğim kişiden geldiğine emin olurum ( ) Bildiğim yerden geldiyse güvenliğe dikkat etmem ( ) Dikkat etmem ( )
11. Oltalama (phishing) ataklarını duydunuz mu?	Evet, duydum ( ) Hayır, duymadım ( )
12. Sosyal medya üzerinden (Facebook, instagram, twitter vb.) hiç kimseyi akrabanız olarak gösterdiniz mi? Gösterdiyseniz bu bilgi herkese açık mı?	Evet, gösterdim. Bilgi herkese açık ( ) Evet ama sadece arkadaşlarım görüyor ( ) Hayır, göstermedim. ( )
13. Google'dan aranıldığında sosyal ağ profiliniz çıkıyor mu?	Evet ( ) Hayır ( )
14.Tanımadığınız birini sosyal ağlarda arkadaş olarak eklediniz mi?	Evet ( ) Hayır ( )
15. Sosyal ağda paylaştığınız verilerin, birileri tarafından kayıt altına alındığı bir durumla karşılaştınız mı?	Evet ( ) Hayır ( )
16. İnternetten alışveriş yapıyorum.	Evet ( ) Hayır ( )
17. İnternette yaptığınız alışverişlerde 3D secure (Cep telefonuna doğrulama mesajı) kullanmaya dikkat ediyor musunuz?	Evet ( ) Hayır ( )
18. İnternetten alışveriş yapma deneyiminiz ne kadardır?	1-5 kez ( ) 5-10 kez ( ) 10 ve üzeri ( ) Hiç ( )
19. İnternette bir kerede en fazla ne kadarlık alışveriş yapmayı düşünürsünüz?	En fazla 100 TL ( ) 100-500 TL ( ) 500-1000 TL ( ) 1000 TL den fazla ( )
20. İnternet alışverişlerinizin önümüzdeki 5 yıl içerisinde tüm alışverişlerinizin yaklaşık ne kadarını oluşturacağını düşünüyorsunuz?	%5 ten az ( ) % 5-10 arası ( ) %10-20 arası ( ) % 20'den fazla ( )