T.C.
MUNZUR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ÜNİVERSİTE ÖĞRENCİLERİNİN SİBER GÜVENLİK FARKINDALIKLARININ BELİRLENMESİ

FATMA ÇAKAN

YÜKSEK LİSANS TEZİ
İŞLETME ANABİLİM DALI

DANIŞMAN
Prof. Dr. Arzu KARACA

TUNCELİ – 2024

T.C.
MUNZUR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ÜNİVERSİTE ÖĞRENCİLERİNİN SİBER GÜVENLİK FARKINDALIKLARININ BELİRLENMESİ

FATMA ÇAKAN
(19120362)

YÜKSEK LİSANS TEZİ
İŞLETME ANABİLİM DALI

DANIŞMAN
Prof. Dr. Arzu KARACA

TUNCELİ – 2024

T.C
MUNZUR ÜNİVERİSTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ÜNİVERSİTE ÖĞRENCİLERİNİN SİBER GÜVENLİK FARKINDALIKLARININ BELİRLENMESİ

Fatma ÇAKAN
YÜKSEK LİSANS TEZİ
İŞLETME ANABİLİM DALI

Bu yüksek lisans tezi 24/04/2024 tarihinde aşağıdaki jüri üyeleri tarafından **oybirliği** ile kabul edilmiştir.

Dr. Öğr. Üyesi Ayşe Esra PEKER (Fırat Üniversitesi) **BAŞKAN**	Prof. Dr. Arzu KARACA (Munzur Üniversitesi) **DANIŞMAN**	Dr. Öğr. Üyesi Eray Ekin SEZGİN (Munzur Üniversitesi) **ÜYE**

Bu tez, Enstitümüz Genel İşletme Anabilim Dalı'nda hazırlanmıştır.

Prof. Dr. Altuğ KAZAR
Enstitü Müdürü

24/04/2024

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analizve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygundavrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

Danışman

Fatma ÇAKAN

Prof. Dr. Arzu KARACA

TEŞEKKÜR

Öncelikle yüksek lisans eğitimim boyunca çalışmamın ilk aşamasından son aşamasına kadar beni destekleyen, cesaretlendiren ve yardımlarını esirgemeyen çok değerli hocam ve aynı zamanda danışmanım Prof. Dr. Arzu KARACA'ya katkılarından dolayı gönülden sonsuz teşekkür ederim. Ayrıca yüksek lisans eğitimi süresince desteklerini esirgemeyen İşletme Anabilim Dalının değerli tüm öğretim üyelerine teşekkür ederim.

Fatma ÇAKAN
Tunceli-2024

İÇİNDEKİLER

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

AKT	:Aktaran
ARK	:Arkadaşları
BGD	:Bilgi Güvenliği Derneği
CMK	:Ceza Muhakemeleri Kanunu
KMO	:Kaiser Meyer-Olkin
MEB	:Milli Eğitim Bakanlığı
STK	:Sivil Toplum Kuruluşları
TBD	:Türkiye Bilişim Derneği
TCK	:Türk Ceza Kanunu
VD.	:Ve Diğerleri
YÖK	:Yüksek Öğretim Kurulu

ÖZET

Günümüzde internetin hayatımızın vazgeçilmez bir parçası olduğu kabulünden hareketle gençlere bilinçli internet öğretmek gerekmektedir. Özellikle son dönemde gençlerin daha fazla bir şekilde siber suç mağduru oldukları gözlenmektedir. Hayatın her alanında internetin getirdiği olumlu gelişmelerden faydalanırken bir yandan da pek çok olumsuz eylem ve davranışlara da maruz kalmak söz konusudur. Her ne kadar siber güvenliği sağlamak için kişiler ve kurumlar teknik önlemler alıyor olsa da son kullanıcıdan kaynaklanan bilgisizlik ve ihmal siber güvenlik açıklarına yol açmakta ve siber suçları teşvik etmektedir. Her geçen gün farklı ve çok sayıda siber suç türleri geliştirilmektedir. Bu tür siber suçlardan korunmanın kullanıcıya düşen sorumluluğu; siber güvenliğin ne olduğunu ve siber güvenliğin nasıl sağlanacağını iyi bilmektir.

Bu noktadan hareketle, en fazla siber suç mağduru olan gençlerin siber güvenlik farkındalık düzeylerini belirlemeyi, araştırma bulguları doğrultusunda yasa yapıcılara, ebeveynlere, eğitimcilere ve nihayetinde gençlere birtakım öneriler geliştirmeyi amaçlayan bu nicel araştırma ilişkisel tarama modeli ile yapılanmıştır. Araştırmanın gerçekleştirilmesinde tesadüfi olmayan örnekleme yöntemlerinden kolayda örnekleme tekniği kullanılmıştır. Bu kapsamda üniversite öğrencilerine, demografik ve siber güvenlik farkındalığına yönelik sorular olmak üzere toplam 33 ifade yöneltilmiştir. Araştırma sonucunda üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin yüksek olduğu belirlenmiştir. Ayrıca siber güvenlik farkındalık düzeylerinde demografik değişkenlere göre (cinsiyet, yaş, bölüm, sınıf) anlamlı bir farklılık tespit edilmemiştir.

Gençlerin erken yaşlardan itibaren internet erişimine sahip olması nedeniyle, ebeveynlerin veya çocukların siber suçlar ve siber zorbalık gibi potansiyel risklerin farkında olması ve bilinçlendirilmesi önemlidir. Bu nedenle, çocukluktan başlayarak gençleri siber güvenlik farkındalığı kazandırmak gerekmektedir. Bu bağlamda ilkokuldan itibaren müfredatlara siber güvenlik dersi konulabilir ve siber suçlar hakkında toplumun farklı kesimlerine eğitimler, seminerler, verilebilir.

Anahtar kelimeler: Siber Güvenlik, Siber Güvenlik Farkındalığı, Üniversite Öğrencileri

ABSTRACT

Determinig Cyber Security Differences of University Studen

Today, the internet is an indispensable part of our lives and it is necessary to teach young people to use the internet consciously. Especially in recent times, it has been observed that young individuals are increasingly becoming victims of cybercrimes. While benefiting from the positive developments brought about by the internet in every aspect of life, exposure to numerous negative actions and behaviors is also prevalent. Despite efforts by individuals and organizations to ensure cybersecurity through technical measures, ignorance and negligence on the part of end-users contribute to cybersecurity vulnerabilities and encourage cybercrimes. Every day, various types of cybercrimes are being developed. The responsibility of protecting against such cybercrimes lies with the users; it is crucial for users to understand what cybersecurity entails and how it can be ensured.

From this point of view, this quantitative research, which aims to determine the cyber security awareness levels of young people, who are the most common victims of cybercrime, and to develop some suggestions for lawmakers, parents, educators and ultimately young people in line with the research findings, was conducted with the relational survey model. Convenience sampling technique, one of the non-random sampling methods, was used in the research. In this context, A total of 33 statements were directed to university students, comprising demographic and cybersecurity awareness-related questions. The research findings indicate that the level of cybersecurity awareness among university students is high. Furthermore, no significant difference in cybersecurity awareness levels was detected based on demographic variables (gender, age, department, class).

Due to the early access to the internet from a young age, it is crucial for parents or children to be aware of and educate children about potential risks such as cybercrimes and cyberbullying. Therefore, instilling cybersecurity awareness in young people from childhood is essential. In this context, cybersecurity lessons can be included in curricula starting from elementary school, and education sessions, seminars, can be provided to various sectors of society regarding cybercrimes.

Key Words: Cyber Security, Cyber Security Awareness, University Students

1. GİRİŞ

Dünyanın her yerinde olduğu gibi ülkemizde de internet kullanımı her geçen gün artmaktadır. Özellikle Covid 19 pandemi dönemi dijital dönüşümü hızlandırmış ve eğitimden, sağlığa, bankacılıktan eğlence sektörüne kadar pek çok alanda daha önce tecrübe edilmemiş iş yapış tarzları ve süreçlerinin yaşanmasına yol açmıştır. Pandemi döneminde bireysel ve kurumsal internet kullanımı çok daha fazla yaygınlaşarak elzem hale gelmiştir. Örneğin; sağlık, eğitim, ticaret, turizm vb. birçok alanda çalışan kurumlar, kuruluşlar, şirketler evden çalışma uygulamasına geçmiş ve bu durumda internet ve elektronik cihaz kullanımını artırmıştır. Özellikle pandemi sürecinde dijital oyunlara, TV platformlarına, sosyal medya uygulamalarına, çevrimiçi sohbet sitelerine yönelim çok artmış ve özellikle gençlerin kullanım oranları katlanarak devam etmektedir. Sadece online oyun platformlarında Türkiye'de yaklaşık 36 milyonu mobil oyuncu olduğu ve yaklaşık 880 milyon dolar oyuncu hasılatı toplandığı düşünüldüğünde olayın ciddiyeti daha iyi anlaşılacaktır (Sayar, 2022).

'We Are Social' sitesine göre internet kullanıcı sayısı dünya genelinde son yıllarda çok hızlı bir şekilde yükselmektedir. Türkiye'de ise Ocak 2023 tarihi verilerine göre 71,38 milyon (%83,4) internet kullanıcısı ve 62,55 milyon (%73,1) sosyal medya kullanıcısı vardır (We Are Social, 2023'ten akt., Zeytin ve Akkaş, 2023). Bu rakamlar 2022 yılında dünya nüfusunun %69'u ve Türkiye nüfusunun %83.8'i internet kullanıcısı olarak istatistiklere geçmiştir (Tokmak, 2023).

Türkiye İstatistik Kurumu verilerine göre internet kullanan kişilerin internet üzerinden özel kullanım niyetiyle ürün satın alma ya da ürün sipariş etme oranı, 2022 yılında %46,2'dir (TÜİK, 2023). Türkiye İstatistik Kurumunun (TÜİK) 2021 yılı verilerine göre internet erişimi olan hane sayısı 2011 yılında %45 iken on yılda %47 artışla %92 seviyesine ulaşmıştır. Bireylerde internet kullanımı 2011 yılında %42,9 iken yaklaşık %40 artış göstererek 2021 yılında %82,6 seviyesine ulaşmıştır. TÜİK'in 2002-2020 tarihleri arasında yapmış olduğu "Hane Halkı Bilişim Teknolojileri Kullanımı Araştırmasına" ilişkin anket sonuçlarına göre 2004 yılında evde internet erişimi olan hanelerin oranı %7 iken, bu oran 2020 yılında %90,7'ye yükselmiştir. Evlerde dizüstü bilgisayar, tablet ve notebook gibi taşınabilir bilgi işlem cihazlarına sahip olma oranı ise %0,9'dan %45,1'e yükselmiştir. Cep telefonu/akıllı telefon oranı %53,7'den %99,4'e yükselmiştir. İnternete bağlanabilen TV'ye sahip olma oranı 2013'te %7,3 iken, 2020'de %33,8'e olarak tespit edilmiştir (TÜİK, 2020).

Bir başka rapora göre ise 2018 yılında cep telefonu kullanımı %92,7 iken 2022 yılında bu oran %95,8 olmuştur. 2022 yılına bakıldığında 25-34 yaş aralığının %98,3 oranla en yüksek cep telefonu kullanımına sahip olduğu görülmektedir (TÜİK, 2023). Ayrıca mobil cihazlardaki bu artış ve endüstri 4.0'ın göstergelerinden biri olan nesnelerin interneti teknolojisinin yaygınlaşması toplumları hızlıca siber dünyaya entegre olduklarının birer göstergesidir.

Modern tarih boyunca, paradigma değiştiren yeniliklerin mümkün kıldığı sanayi devrimleri, ekonomileri ve toplumları iyi ve kötü yönde yeniden şekillendirmiştir. 1700'lerin ortalarından 1800'lere kadar mekanizasyon, fiziksel süreç verimliliğini radikal bir şekilde artırmak için demiryollarının, buhar motorunun ve makinelerin kullanımını içermiştir (Gelderblom ve Trivellato, 2019). Bunu, 1900'lerin başında, büyük ölçekte elektrikle çalışan yeni fiziksel üretim süreçlerinin geliştirilmesini, mamul malların fiyatlarının düşürülmesini ve tüketimciliğin körüklenmesini içeren seri üretim teknolojileri izlemiştir (Powell, 1987). Bilgisayar otomasyonu daha sonra 20. yüzyılın ortalarında, mal ve hizmetlerin üretiminin ve daha sonra tüketiminin doğasını değiştiren süreç verimliliğini artırmaya yönelik yeni dijital teknolojiler ve sistemler tarafından etkinleştirilerek ortaya çıkmıştır (Kling, 1980). Son zamanlarda değişimin ölçeği ve kapsamı, bilgi çağının bilgisayar otomasyonunu aşarak ve dördüncü bir sanayi devriminin ortaya çıkmasına yol açmıştır (Bordeleau ve Felden, 2019). Genellikle 4. Sanayi Devrimi, sosyal ve ekonomik dönüşümü yaratan, ayırt etme, karar verme, yaratma ve iş birliği yapma konusunda insan benzeri yeteneklere sahip makinelerin yaygın olarak ortaya çıkmasını ifade etmektedir. Örneğin, otonom bir depo robotu, kutuların ve paletlerin varlığını ayırt edebilir, uygun eyleme karar verebilir ve bunları öğrenilen ilkelere göre başka bir yere taşıyabilir, bir makine sanatçısı ise insanlar tarafından yaratılanlardan ayırt edilemeyen güzel görüntüleri hızla yaratabilir (Rombach ve ark., 2022). 4. Sanayi Devriminde, gelişen dijital teknolojilerin kombinasyonları fiziksel, dijital ve biyolojik sistemler arasındaki sınırları bulanıklaştırarak sistemik dönüşümü daha da hızlandırmaktadır. Böyle bir değişim ve dönüşüm son derece faydalı olmasının yanı sıra son derece riskli ve zarar verici de olabilir. Algılanan riskin bir göstergesi olarak, yapay zekâ sistemlerinin belirli kullanımlarını yasaklama ve düzenleme önerileri de dahil olmak üzere dijital teknolojileri hedef alan benzeri görülmemiş bir düzenleyici yasal girişim dalgası ortaya çıkmıştır (Wallace, 2020'den akt., Melville, Robert, ve Xiao, 2023).

1980'lerin başında internetin doğuşundan bu yana, "Nesneleri" internete bağlamak için girişimlerde bulunulmuştur (Ding ve ark., 2023). 1990'da John Romkey, internet

üzerinden açılıp kapatılabilen bir ekmek kızartma makinesi olan ilk cihazı yarattı (Romkey, 2017). Paul Saffo, 1997'de sensörlerin ilk kısa tanımını ve bunların internetle bağlantılı olarak nasıl kullanılabileceğini ortaya atmıştır (Saffo, 1997). İnternet üzerinden gerçek zamanlı bilgi sağlayan sensörlerin ve benzeri cihazların bu artan bağlantısını tanımlamak için, 1999 yılında "Nesnelerin İnterneti" terimi, tedarik zinciri optimizasyonunda çalışan ve aynı yıl Radyo Frekansı Tanımlama (RFID) tabanlı ürün tanımlama adı verilen yeni bir teknoloji icat eden Kevin Ashton tarafından icat edilmiştir (Suresh ve ark., 2014'ten akt., Ding,Tukker ve Ward, 2023). 2003 yılında Walmart, ürün stoklarını ve satışlarını ölçmek ve tedarik zinciri yönetimini desteklemek için dünya çapındaki tüm mağazalarında RFID'yi kullanmaya başlamıştır (Harold, 2007'den akt., Ding,Tukker ve Ward, 2023). 2005 yılında, Uluslararası Telekomünikasyon Birliği (ITU, 2005), nesnelerin internetini dünyanın bilgi endüstrisinde dönüşümünün üçüncü dalgası olarak ifade etmiştir. Daha sonra Cisco, IBM ve Ericsson gibi BT devleri nesnelerin interneti ile birçok eğitim ve ticari girişimde bulunmaya başlamıştır. Çin gibi bazı ülkeler, nesnelerin internetini uzun vadeli planlarında stratejik olarak gelişen bir teknoloji olarak değerlendirmektedir (MIIT, 2012). Nesnelerin interneti teknolojisi basitçe insanlar-bilgisayarlar-nesneler arasındaki bir bağlantı olarak açıklanabilir.

Avrupa Parlamentosu'nun Yapay Zekâ Yasası, yapay zeka sistemlerinin amacını; ister fiziksel ister dijital boyutta olsun, sistemin etkileşimde bulunduğu ortamı etkileyen içerik, tahminler, öneriler veya kararlar gibi çıktılar üretmek şekilde tanımlamaktadır (EC, 2021'den akt., Melville, Robert, ve Xiao, 2023). Benzer şekilde, Singapur Hükümeti tarafından geliştirilen "Yapay Zekâ Yönetişim Çerçevesi" yapay zekayı bilgi, akıl yürütme, problem çözme, algılama, öğrenme ve planlama gibi insan özelliklerini simüle etmeye çalışan ve yapay zeka modeline bağlı olarak bir çıktı veya karar (tahmin, öneri ve/veya sınıflandırma gibi) üreten bir dizi teknoloji olarak ifade etmektedir (Iswaran, 2020:18).

4. Sanayi devriminin hayatımıza getirdiği yeniliklerden biri de makinalar arasında ekipler oluşturmaktır. Makineler arası ekip oluşturmaya örnek olarak, bir hastane uyarı uygulaması verilebilir. Bu, bir kasırga tarafından tahliye bildirim sistemi tetiklendiğinde, yapay zekâ devreye girerek hastalara tahliye edilirken ilaçları yanlarında götürmeleri için hatırlatıcı mesajlar göndermek şeklinde olabilir. Diğer örnekler arasında, hareket algılandığında bir video kamerayı açmak, bir araba paylaşım uygulaması istediğinde bir haritayı açmak, bir görüntülü sohbet uygulaması içindeki başka bir makineden canlı altyazı özelliği eklemek ve görme engelli kişilerin yaşam kalitesini artırmak için bulut tabanlı bir hizmet kullanarak ortamdaki öğeleri tanımlamak ve açıklamak sayılabilir. Bu örnekler,

makinelerin, örneğin uygulama kullanıcıları olarak insanlarla ilişki içinde bir hedefe ulaşmak için geçici yollarla koordine ettiği (bir yeteneği paylaştığı, verileri birleştirdiği vb.) makineler arası ekip oluşturmanın temel özelliklerini göstermektedir. Makineler arası ekip oluşturma, örneğin işçi güvenliği için çevresel verilerin gerçek zamanlı paylaşımını sağlayarak, endüstriyel bağlamlarda bağlama duyarlı nesnelerin tasarımı hakkında yeni bir literatür ortaya çıkarmaktadır (Rajendran ve diğ, 2020). Diğer faydalı örnekler arasında giyilebilir bir cihaz sayılabilir: Postoperatif kalp fonksiyonlarını izleyen ve ikincil bir sistem kullanarak doktoru otomatik olarak uyaran ve dijital deftere dayalı bir hizmet ekosistemi içinde izin verilen belge ve bilgi paylaşımı sağlayan bir yapay zekâ olabilir (Jensen ve ark., 2019). Bunlar yapay zekanın insan hayatını kolaylaştıran, güzelleştiren faydalı tarafları olarak görülebilir. Fakat yapay zekâ uygulamalarının olumsuz, zararlı yanları da ne yazık ki vardır. Makineler arası ekip oluşturma sayesinde, siyasi bir kuruluş tarafından hedefli reklam kampanyaları için kullanılan özel verilerin aldatıcı bir şekilde toplanması gibi özel verilerin vicdansız, zararlı ve yasa dışı kullanımına da yol açabilir. Ayrıca kişisel mahremiyetin ihlali, yanıltıcı seçim bilgilerinin kolaylaştırılması ve demokratik süreçlerin tehdit edilmesi yer alabilir. Araştırmalar, çalışanların insan yeteneklerini taklit eden makinelerin kendi yerlerini alacakları korkusunun iş tatminlerini azalttığını göstermektedir (Schwabe ve Castellacci, 2020). Bu tür bir değişim, yönetim seviyelerinde de gerçekleşebilir ve bu da "kalpsiz patronlara" yol açabilir (Mantello ve ark., 2021'den akt., Melville, Robert, ve Xiao, 2023). Otomatik makinelerle iş birliği içinde anlamlı işler yapan yaratıcı çalışanların pembe bir resmi, bir yapay zekanın hizmetkarı gibi hissetmek, makinelere karşı görünüşte beyhude bir yarış yürütmek ve kelimenin tam anlamıyla kalpsiz bir patrona sahip olmak gibi ampirik bulgularla çelişmektedir. Belki de en korkulan şey; kişisel mahremiyetin ortadan kaldırılması ve makinalara karşı bir siber savaş içinde kalmak olacaktır.

İnternet teknolojilerinin gelişmesi işletmelerin pazarlama anlayışını da büyük ölçüde değiştirmiştir. Son 30- 40 yıl içerisinde ticaret dünyasında geleneksel pazarlama aktörlerinin yerini çevrimiçi alışveriş siteleri, web sayfaları ve sosyal medya platformları üzerinden pazarlama faaliyetlerine bırakmıştır. Sanal mağazaların sunduğu karşılaştırma imkânı ve cazip fiyat politikalarıyla birlikte alışverişte mekân ve zaman kısıtlamalarının olmaması önümüzdeki yıllarda e-ticaretin daha fazla yaygınlaşacağını göstermektedir.

Son dönemde gençler arasında yaygınlaşan bir başka durum da sosyal medya kullanımıdır. Neredeyse her yaş grubunun sosyal medyayı aktif şekilde kullandığı

gözlenmektedir. Sosyal medyayı bilgi edinme, bilgi paylaşma, boş vakit geçirme, eğlenme, sosyal ilişkiler kurma, alışveriş yapma gibi çok farklı saiklerle yoğun şekilde kullandıkları anlaşılmaktadır. Facebook, Twitter, Instagram gibi popüler sosyal medya platformları, kişilerin kendi ya da oluşturdukları farklı kimliklerle katıldığı ve interaktif etkileşimin olduğu sosyal medya araçları hem bireysel hem de kurumsal olarak yaygın şekilde kullanılmaktadır.

İnternetin yaygınlaşmasıyla birlikte hayatımıza giren ve özellikle gençler için sakıncalı olaylara yol açan bir başka kavram da siber flört kavramıdır (Kaplan, Kaplan ve Mucuk, 2023). İnternet kullanımının çok fazla alanda avantajları olduğu gibi çok sakıncalı olayların yaşanması gibi dezavantajları da vardır. Gençler ve yetişkinler arasında kullanılmaya başlayan arkadaşlık siteleri, yeni dolandırıcılık yöntemlerinin yanı sıra cinsel istismar vakalarının yaşanmasına da sebep olabilmektedir. Siber flört istismarı cep telefonları, mesajlaşma, sosyal ağlar dahil olmak üzere teknoloji veya elektronik medya kullanımı yoluyla flört partnerleri arasında psikolojik istismar mağduriyeti ve/veya failliği olarak tanımlanmaktadır (Borrajo, Gámez-Guadix, Pereda ve Calvete, 2015). Bu doğrultuda sıkça karşılaşılan davranışları; tehdit, hakaret, aşağılama, küçük düşürme, cinsel şiddet, kişisel bilgilerin rıza dışı yayılması, resim veya video gibi görsel materyallerin rıza dışında yayılması, şifre kırma, hesapları hackleme, internet kullanımını yasaklama ve kontrol etme gibi çok farklı davranışlar sıralanabilir. Bu tür istenmeyen istismar davranışları yetişkinlerde de görülmekle birlikte yoğun şekilde gençler ve çocuklarda da yaşanmaktadır (Rojas-Solís, Guzmán-Toledo, Sarquiz-Garcia, GarcíaRamírez, Hernández-Cruz, 2021).

Verilerinde gözler önüne serdiği gibi bugün artık internet kullanımı vazgeçilmez olmuştur. Fakat internet kullanımı günlük yaşamı kolaylaştırsa da verilerin güvenliği açısından da çok ciddi riskler yaratmaktadır. Son çeyrek asırdır yaşanılan endüstri 4.0 devrimi ile nesnelerin interneti, bulut sistemleri, yapay zekâ vb. teknolojiler kullanılarak günlük hayattaki pek çok makine, cihaz gömülü sistemler aracılığıyla internete bağlanabilmektedir. Bu sayede insanlar, süreçler ve cihazlar arasında dijital verinin üretilmesi, işlenmesi, kaydedilmesi, depolanması ve dağıtılması sağlanmaktadır. Kurumlar içinde extranet kullanımının artması, cihazların birbirleriyle haberleşmeleri, ağ içerisinde çok sayıda kullanıcının olması birtakım tehditlerin ve risklerin de ortaya çıkmasına sebebiyet vermektedir. Ağ içerisindeki veri ve bilgilerin çalınması, değiştirilmesi, başka kişilerle paylaşılması, herkese dağıtılması gibi riskler daha fazla artmaktadır. Bu nedenle ağların ve dijital verilerin korunmasına ihtiyaç duyulmaktadır.

Siber güvenlik; Siber ortamı, kuruluşu ve kullanıcıya ait varlıkları koruma amacıyla kullanılabilecek olan araçlar, güvenlik amaçlı önlemleri, uygulanan politikalar, yönergeler, risklerin yönetilmesi yaklaşımları, eylemler, verilen eğitimler, geliştirilen uygulamalar ve bu alandaki teknolojilerin toplamı olarak tanımlanmaktadır (Tokmak, 2023). Kuruluşlar ile kullanıcıların varlıkları kavramı ise bilgi işlem cihazlarını, çalışan personeli, oluşturulmuş altyapıyı, verilen hizmetleri, geliştirilen uygulamaları, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya depolanan bilgi ve belgelerin tamamını kapsamaktadır (Alzahrani, 2021).

Araştırmalar siber güvenlik zafiyetlerinin çoğunun insan kaynaklı olduğunu göstermektedir. Bu nedenle insan kaynaklı yanlış kullanımı ya da hatayı azaltmak için "siber güvenlik farkındalığı" kazandırılması yapılması gereken ve ciddiye alınması gereken asıl konudur. Siber güvenlik farkındalığı "bilgi güvenliği kavramının önemi, bir kuruluşa ait verileri ve ağları korumak amacıyla yeterli düzeyde bilgi kontrolü ve uygulama sorumluluklarını anlama derecesi" olarak tanımlamıştır (Tokmak, 2023). Siber güvenlik farkındalığının amaçlarını; toplumu siber dünya ve siber riskler hakkında bilgilendirmek, siber güvenlik kavramını ve olası riskler hakkında bilgilendirmek, kullanıcı hatalarını minimize edecek çözümler üretilmesini sağlamak ve kişileri siber suçlar ve yasal hakları gibi konularda bilinçlendirmek olarak saymak mümkündür.

Bu alandaki literatür incelendiğinde sıklıkla bilginin korunmasının altındaki teknolojinin, bilgi güvenliği yönetim sistemlerinin, risklerin, risk analizinin ele alınarak araştırıldığını görmek mümkündür. Son dönemde az sayıda çalışmanın ise siber güvenliğin en önemli parçası olan insan unsuru ve özellikle çocuk ve gençlerin siber güvenlik farkındalık düzeyinin incelendiği görülmektedir.

Bilgi güvenliğini sağlamak için öncelikle eğitim programları aracılığıyla farkındalık yaratılmalı ve özellikle çocuk ve gençlere, güvenlik önlemlerinin nedeninin ve öneminin anlatılması gerekmektedir. İnternet ile ilk defa ciddi anlamda ortaöğretim yaşlarında tanışıldığından siber güvenlik farkındalık eğitimlerine başlamak için en uygun dönemin bu dönem olduğu belirtilmektedir (Bintziou ve ark.1999'dan akt., Güldüren, Çetinkaya ve Keser, (2016). Siber güvenlik eğitim sürecine çocuk ve gencin de bizzat dâhil olması gerektiği düşünceler vardır. Siber güvenlik konusunda en üst seviyede bilgi sahibi olması beklenenler üniversite öğrencileridir. Mevcut literatür çalışmalarında üniversite öğrencilerinin özellikle siber güvenlik uygulamaları konusunda yetersiz oldukları görülmektedir (Alqahtani, 2022; Gabra ve diğer., 2020; Moallem, 2019; Zwilling ve ark.,

2022'den akt., Demir ve Sarı, 2023). Yeterli bilgi ve tecrübesi bulunmayan çocuklar ve gençler daha fazla siber mağduriyet yaşama riski taşımaktadırlar. Bir başka ifadeyle siber güvenlik farkındalıkları yeterli olmayanlar sanal ortamlardaki tehdit ve tehlikelere karşı daha savunmasızdırlar (Yiğit ve Seferoğlu, 2019). Bu grubun kendini olası risklerden ve tehlikelerden koruyabilmesi için bilgilendirme ve bilinçlendirme çalışmaları ile siber güvenlik farkındalık düzeylerinin artırılması oldukça önemlidir (Varkan Kavas, Özbudak ve Çetkin, 2022).

Bu bağlamda hazırlanan bu tez çalışmasının birinci bölümünde; siber güvenlik kavramı, siber güvenliği tanımlamak için kullanılan teoriler, siber güvenliğe hazırlık, kişisel veri güvenliği, siber suç türleri, siber güvenlik ve bilgi güvenliğini tehdit eden unsurlar, siber saldırı kavramı, siber güvenlik farkındalığı ve gençlere ve çocuklara yönelik siber güvenlik tehditleri ve siber güvenlik farkındalığı çalışmaları ayrıntılı olarak ele alınmıştır. İkinci bölümde ise gençlerin siber güvenlik farkındalığını belirlemek amacıyla yürütülen bir alan araştırmasının detayları yer almıştır. Araştırma sonucunda; gençlerin siber güvenlik farkındalığının yüksek düzeyde olduğu görülmüş ve bu farkındalığı artırmak, konu hakkında bilinçlendirmek için bireylerin, ailelerin, eğitim kurumlarının ve yasa yapıcıların neler yapabileceği tartışılarak birtakım öneriler sunulmaya çalışılmıştır.

2. SİBER GÜVENLİK KAVRAMI

Bilgisayarın tarihi, M.Ö. 1000'li yıllarda Çinliler tarafından bulunan ve kullanılan abaküs ile başlamıştır. Abaküs, ilk hesap makinesi ve bilgisayar olma özelliğini taşımaktadır. 17. yüzyılda Pascal tarafından mekanik hesap makinesi icat edilmiştir. Bu hesap makinesi Alman Matematikçi Gottfried Wilhem Leibniz tarafından geliştirilmiştir. 1900'lü yıllara gelindiğinde ENIAC (Elektronik Sayısal Bütünleştirici ve Hesaplayıcı) adını taşıyan sayısal tabanlı elektronik bilgisayar, Pensilvanya üniversitesinden John William Machly tarafından geliştirilmiştir (Köprülü, 2023). 1950'li yıllarda günümüz bilgisayarlarına benzer aygıtlar geliştirilmeye başlanmış, bu cihazlar arasında iletişimin sağlanması ve veri aktarımı konusu gündeme getirilmiştir. İletişim kurmak ve cihazlar arasında haberleşmeyi sağlamak amacıyla ABD başta olmak üzere, Fransa ve İngiltere'deki laboratuvarlarda çalışmalar yapılmıştır. 1960'lı yıllarda Amerika Birleşik Devletleri Savunma Bakanlığı, savaş olması durumunda askeri iletişimlerini sürdürebilmek amacıyla, bilgisayarlar arasında veri aktarımını sağlamak için ARPANET ağını oluşturmuştur. 1980'li yıllarda, ARPANET büyük ağlara bağlanabilen bir yapıya ulaşmıştır (Of, 2019'dan akt., Köprülü, 2023). Bu ağlar, internet kelimesinin ortaya çıkmasına neden olmuştur.

Türk Dil Kurumu (TDK, 2022), günümüzde internet kelimesinin karşılığı olarak, "genel ağ" kelimesini kullanmaktadır. Genel ağ, bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan, herhangi bir sınırlaması ve yöneticisi olmayan bilgi iletişim ağıdır. İnternet, büyük kapsamlı olup, çok sayıda bilgisayar sistemini belirli kurallara göre bir araya getiren ve gittikçe büyüyen bir iletişim ağıdır. Bilgi üretme, aktarma, kullanıcılar arasında bağlantı kurma, eğlence, sosyalleşme gibi pek çok nedenden ötürü internet kullanımı tüm dünyada olduğu gibi ülkemizde de artmaktadır. Ülkemizde ilk kez 12.04.1993 tarihinde internet bağlantısı gerçekleştirilmiştir (Köprülü, 2023).

Elektronik cihaz ve internet kullanımı günlük hayatımızı kolaylaştırsa da verilerimizin güvenliği açısından ciddi riskler oluşturmaktadır. Kullanıcıların internet ortamında karşılaştıkları ihlal ve riskler yıllara ve değişen teknoloji nedeniyle farklı tanımlamalarda bulunulmuştur. 2004-2010 yılları arasında yaşanan bu ihlaller için "Bilgi Güvenliği (Information Security)" ve "Bilgisayar Güvenliği (Computer Security)" kavramları kullanılmış, 2016 yılında "Siber Güvenlik" (Cyber Security) kavramı daha fazla tercih edilmeye başlamıştır (Yılmaz, 2023). 2021 yılı itibariyle alana hâkim kavram siber güvenlik olmuştur.

İnternet, bilgi edinme, bilgiyi paylaşma, eğlence, sosyalleşme, alışveriş, e-vatandaşlık, iletişim gibi pek çok alanda faydalı bir araç olmasının yanı sıra, başta mahremiyet, gizlilik ve güvenlik olmak üzere, farklı tehlike ve zararlarında oluşmasında etkili olmuştur. Örneğin; yanlış bilgilendirme, zararlı bilgiye erişim, siber saldırı, siber zorbalık, siber dolandırıcılık, zararlı yazılımlar, oltalama, internet bağımlığı, teknostres, psikolojik şiddet ve düşmanlık ve telif hakları ihlali gibi olumsuz durum ve konularda internetin zararlı olduğu gözlenmektedir. Bunlar gibi zararlardan korunmak ve tedbir almak için "siber güvenlik" kavramı ortaya çıkmıştır. Uluslararası Telekomünikasyon Birliği (ITU), internette oluşabilecek tehlikelere karşı ortaya çıkan siber güvenliği; kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, siyaset, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojilerin bütünü olarak tanımlamıştır (Sağıroğlu, 2018'den akt., Köprülü, 2023).

Siber saldırılar, ABD'yi altyapı, ekonomi ve sivillerin güvenliği açılarından tehdit eden birincil endişe kaynağı haline gelmiştir. Symantec Inc. (2014) tarafından yayınlanan İnternet Güvenliği Tehdit Raporu, siber saldırılarda genel olarak %91'lik bir artış olduğunu rapor etmektedir. Bu rapor endişe verici bir şekilde, 552 milyondan fazla kimliğin açığa çıkmasını ve mobil kullanıcıların yaklaşık %38'i aynı zamanda mobil siber suçlara maruz kaldığını göstermektedir (İnan, Namin, Pogrund, & Jones, 2016). Siber suçların 2010'lu yılların başında küresel ekonomiye yıllık maliyetinin tahmini 400 milyar dolardan fazla (McAfee, 2014) olduğu düşünüldüğünde günümüzde bu rakamın kat ve kat üzerinde olacağını ön görmek yanlış olmayacaktır.

Siber güvenlik kavramı çoğu kişi tarafından bilgisayarların sadece internet üzerindeki güvenliğini sağlamakla sınırlı olduğunu düşünerek kavramı yanlış anlamaktadır. Halbuki, siber güvenlik, donanım, yazılım, veri ve bilgilerin her türlü ihlalden korunması olarak tanımlanabilir (Yılmaz, 2023). Siber güvenlik, veri koruma ve bilgi güvenliğinin uygulanması için kurum ve kuruluşlar için en yüksek önceliği, bireyler için ise gizlilik, erişim kontrolü ve güvenliğidir. Şu anda, siber güvenliğin kapsamı, bireyleri siber zorbalığa karşı korumaya ve gelişmiş makine öğrenimi teknikleri kullanarak siber savaşı tanımlamaya kadar çok geniş şekilde gelişmiştir (Blanke, Nielsen ve Wrozek, 2022; Tirumala, Valluri ve Babu, 2019'dan akt., Yılmaz, 2023).

Son yıllarda siber saldırıların hızlanması, dünya çapındaki kuruluşların genel performansını olumsuz etkilemektedir. Kuruluşlar, siber saldırıları önlemek ve bunlarla mücadele etmek için siber güvenliklerini geliştirme zorluğuyla karşı karşıyadır, ancak kuruluşların siber güvenlik farkındalığını/hazırlığını etkileyen faktörleri bütünsel bir bakış açısıyla inceleyen çalışmalar az sayıdadır. Siber saldırılara hazır olmanın kurumsal güvenlik performansını olumlu yönde etkilediği, bunun da finansal ve finansal olmayan performansı olumlu yönde etkilediği bilinmektedir.

2.1. Siber Güvenliği Tanımlamak İçin Kullanılan Teoriler

Bu konudaki yerli ve yabancı literatür incelendiğinde bilgi güvenliğini tanımlamak için kullanılan bazı teoriler olduğu dikkat çekmektedir. Aşağıda bu teorilerden çok kısa olarak bahsedilecektir.

2.1.1. Kurumsal teori

DiMaggio ve Powell (1983) tarafından geliştirilen kurumsal teori, bilgi güvenliği araştırmacıları tarafından iç kurumsal faktörlerin teknoloji girişimleri üzerindeki etkisini anlamak için kullanılan teorik bir mercektir. Kurumsal teoriye göre her kurumun teknoloji girişimlerini etkileyebilecek kendi yapısı, kültürü ve eylemleri vardır. Kurumsal teori, meşruiyeti sürdürmek için bir kurumun, yapı, kültür ve diğer içsel yönlerde değişiklikler gerektirebilecek çevresine uyum sağlaması gerektiğini öne sürmektedir (Oliveira ve Martins, 2011). Üç eşbiçimli mekanizma bir kurumdaki iç değişiklikleri yönlendirir: taklitçi, zorlayıcı ve normatif baskılar (DiMaggio ve Powell, 1983). Kurumsal teori, bu üç baskının iç çevre üzerindeki etkisini açıklamak açısından özellikle önemlidir. Hsu ve arkadaşları (2012) IT yeteneği, üst yönetim desteği ve organizasyon kültürü gibi iç çevresel faktörlerin bilgi güvenliği yenilikleri üzerindeki etkisini incelemek için kurumsal teoriyi kullanmışlardır.

Kurumsal teori tarafından açıklanan örgütsel faktörler arasında üst yönetim desteği, örgütsel beceriler ve örgüt kültürü yer almaktadır (Daud, Rasiah, George, Asirvatham ve Thangiah, 2018). Önceki çalışmalar, bilgi güvenliği konusunda üst yönetimin desteğinin siber saldırıları azalttığını ortaya koymaktadır (Puhakainen ve Siponen, 2010). Araştırmalar üst düzey yöneticilerin bilgi sistemi güvenliği politikasına bağlılıklarını göstererek bilgi sistemi güvenliğini artırabileceklerini ileri sürmektedirler. Ayrıca, bilgi güvenliği yönetimi

için en iyi uygulamaların belirlenmesi gibi bilgi güvenliği yönetiminin üst yönetim desteği, bilgi güvenliğinin başarılı bir şekilde benimsenmesine yol açmaktadır (Kankanhalli ve ark., 2003).

Çalışmalar, kurumlarda siber güvenliği yönetmek için organizasyonel becerilerin önemini açıkça ortaya koymaktadır. Çalışanların iyileştirilmesi becerilerinin eğitim, öğretim ve farkındalık programları yoluyla geliştirilmesi, kuruluşlarda karar alma süreçlerine yardımcı olabilir.

Kurumsal teoriye uygun olarak, birçok çalışma organizasyonlarda siber güvenliği desteklemek için organizasyonel becerilerin, özellikle de çalışanların IT ve siber güvenlik becerilerinin kullanılabilirliğinin önemini vurgulamaktadır. Örneğin Wixom ve Watson (2001), güvenlik sorunlarını daha iyi çözmek için güçlü teknik becerilere sahip çalışanlar edinmenin önemine vurgu yapmaktadır. D'Arcy ve arkadaşlarına (2014) göre bir kuruluşun çalışanlarına en son güvenlik teknik becerilerini aktaran periyodik eğitim, farkındalık ve eğitim programları, güvenliğin karmaşıklığıyla mücadele etmeye ve dolayısıyla siber güvenliği artırmaya yardımcı olacaktır. Periyodik eğitim, kurumsal teorinin normatif ve zorlayıcı baskılarıyla tutarlıdır. Ravichandran ve Rai (2000) eğitim süreçlerinin sorunsuz ilerlemesi için yeterli kaynakların tahsis edilmesi gerektiğini vurgulamaktadır.

Kurumsal teoriyi takip ederek, Hsu ve arkadaşları (2012) siber güvenliğin, taklitçi, zorlayıcı ve normatif baskılarla şekillenen organizasyon kültüründen etkilendiğini öne sürmektedir. Örgüt kültürü, çalışan davranışlarına rehberlik ve destek sağlayarak bir kuruluşun eylemlerini ve çalışan uygulamalarını bilgi güvenliğine yönlendirir. Bilgi ve bilgi paylaşımı, kuruluşun güvenlik bilgisini ve süreçlerini zenginleştirerek bilgi güvenliği yönetimini büyük ölçüde etkiler ve bu da kuruluşun hedeflerine ulaşmasını olumlu yönde etkileyebilir. Bu ilişkiler, kurumsal teorinin taklitçi ve normatif baskılarına dayalı olarak paylaşılan organizasyon kültürünün siber güvenliğe hazırlık üzerindeki etkisini araştırmanın önemini vurgulamaktadır.

Farklı gruplar arasında iş birliğini teşvik ederek işbirlikçi bir organizasyon kültürü yaratmanın önemi Gopal ve Gosain (2010) tarafından vurgulanmaktadır. Hsu ve arkadaşları (2012) işbirlikçi bir organizasyon kültürünün, ekip üyelerinin organizasyonun siber güvenliğine yönelik sorumluluk duygusunu artırmaya yönelik katkılarını teşvik ederek organizasyonel performansta önemli bir rol oynayabileceğini belirtmektedir.

Iivari ve Huisman (2007), kurum kültürünün güvenlik sistemi geliştirme üzerindeki etkisini incelemek için resmi ve bağlı kültürü dâhil ederek hem güvenlik kurallarına uymanın hem de kurumda güvenlik geliştirmeye bağlılığın önemli olduğunu ve bunun kurumsal teorinin zorlayıcı baskısına uygun olduğunu bulmuştur.

Kurumsal teori çerçevesinde bu bulgular, organizasyonlarda siber güvenliğin şekillenmesinde organizasyon kültürünün önemini açıkça ortaya koymaktadır.

2.1.2. Oyun teorisi

Neumann ve Morgenstern (1944) tarafından geliştirilen oyun teorisi, bir organizasyonun, iş birliğini yönetmek için bir dizi kuralı takip eden oyun oyuncuları olarak rakipler, tedarikçiler ve iş ortaklarıyla olan etkileşimlerini anlamak için yararlı bir teorik mercek sağlamaktadır (Hassan ve ark., 2021). Oyun teorisi kapsamında rakipler ve iş ortaklarıyla iş birliğinin temel ilkeleri belirlenmiştir. Mohebbi ve Li'ye (2015) göre iş birliği, faydaları en üst düzeye çıkarmak ve belirsizlikleri azaltmak için bilgi, kaynak ve yardımcı programların paylaşılmasıyla gerçekleştirilebilir.

Gao ve Zhong (2016) ile Nagurney ve Shukla (2017) rakiplerle iş birliğinin siber güvenlik yatırımı üzerindeki etkisini incelemek için oyun teorisini kullanmışlardır. Teorik bir mercek olarak kullanan Gao ve Zhong (2016) ile Nagurney ve Shukla (2017) bir kuruluşun güvenlik konularında rakipleriyle işbirliği yaptığında siber saldırılarla daha iyi mücadele edebileceğini varsaymaktadırlar. Çok sayıda çalışma, rakipler arasındaki iş birliğini siber güvenlik bağlamında deneysel olarak değerlendirmektedir ve rakiplerin onları sürekli olarak yeni saldırılar hakkında bilgilendirmesi durumunda kuruluşların saldırıları daha iyi tahmin edebileceği ve bunlarla mücadele edebileceği sonucuna varmışlardır (Kianpour M, Øverby H, Kowalski SJ, Frantz, 2019'dan akt., Hasan, 2021); bu da siber saldırıların azaltılmasında rakipler arasındaki bilgi paylaşımının hayati bir rol oynadığını göstermektedir. Dahası, bilgi paylaşımı örgütsel performansı büyük ölçüde artırabilir (Ruivo, Oliveira, Neto, 2014).

Bouncken ve Fredrich'e (2016) göre örgütler rakiplerinden edindikleri bilgileri kullandıklarında sorunları daha hızlı çözmektedirler. Bilgi paylaşımı için kolay iletişim şarttır ve bu nedenle kuruluşlar iletişim kolaylığını teşvik etmelidir. Daha iyi bilgi paylaşımı için rakipleriyle iş birliği aynı zamanda bir kuruluşun güvenlik performansını iyileştirme verimliliğini de artırabilir. Buna göre rakiplerle iş birliğinin bir kuruluşun güvenliğini

artıracağı düşünülmektedir. Dolayısıyla oyun teorisini takip eden araştırmalar, rakiplerle iş birliğinin kuruluşların siber güvenliğini nasıl etkilediğine dair anlayışı geliştirme potansiyeline sahiptir. İş birliği ve bilgi paylaşımı, kuruluşlara siber saldırılara karşı kendilerini korumak için rakipleriyle daha iyi iş birliği yapma fırsatı sağlayabilir (Hasan ve ark., 2021).

2.1.3. Caydırıcılık teorisi

Caydırıcılık teorisi kriminoloji araştırmacıları tarafından oluşturulmuş ve daha sonra bilgi sistemleri araştırmacıları tarafından Wall ve diğerleri (2016) tarafından tanımlandığı gibi bilgi güvenliği politikasına uygunluğu incelemek için kullanılmıştır. Gibbs (1975) caydırıcılık teorisinin, kuruluşların uygulamalarını düzenlemek ve desteklemek için hükümetler ve uluslararası kuruluşlar tarafından sağlanan kuralları ve standartları anlamaya yardımcı olmak için kullanılabileceğini öne sürmektedir (Hasan ve diğ., 2021). Wall ve arkadaşları (2016) kuruluşların kural uygulamasını ve yaptırımlarını tartışmak için caydırıcılık teorisini kullanmışlardır. Dolayısıyla caydırıcılık teorisi, bir kuruluşun siber güvenliğini etkileyen hükümet düzenlemeleri ve endüstri standartları gibi dış güçleri incelemek için iyi bir mercek sağlar. Quigley ve arkadaşları (2015) ve Wall ve diğ. (2016) hükümet kurallarının ve düzenlemelerinin kuruluşların siber güvenlik risklerini azaltma üzerindeki etkisini açıklamak için caydırıcılık teorisini kullanmışlardır. Hwang ve Choi (2017) ve Quigley ve arkadaşları (2015). bilgi sistemleri güvenliğini arttırmada devlet desteğinin rolünü araştırmışlardır. Njenga ve Jordaan (2016) caydırıcılık teorisi ve nötralizasyon teorisi kullanmışlardır. Bu yazarlar, Ulusal Teknoloji Enstitüsü (NIST) standartları gibi endüstri standartlarının kuruluşlara güvenliklerini planlamak ve güvenlik uygulamalarını düzenlemek için yönergeler sağladığını ileri sürmektedir.

Çevresel bağlamda, kuruluşların siber güvenliğe hazır olma durumunu etkileyen çeşitli faktörler vardır (Hasan ve ark., 2021). Caydırıcılık teorisine uygun olarak bu faktörler arasında hükümet düzenlemeleri, hükümet desteği ve endüstri standartları gibi dış düzenleyici girişimler yer almaktadır. Hükümet düzenlemeleri, güvenli e-iş işlemlerinin temel itici güçleridir ve bu nedenle kuruluşların siber güvenlik altyapısını etkiler. Caydırıcılık teorisine dayanarak Wall ve arkadaşları (2016), hükümet düzenlemelerinin kuruluşların makul bilgi güvenliğini sürdürmelerine yardımcı olduğunu varsaymaktadır. Hükümetler, kuruluşların siber güvenliğini düzenlemek için farklı rol ve eylemler

benimseyebilir (Nagurney ve Shukla, 2017). Zhu ve Kraemer (2004), kuruluşların siber güvenliğini düzenlemede hükümetlerin iş kanunları oluşturmak ve interneti güvenilir bir iş platformu haline getirerek internet işlemlerini korumak şeklindeki iki önemli rolüne dikkat çekmişlerdir. Caydırıcılık teorisi, kuruluşların kuralları daha iyi uygulayabilmesini ve yaptırımlar oluşturabilmesini sağlamak için görünür hükümet düzenlemelerini vurgular ve bu da daha yüksek hazırlığa yol açar. Caydırıcılık teorisine uygun olarak bu çalışma, düzenlemelerin hükümetin siber saldırılarla mücadele konusundaki farkındalık ve kararlılık düzeyinin bir göstergesi olduğunu ve bunun da bir kuruluşun siber saldırılarla mücadeleye hazır olma durumunu etkilediğini öne sürmektedir. Ayrıca düzenlemeler, çevrimiçi platformlar ve diğer ilgili faaliyetlerle ilgili hükümet kurallarının kapsamının genişliğini de göstermektedir.

Caydırıcılık teorisine uygun olarak, devlet desteği kuruluşların siber güvenliğinin sağlanmasında kritik bir rol oynar ve hükümetler, kuruluşların siber güvenliğini desteklemek için farklı faaliyetler gerçekleştirebilir. Knapp ve arkadaşları (2006), hükümetlerin siber güvenlik programları oluşturarak bilgi güvenliğini destekleme sorumluluğunu üstlenmesi gerektiğini belirtmektedir. Ayrıca Looi (2005), uygun karşı önlemlerin alınmasını sağlamak için hükümetlerin kuruluşları son siber saldırılar hakkında bilgilendirmekten sorumlu olması gerektiğine dikkat çekmektedir. Hükümet desteği, siber güvenlik farkındalığı yaratarak kurumsal olarak siber saldırılarla mücadeleye hazır olmanın sağlanmasında önemli bir rol oynamaktadır (Knapp ve ark., 2006).

Caydırıcılık teorisine dayanarak, uluslararası siber güvenlik standartlarının ve çerçevelerinin kuruluşların siber güvenliğini desteklemedeki önemi birçok araştırmacı tarafından incelenmiştir. Örneğin Knowles ve arkadaşları (2015) kuruluşların siber güvenliğini desteklemede endüstri standartlarından yararlanmanın önemini vurgulamaktadır. Ayrıca Njenga ve Jordaan (2016) endüstri standartlarını takip etmenin kuruluşlar için daha fazla iş güvenliği sağladığını belirtmektedir.

Rowe ve Gallaher (2006) uluslararası kurum ve kuruluşlar tarafından yayınlanan üç farklı siber güvenlik sektörü standardını ki bu standartlar; Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) en iyi uygulamaları, Uluslararası Standartlar Örgütü (ISO) yönergeleri ve Amerikan Ulusal Standartlar Enstitüsü (ANSI) düzenlemeleri vurgulamaktadır (Hasan ve diğ., 2021). Sommes-tad ve arkadaşlarına (2014) göre, ISO, güvenliği ihlal edenlere yönelik cezalar, bilgisayar kaynaklarının kullanımına yönelik öneriler, bilgi güvenliğine ilişkin hesap verebilirlik ve çalışanlara sağlanacak eğitim türleri hakkında öneriler de dahil olmak

üzere siber güvenlik için yönergeler sağlar. Siber güvenlik için NIST çerçevesi beş işlevi içerir: tanımlama, koruma, tespit etme, yanıt verme ve kurtarma. Bu çerçeve kurumsal siber güvenlik yönetimi için kullanılabilir (Hasan ve ark., 2021). Rowe ve Gallaher (2006)bu standartların, en iyi kararları almaları için yönergeler sağlayarak kuruluşların siber güvenliklerini düzenlemelerine yardımcı olduğunu belirtmektedir (Hasan ve ark., 2021). Ayrıca Li ve arkadaşları (2019) endüstri standartlarını takip etmenin organizasyonel performansı önemli ölçüde artırabileceğini belirtmektedir.

Caydırıcılık teorisine uygun olarak bu çalışmalar, siber saldırıların daha iyi tanımlanması, korunması ve tespit edilmesi yoluyla kurumsal siber güvenlik altyapısını ve hizmetlerini geliştirmek için bilgi kaynakları olarak farklı endüstri standartlarının benimsenmesinin önemini göstermektedir.

2.1.4. Diğer teoriler

Siber güvenliği açıklarken bir dizi başka teori de kullanılmıştır Ayrıntılandırma Olasılık Modeli (ELM) teorisi, Petty ve Cacioppo (1986) tarafından iki alternatif etki modunu anlamak ve aralarında ayrım yapmak için geliştirilmiştir (Hasan ve ark., 2021). ELM teorisi, çoğunlukla bireylerin davranışlarına odaklanan bireysel düzeyde modeller ve organizasyon düzeyindeki modeller geliştirmek için kullanılır (Bhattacherjee ve Sanford, 2006). ELM teorisine dayanarak Puhakainen ve Siponen (2010) çalışanların bilgi güvenliği politikası uyumuna yönelik tutumlarındaki değişiklikleri araştırmışlardır. Siber güvenlik becerilerinin kuruluşların siber güvenliği üzerindeki etkisini araştırmak için ELM teorisini kullanan birçok çalışma bulunmaktadır (Wixom ve Watson, 2005). Bu araştırmacılar, çalışanlara becerilerini geliştirmek amacıyla düzenli siber güvenlik eğitimi vermenin bilgi ve varlıkların korunmasını iyileştirdiğini, siber saldırılara karşı hassasiyeti azalttığını ve çalışanların güvenlik politikalarına uyumunu iyileştirdiğini iddia etmektedirler. Son olarak, kültürün kurumların siber güvenlik yönetimi üzerindeki etkisine ilişkin çalışmalar, güvenlik yönetişimi, kontrolü ve koordinasyonu dahil olmak üzere bilgi sistemleri güvenliğinin kurum kültürü tarafından desteklenmesinin siber saldırılara karşı kırılganlığı azalttığını ortaya koymaktadır (Hasan ve ark., 2021).

Benzer şekilde, Koruma Motivasyon Teorisi, Rogers (1983) tarafından bireylerin güvenlik davranışlarını ve güvenlik teknolojilerini benimseme niyetlerini incelemek için geliştirilmiştir. Li ve diğerleri (2019) ve Anwar ve arkadaşları (2017) bireylerin güvenlik

olaylarına karşı davranışlarını incelemek için PMT teorisini kullanmışlar fakat önemli örgütsel faktörleri ihmal etmişlerdir.

Nötralizasyon teorisi; Sykes ve Matza (1957) tarafından bireylerin endüstri standartlarına ve yönergelerine göre nasıl davrandıklarını açıklamak için geliştirilmiş ve tanımlanmıştır (Hasan ve ark., 2021). Njenga ve Jordaan (2016) bireylerin rasyonelleştirmelerinin kuruluşların güvenlik duruşları üzerindeki etkisini incelemek için nötralizasyon teorisini kullanmışlardır. ELM teorisi gibi, nötralizasyon teorisi de çoğunlukla bireylerin davranışlarına odaklanan bireysel düzeyde modeller geliştirmek için kullanılmaktadır.

Dengeli Puan Kartı (BSC) teorisi, Kaplan ve Norton (1992) tarafından, farklı nedensel değişkenler ile iş performansının iyileştirilmesi arasındaki neden-sonuç ilişkilerini yansıtmak için geliştirilmiştir. Kong ve arkadaşları (2012) bilgi güvenliği yatırımı ile varlık riski yönetimi arasındaki neden-sonuç ilişkilerini yansıtmak için BSC teorisine dayanan bir araştırma modeli kullanmışlardır. BSC teorisinin en büyük sınırlaması, yalnızca nedensel ilişkilerle ilgilenmesi ve bir model oluştururken olası etkili faktörlere ilişkin bir bakış açısı sunmamasıdır (Hasan ve ark., 2021).

Böyle bir çerçeve, siber güvenliği etkileyen tüm temel faktörlerin genel etkisine ve her faktörün göreceli önemine ilişkin araştırmalara rehberlik etmesi açısından önemlidir. Bu bağlamda, Ernest Chang ve Ho (2006) ile Rhee ve diğerleri (2009), güvenliği artırmak için sadece tek bir boyutun dikkate alınmasının yeterli olmadığını ve farklı bakış açılarından/bağlamlardan çeşitli faktörleri anlamak için daha kapsamlı bir modele ihtiyaç olduğunu savunmaktadır. Eilts (2020) küçük işletmelerde siber güvenliğe hazır olma durumunu değerlendirirken, kuruluşların siber güvenliğe hazır olma durumunun performans üzerindeki etkisini inceleyen bir çalışma yapılmamıştır. Bu çalışma, kuruluşların siber güvenliğe hazır olma durumuna odaklanmakta, önceki çalışmalardan belirlenen siber güvenliği etkileyen faktörlerin ilgisini değerlendirmekte ve siber güvenliğe hazır olmanın kurumsal performansın üzerindeki etkisini araştırmaktadır (Hasan ve ark., 2021).

2.1.5. Siber güvenliğe hazırlık

Eilts'e (2020) göre, siber güvenliğe hazır olma durumu, siber güvenlik altyapısını iyileştirmeye yönelik NIST Siber Güvenlik Çerçevesi temel alınarak ölçülebilir. Çerçeve aşağıdaki beş işlevden oluşur (Hasan ve ark., 2021):

• **Belirleyin:** Kuruluşların karşı karşıya olduğu siber güvenlik risklerini anlamaya yönelik faaliyetler. Ten ve arkadaşları (2010), siber saldırıları tanımlamak amacıyla güvenlik açıklarını değerlendirmenin ve bilgisayar bağlantı noktalarını kontrol etmenin önemini vurgulamaktadır

• **Koruyun:** Siber altyapıyı ve hizmetleri korumaya yönelik faaliyetler, veri şifreleme ve virüs koruma yazılımı kullanmanın ve güçlü bir şifre politikasının, siber saldırılara karşı korunmanın ana yolu olduğunu belirtmektedir.

• **Tespit Etme:** Siber saldırıların oluşumunu belirlemeye yönelik faaliyetler. Siber saldırıların erken tespitini sağlamak için kuruluşlar, olayların operasyonel ve stratejik analizlerini gerçekleştirebilir ve güvenlik uyarılarını sürekli olarak izleyebilir.

• **Yanıt:** Tespit edilen siber saldırılara tepki verme faaliyetleri. Arızalara yanıt verebilmek için kuruluşların yük devretmeyi izlemeye yönelik bir sisteme sahip olması önemlidir. Siber saldırılara yanıt verirken iyileşmeyi planlamak da önemlidir.

• **Kurtarma:** Siber saldırıların neden olduğu arıza ve hasarlardan kurtulma faaliyetleri. Açık prosedürler bir uygulamanın uygulanması için kritik öneme sahiptir.

Bu siber güvenlik çerçevesi her ne kadar kurumların kullanımı için uygunmuş gibi değerlendirilse de bireysel açıdan da bu beş aşamalı çerçeve kişisel siber güvenliği sağlamada kullanılabilir. Kişisel siber güvenlik çerçevesinin araştırmacılar tarafından uygulamaya yönelik yeni araştırmalarla geliştirilmeye ihtiyacı vardır.

2.1.6. Kişisel veri güvenliği

Kişisel verilerin dijital ortamda depolanması ve korunması günden güne daha fazla tartışılmaya ve önem kazanmaya devam etmektedir. Kişisel veri kavramını kişiye ait ve onu tanımlayabilecek her türlü veri ve bilgi olarak tanımlanabilir (Ünal ve Sezer, 2023). Kişisel veri olarak iki tür veriden bahsedilir. İlki kişinin ad, soyad, yaş, cinsiyet medeni durum, eğitim gibi bilgileri kapsarken ikinci tür veriler ise teknolojinin hayatımıza getirdiği kimlik numarası, vergi numarası, banka bilgileri, şifreler, e-devlet bilgileri, sağlık sitemindeki kayıtları, tapu kayıtları vs gibi bilgilerdir. Bilgi teknolojilerinin yaygınlaşması bilginin oluşmasını, depolanmasını, işlenmesini ve yeniden kullanımı gibi işlemlerin sürekli artması insanlarda endişe ve korku yaratmaktadır. Özellikle kişisel verilerinin başka kişi ve kurumların eline geçmesi, kötü amaçlarla kullanılması gibi bilgi mahremiyetinin ihlal edilmesi en büyük endişelerden biridir. Dimitropoulos ve diğerleri (2011) yaptıkları bir

çalışmada, tüketicilerin genellikle mahremiyet ve güvenlik konusunda endişe duymaya devam ettiğini ve bu endişelerin 40 ila 64 yaş arasındaki bireyler arasında daha yaygın olduğunu bulmuşlardır.

Potansiyel olarak siber güvenlik tehditlerini; zararlı süreçler ve özel bilgilere erişmek ve bunları kullanmak için gerçekleştirilen eylemler (örn. kimlik) hırsızlık), kullanıcıları aldatmaya ve dolandırmaya çalışmak (ör. spam e-postalar), yetkisiz bir işlem gerçekleştirmeyi amaçlayan yazılımlar yüklemek (örn. virüsler ve kötü amaçlı yazılım) veya bilgisayar sistemlerine ve ağlarına doğrudan saldırmak (örn. bilgisayar korsanlığı) gibi eylemleri sıralamak mümkündür. Bilgi mahremiyeti ya da bilgi güvenliği, bilginin kullanım hakkına sahip olan kişi ya da kurum dışındaki kişi ve kurumların ele geçirmesi durumunda bilgi güvenliğinden söz edilemez.

McCumber (2005), bilgi güvenliğini, bilgi ve bilgi sistemlerine yetkisiz erişim, bilginin kullanımı, ifşa edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak koruma olarak tanımlamıştır.

Kötü niyetli kişiler, insanların bilgi sistemlerine karşı olan davranışları konusunda bilinçli kişiler olup kullanıcıların nerede, hangi aşamada, nasıl hatalar yapabileceğini ve zafiyetlerini çok iyi analiz ederler ve bunu kullanırlar. Kötü niyetli bu kişiler çoğu zaman siyasi propaganda yapmak veya üst düzey bir siyasi ya da bürokratı karalamak, kişilere zarar vermek, imajını zedelemek, parasal kazanç elde etmek, bilgilerini çalıp farklı alanlarda kullanmak veya bazen de tamamen zevk için kişisel veri hırsızlığı yaparlar. Bu nedenlerden dolayı, son kullanıcıların tehditlerden, saldırılardan ve risklerden haberdar ve bilinçli olması, yapılan tüm teknolojik yatırımlardan çok daha önemlidir ki araştırmalar da kullanıcı davranışlarıyla bilgi güvenliği arasında bir ilişki olduğunu söylemektedir (Crossler vd., 2013: 94; Öğütçü vd., 2016: 83; Şen, 2020:51; Kruger vd., 2010:317 akt., Değirmenci ve Demiral, 2023).

Genel olarak bilgi güvenliği problemlerinin temel nedenlerinin; internet kullanıcı sayısının artmasıyla elektronik verilerin çok artması, mobil cihaz kullanım oranlarının yükselmesi, suçların artık şekil değiştirerek siber suçların artması, kötü niyetli siber saldırganların artması ve siber suçları ortaya çıkarmanın zorluğu, bu konudaki yasal boşlukların olması ve en önemlisi de kullanıcıların siber güvenlik konusundaki bilgi ve bilinç yetersizliği olarak sayılabilir (Değirmenci ve Demiral, 2023). Büyük işletmeler ve kamu kurumları bilgi güvenliği sağlamada yüksek maliyetli ve teknoloji tabanlı güvenlik

mekanizmaları kullanarak siber saldırılara ve veri hırsızlığına karşı önlemler almaktadır. Fakat araştırmalar göstermektedir ki bilgi güvenliğindeki en zayıf halka halen daha kullanıcılardır (Parsons vd., 2017: 40; Arce, 2003: 72).

Günümüz gençliği hemen hemen bütün aktivitelerinde, dijital teknolojileri kullanmaktadır. Bu noktada kişisel tüm kritik bilgiler, teknolojik cihazlarda veya kullanılan uygulamalar ile sanal dünyada saklanmaktadır (Güldüren, Çetinkaya ve Keser, 2016). Bilgi güvenliği ve bilginin korunması kurumsal açıdan önemli olduğu kadar bireysel açıdan da oldukça önemlidir. Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir; gizlilik, bütünlük ve erişilebilirlik olarak isimlendirilen üç temel unsurdan meydana gelir (Puhakainen, 2006'dan akt., Güldüren, Çetinkaya ve Keser, 2016).

Günümüz modern dünyasında basit kötü amaçlı bir yazılım saldırısı felaketle sonuçlanabilir (Başeskioğlu, 2021). Bilişim sistemleri ve özellikle İnternet teknolojilerinin yaygınlaşmasıyla birlikte, bu sistemlerdeki açıklıklardan kaynaklanan güvenlik olayları da artmaya başlamıştır. Piyasada bulunan birçok virüs programı, kötü amaçlı yazılımları tespit edemediği için sorunlar yaşanabilir. Kişi, kurum ve kuruluşların bilgiyi saklayarak ve mahremiyetini koruyarak bu bilgileri yetkili kişilere ulaştırması oldukça önemlidir. Gelişen teknoloji ile, geçmişe dair bilgilerin önemi de artmakta ve bu veriler istatistiksel olarak çeşitli araştırma sonuçları için kullanılmaktadır. Bu sebeple bilginin güvenli bir şekilde saklanması ve istenildiği zaman, yetkili kişiler tarafından kullanılabilir durumda olması oldukça önemli bir hal almıştır. Bilginin önem düzeyinin artması ve bu sebeple bilgiye olan bu bağımlılığın yükselmesi bilginin korunması için kullanılması gerekli olan sistemleri de zorunlu kılmaktadır. Bu sistemler bilgiye yönelik olası tehditlerin veya saldırıların tespit ve engellenmesinde kullanılırlar. Ayrıca saldırılar sonucu oluşabilecek bilgi tahribi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, sistem altyapısının bozulması ve dolayısıyla meydana gelebilecek maddi manevi kayıpların önlenmesi açısından önem arz ederler. Bilgi güvenliği sistemlerinin vazgeçilmez unsurlarından biri de Saldırı Tespit Sistemleri (STS) araçlarıdır (Baykara ve Daş, 2019).

Her ne kadar bilgi güvenliğinin sağlanmasına yönelik dijital önlemler, yazılımlar, programlar geliştirilse de bu teknolojileri kullananlar yine insanlardır. Yalnızca teknoloji temelli önlemlerle bilgi güvenliğinin sağlanması ve olası problemlere çözüm bulma düşüncesi, bilgi güvenliğinin sağlanmasında belki de en önemli unsur olan insan faktörünün

göz ardı edilmesine neden olmaktadır (Chen, Shaw ve Yang, 2006; Kjorvik, 2010; Öztemiz ve Yılmaz, 2013; Rezgui ve Marks, 2008 akt Güldüren, Çetinkaya ve Keser, 2016).

Bireysel ve kurumsal bilgilerin güvenliğinin en zayıf halkasını insan unsuru oluşturmaktadır (Kritzinger ve Smith, 2008; Penmetsa, 2010; Veiga, 2008). Saldırganlar artık gelişmiş duvarları ve cihazları aşmaya uğraşmaktansa insan faktörünün daha kolay bir hedef olduğunu düşünmektedir Kötü niyetli kişiler, alınan siber güvenlik önlemleri sayesinde sistemsel hata ve açıklar azaldığından kullanıcının hatalarından faydalanarak eylemlerini gerçekleştirmeye başlamışlardır. Bu durum bilgi güvenliği sorunun, insan faktörünü göz ardı ederek ve yalnızca teknoloji temelli yöntemlerle çözümlenemeyeceğini göstermektedir. Kurumsal ve kişisel bilgilerin güvenliğini sadece teknik güvenlik önlemleriyle (güvenlik duvarı, sanal özel ağ, saldırı tespit/önleme sistemi, anti virüs, içerik kontrolü yazılımı, veri şifreleme, kimlik doğrulama, yetkilendirme vb.) sağlamak mümkün değildir (Rezgui ve Marks, 2008). Bu nedenle de küçük yaşlardan itibaren siber güvenlik eğitimi ve bilinci verilerek siber güvenlik farkındalığı yaratmak gerekir. İnsan faktörüne bağlı bilgi güvenliği risklerini tamamen ortadan kaldırmak mümkün olmasa da iyi planlanmış bir farkındalık etkinliği ile güvenlik risklerinin kabul edilebilir bir seviyeye çekilmesi sağlanabilir (Acılar, 2009; Gülmüş, 2010; Keser ve Güldüren, 2015; Kruger ve Kearney, 2006; Şahinaslan, Kandemir ve Şahinaslan, 2009; Vardal, 2009; Vural, 2007 akt Güldüren, Çetinkaya ve Keser, 2016). Bu noktada da bilgi güvenliği risklerinden korunmanın en iyi yolu insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisini doğru yer ve zamanda kullanmakla mümkündür (Albrechtsen, 2007; Al-Shehri, 2012; Puhakainen, 2006; Siponen, 2001; Şahinaslan, Kantürk, Şahinaslan, ve Borandağ, 2009'dan akt., Güldüren, Çetinkaya ve Keser, 2016).

Literatürde bireylerin siber güvenlikle ilgili alacağı eğitimler sayesinde siber suçlar hakkında bilgi, tutum ve farkındalık kazandırılarak, önlenebilmesinin mümkün olabileceğini belirtmişlerdir (Peltier, 2005; Atkinson, Furnell & Phippen, 2009; Öğün ve Kaya, 2013). Teknolojik anlamda ise, her hizmet için farklı 12 karakterden oluşan harf, rakam, sembol gibi özel karakterler barındıran güçlü şifreler oluşturma, sosyal ağların adres defterimizi taramasına izin vermeme, kullandığımız yazılım ve uygulamaların güncel versiyonlarını kullanma, sahte sitelerden gelen linklere dikkat ederek tıklamadan silme gibi önlemler güvenliğimizi koruma adına alınabilir (Yavanoğlu, Sağıroğlu, Çolak, 2012; Canbek ve Sağıroğlu, 2006).

Ülkemizde 2019 yılında kamu kurumlarında yapılan veri ihlallerine yönelik bir ankette, 980 kullanıcının %92,3'lük çok büyük bir kısmı "kişisel verilerim benim için önemlidir" demiştir, %61,4'ü kullandıkları bilgisayar veya telefonlara yönelik saldırılardan bilgileri olmadığı cevabını vermiştir (Başeskioğlu, 2021). Bu sonuç veri ihlallerinin önlenmesinde insanların farkındalık eğitimlerinin artırılması gerektiğini göstermiştir.

2020 yılında IBM Güvenlik İş Birimi, veri ihlallerinin kuruluşlar üzerindeki maliyetini inceleyen yıllık araştırmasına göre Türkiye'deki her veri ihlalinin ortalama maliyeti, bir yılda yüzde 10,3 oranında artış göstermiş ve 12,3 milyon TL'ye ulaşmıştır (Başeskioğlu, 2021:3). Bu artış verilerin korunmasını zorlaştırmanın yanında saldırılara açık olan verilerin de her geçen gün artmasına neden olmaktadır.

Watch Guard'ın 2020 yılı için hazırladığı rapora göre Türkiye'de bir yılda 1,692,320 adet kötü amaçlı yazılım saldırısı düzenlenmiştir (Saprikin, 2021). Geçen yıla göre %81 oranında artışın gerçekleştiği Türkiye'de, dakikada 3 adet kötü amaçlı yazılım saldırısı yaşanmıştır. Gerçekleşen saldırıların birçoğunu "Truva Atı" ve "Exploit" türünde saldırıların oluşturduğu belirtilmiştir. Son yıllarda veri güvenliği ve siber güvenlik alanında birçok çalışma ve akademik araştırma yapılmıştır. Teknoloji ilerledikçe siber zafiyet türleri de değişmiştir. Veri güvenliğini sağlamak amacıyla gerekli eğitimlerin alınması için teknik personelin eğitimi ve fiziksel güvenlik önlemleri de dikkate alınmalıdır (Yılmaz ve Sağıroğlu, 2008).

Dijital teknolojiler, cihazlar ve ara bağlantılardaki önemli ilerlemeler, kuruluşlara gelişmiş sistem erişilebilirliği, artan iletişim hızı, artan verimlilik ve azaltılmış işletme maliyetleri dâhil olmak üzere çeşitli şekillerde fayda sağlamaktadır (Hasan ve diğ. 2021). Dijital teknolojiler kuruluşlara yeni pazar fırsatları ve daha kaliteli ürünler sunmaktadır. Ancak dijital dönüşüm geçiren kişi ve kuruluşlar, bilgi teknolojisi, siber tehditler ve varlıklarına yönelik saldırı riskiyle karşı karşıya kalmaya devam etmektedir. Amerikan Federal Soruşturma Bürosu'na (FBI) göre, kuruluşlara her gün 4.000'den fazla fidye yazılımı saldırısı yapıldığını ve her gün 330.000'den fazla kötü amaçlı yazılım uygulaması oluşturulduğunu bildirmektedir (Kasperskylab, 2018).

Siber saldırıların ölçeği ve karmaşıklığı arttıkça bu sayıların daha da kötüleşmesi beklenmektedir. Bu tür saldırıların kuruluşlara ve hükümetlere maliyeti ve etkileri oldukça büyüktür. Siber saldırıların maliyeti 2017 yılında 5 milyar doları aşmış ve bu rakamın 2021 yılında ise 6 trilyon doların üzerine çıkmıştır (Morgan, 2021). Bu maliyetler arasında gelir ve itibar kayıpları ile hassas bilgilerin sızması yer almaktadır. Gyde'a (2017) raporuna göre,

küresel kuruluşların %49'u 2017 yılında siber saldırılardan kaynaklanan iş kayıpları yaşadı. Aslında, siber saldırıların gerçek maliyetleri bildirilenden daha fazla olabilir. Çünkü birçok işletme itibar kaybı veya utançtan kaçınmak için siber saldırı olaylarını bildirmeyi reddedebilir (Pearson, 2014).

Siber saldırıların görülme sıklığının artması, uygun siber güvenliğin önemini vurgulamaktadır. Siber güvenlik, bir kuruluşun veriler, sistemler ve ağlar da dâhil olmak üzere bilgisayar teknolojisi ile ilgili varlıklarını, hassas bilgilere erişebilecek, bunları yok edebilecek veya değiştirebilecek veya iş operasyonlarını bozabilecek dijital saldırılara karşı koruma uygulaması olarak tanımlanabilir. Siber güvenlik; kuruluşları, bireyleri veya ağları dijital saldırılardan korumak için insanların, süreçlerin ve teknolojinin bir araya getirilmesini içerir (Cisco, 2019'dan akt., Hasan ve ark., 2021). Bir kuruluşun siber güvenliği, itibarını artırabilir ve temel yetkinliğini ve üstün organizasyonel performansını kolaylaştırabilir. Ancak bir kuruluşun siber güvenliği tesis edebilmesi için öncelikle siber saldırı olasılığının farkında olması ve bu tür saldırıları önleme, tespit etme ve bunlarla mücadele etme konusunda kararlı olması gerekir.

Siber güvenliğe hazır olmanın önemine rağmen, literatür incelendiğinde kişi ve kuruluşların siber güvenliğe hazır olup olmadığına ilişkin mevcut araştırmaların yetersiz ve yeterince kapsamlı olmadığı ortaya çıkmaktadır. Siber güvenliğin tehdit ve saldırıları azaltmadaki rolüne ilişkin önceki çalışmalar, kurumlardaki bilgi güvenliği yönetimini bilgi güvenliği yatırım kararları ve idari bilgi sistemleri güvenliği yenilikleri açısından incelemiş, ancak siber güvenlik hazırlığı ve bunun kurumsal performans üzerindeki etkisini incelememiştir (Kong, Kim ve Kim, 2012). Smith ve arkadaşları (2010) ve Tsou ve Hsu (2015), siber güvenliğin sağlanmasıyla kuruluşların daha iyi finansal getiriler ve daha iyi itibar elde edebileceklerini savunmaktadırlar. Buna ek olarak, kuruluşlarda siber güvenlik politikalarına ve standartlarına bağlı kalmak, güvenlik kontrolünü, sistem kontrolünü, yedekleme kurtarmayı ve acil durum planlamasını güçlendirir ve bu da temel yetkinliğe ve üstün şirket performansına ulaşmada güçlü bir etkiye sahiptir (Daud ve ark., 2018).

Son dönemlerde araştırmalarda veri fidyeciliğine ve çeşitliliğine dikkat çekmiştir. Bilgisayar kullanıcılarının son zamanlarda verilerinin şifrelendiğini belirterek bu şifreler karşılığında para istendiğini ve bu hususta alınması gereken tedbirler hakkında öneriler sunulmuştur (Başeskioğlu, 2021). Ayrıca veri güvenliği ihlallerinden biri olan sosyal mühendislik üzerine incelemeler yapılmıştır. Sosyal mühendisliğin ne olduğu, kapsadığı saldırı çeşitlerinin neler olduğu, sosyal mühendislik saldırılarına karşı alınacak önlemlerin

neler olduğu ve bu konuda nelere dikkat edilmesi gerektiği anlatılmıştır (Acılar ve Baştuğ, 2016).

Araştırmacılar kimlik avı saldırılarının önlenmesi için tek seferlik parolalar, çok düzeyli masaüstü engelleri, davranış değişikliği şeklinde üç aşamalı bir strateji uygulamak gerektiğini belirtmektedirler. Bu yaklaşımları kullanarak bireyler ve kurumlar veri güvenliklerini koruyabilmeli, neden olabilecek zararları en aza indirebilmelidir (Miller, Miller, Zhang ve Terwilliger, 2020). Başeskioğlu (2021) çalışmasında siber saldırıların nasıl yapıldığı, kimler tarafından yapıldığı, hangi araçların kullanıldığı konusunda güncel bilgiler sunarak farkındalık yaratmak ve uygulama ile bunu ortaya koymaya çalışmıştır.

Veri ihlallerinin önüne geçmek, siber saldırı yöntemlerini bilmek davranış ve hareketlerini incelemekten geçmektedir. Bu ihlaller konusunda teknik olarak ne kadar tedbir alınırsa alınsın en zayıf halka olan insan, eğitimlerle elde edeceği farkındalıklarla bu ihlallerin önüne geçecektir. İnsan faktörünün de bütün bu bilgilere sahip olması, geçmişte karşılaşılan tecrübelerden haberdar olmasının çok önemli bir durum olduğu bu nedenle örneklere dayalı bir eğitim sürecinden geçirilerek farkındalık yaratılmasını önemlidir.

2.2. Siber Suç Türleri

Siber güvenliği sağlamak için önlemler alabilmek için öncelikle art niyetli kişilerin yaptığı siber suçları öğrenmek, farkında olmak gerekir. Ancak bu sayede siber güvenliği sağlayabilmek için uygun tedbirler alınabilir. Aşağıda siber suç türlerine kısaca değinilecektir.

2.2.1. Siber taciz / Siber zorbalık

Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bilinçli bir şekilde mağdura zarar vermeyi amaçlayan yeni bir şiddet türüdür. Bir kişiyi taciz ve tehdit etmek, aşağılamak veya küçük düşürmek için teknolojik platformların kullanılmasıdır. Bilgi edinme, paylaşma ve sosyalleşme gibi fırsatlar sunan bilişim teknolojileri çocuklar için fırsatlar yaratmakla birlikte bilinçsiz ya da kötü niyetli kullanımı, siber zorbalık gibi olumsuz durumları yaşamalarına da sebebiyet verebilmektedir. Siber zorbalığa daha çok çocuk ve gençler maruz kalmaktadır. Bir yetişkin söz konusu olduğunda buna “Siber Taciz’’ ya da “Siber Saldırı’’ denilmektedir. Hapis cezasına kadar giden hukuki yaptırımları olan bir suç türüdür. Sahte

hesaplar açarak paylaşımlara yorum yapma, mağdurun kimlik bilgilerini yayma, utandırma, resim ve vidolarını paylaşma gibi eylemler siber zorbalığa ve siber tacize verilebilecek örneklerdir (Başeskioğlu, 2021).

Livingstone ve Brake (2010) sosyal paylaşım sitelerinin tüm dünyada çocuklar ve gençler tarafından hızla benimsenmesinin temelinde onlara; kendini temsil etme, öğrenme, ilişki ağları kurup geliştirme, samimi ilişkileri ve kişisel mahremiyeti koruyup yönetme gibi temel bazı konularda kayda değer yeni fırsatlar sunduğunu öne sürmektedirler (Akça ve Sayımer, 2017). Öte yandan kullanıcılara birçok fırsat sunan İnternet teknolojileri ve yeni medya ortamları aynı zamanda anonim kimliklerle karşılaşma ve mahremiyet kaybı gibi güvenlik sorunlarına neden olmuş ve bazı riskleri beraberinde getirmiştir.

Çalışmalar neredeyse tüm dünyada çocukların ve gençlerin siber zorbalığın kurbanı olduğunu göstermektedir. Araştırmacılar siber zorbalığın dedikodu yayma, anti grup açma, sırrını ifşa etme vb. her türünün kız ve erkek ergenler arasında yaygın olarak gözlendiğini ortaya koymuştur (Arıcak, 2008; Li, 2007; Kowalski ve Limber, 2008; Erdur-Baker, 2010; Schneider, O'Donnell, Stueve ve Coulter, 2012'den akt., Akça ve Sayımer, 2017). Ancak kimi araştırmacılar tarafından ergenler arasında en yaygın olan siber zorbalık türünün taciz olduğu ve ergenlerin eğlenmek amacıyla yaptıkları siber saldırıları zorbalık olarak görmedikleri bulunmuştur (Huang ve Chou, 2010).

2.2.2. Siber flört zorbalığı

Ülkemizde yaklaşık 63 milyon sosyal medya kullanıcının bulunduğu göz önüne alındığında, bu kadar büyük bir ortamın güvenlikle ilgili birçok problemi de içinde barındıracağı tahmin edilebilir (Zeytin ve Akkaş, 2023). Son on yılda teknolojinin ortaya çıkışı insan iletişimini kolaylaştırmış ancak bu araçlar aynı zamanda bazı bireylerin diğerleri üzerinde kontrol kurması için yeni fırsatlar da yaratmıştır. Birini çeşitli mecralarda gizlice takip etmek, bilgi toplamak ve taciz etmek artık her zamankinden daha kolaylaşmıştır. Yakın ilişkilerde bu olaylardan nasibini almıştır.

Sosyal medya uygulamaları, sayesinde özel ilişkilerde çiftlerin birbirlerine her zaman ulaşmalarını ve iletişim halinde olmalarını kolaylaştırmıştır. Bu durum beraberinde kişilerin birbirlerini takip etmelerini, kontrol etmelerini ve siber zorbalığa olan yatkınlığı da artırmaktadır (Zweig, Lachman, Yahner ve Dank, 2014). Siber flört şiddeti geçler arasında büyüyen bir sorun olup gençlerin %12 ila %56'sının bu konuda mağdur olduğu tahmin

edilmektedir (Stonard, Bowen, Lawrence ve Price, 2014). Covid 19 pandemi döneminde karantina altında olunması sosyalleşme ve iletişim ihtiyacının internet üzerinden yapılmasına yol açmış ve bu dönemde siber flört istismarı daha yaygınlaştığı düşünülmektedir (Kaplan, Kaplan ve Mucuk, 2023).

Yakın partner şiddeti ve flört şiddeti, olumsuz sağlık sonuçlarına neden olan ve bazı durumlarda cinayetle sonuçlanan önemli sağlık sorunlarından biri olarak görülmektedir. Yaşamları boyunca neredeyse her iki kişiden biri, mevcut veya eski bir partneri tarafından mağdur edildiğini bildirmiştir; kadınlarda mağduriyet oranları daha yüksektir. İletişim teknolojilerinin gelişimi ve çevrimiçi sosyal ağlara olan bağımlılık, mevcut veya eski partnerleri takip etmek, taciz etmek ve baskı yapmak için yeni zorbalıklar yaratmıştır. Kadınlarda doğrudan ve dolaylı mağduriyet biçimlerini (takip etme ve kontrol, taciz, cinsel) tanımlanan siber flört zorbalığı tartışılmaya başlanmıştır (Fernet, Lapierre, Hébert, & Cousineau, 2019).

Gençler, partnerlerinde ve aile ilişkilerinde eksik kalan yönlerini tamamlayabilmek için sanal ortamda kabul görülen davranışları sergilemektedir. Bu davranışlar istenilen etkiyi bırakmadığında olumsuz duygu ve davranışlara dönüşebilmektedir. Bu duygu ve davranışlar romantik ilişki yaşayan gençlerde siber flört istismarı olarak ortaya çıkabilmektedir. Teknoloji, yakın ilişkilerde psikolojik ve cinsel şiddetin uygulanabileceği yolları değiştirmiştir. Şiddet artık anlık olabilir, fiziksel sınırların ötesinde olabilir ve minimum çabayla geniş bir sosyal ağa ulaşabilir, mağdurun yaşamının farklı alanları üzerinde daha hızlı ve daha büyük bir etkiye sahip olabilir (Hinduja ve Patchin, 2011). Örneğin, siber partner zorbalığının mağduriyeti daha fazla kaygı ve psikolojik sıkıntıyla ilişkilidir (Lindsay ve ark., 2016). Bu tür davranışlara maruz kalma yetişkin nüfusun %6-91'i tarafından ifade edilmiştir (Brown ve Hegarty, 2018). 25 yaşın altındaki gençler, özellikle de kadınlar, mevcut veya eski partnerlerinden kaynaklanan siber yakın partner şiddetine karşı özellikle risk altındadır. Üniversite ortamlarında gençler arasında da yüksek oranlarda siber partner şiddeti gözlemlenmiştir (Fisher, Cullen ve Turner, 2002 aktaran Fernet, Lapierre, Hébert, Cousineau, 2019).

Kadınlar şiddete karşı özellikle savunmasız olduğundan, partner şiddetinin yeni bir biçimi olan siber partner şiddetinin kadınlara karşı nasıl kullanıldığını anlamak çok önemlidir. Ergenlik dönemindeki ilk yakın ilişki deneyimlerinde iletişim stratejileri ve şiddet içeren çatışma çözme ve kontrol taktikleri geliştirildiğinden, ergen kızların deneyimlerine odaklanmak da önemlidir (Connolly ve McIsaac, 2009). Üstelik gençler internetin ve

çevrimiçi sosyal ağların ana kullanıcılarıdır, yalnızca kadınların değil aynı zamanda ergen kızların da yakın ilişkiler bağlamında siber partner şiddetini deneyimledikleri görülmektedir. İlişkide ayrılma sürecinde, geleneksel partner şiddetine uğrama riskinin yanı sıra kadınlar, çevrimiçi taciz ve diğer şiddet türleri dahil olmak üzere siber partner şiddetinin kurbanı olma riskiyle de özellikle karşı karşıyadır (Catalano, 2012, Davies, 2013 aktaran Fernet, Lapierre, Hébert, Cousineau, 2019).

Ayrılık bağlamında siber flört zorbalığı için risk faktörlerini yalnızca iki çalışma incelemiştir. Sonuçlar kaygılı bağlanma stiline sahip olmanın, öfke kontrolünde zorlanmanın, psikolojik ve fiziksel geleneksel flört şiddeti davranışının olmasının, cinsiyet (kadın olmak), ayrılığın yoğunluğu ve ilişkinin uzunluğunun eski bir partner tarafından çevrimiçi ortamda mağdur edilme riskini artırdığını ortaya koymaktadır. Siber flört şiddeti mağduriyetinin genel nüfus içerisinde, üniversite nüfusunda yaygın bir olgu olduğu ve farklı davranışlar ile yapılacağı iddia edilmektedir.

Eğitimcilerin toplumu bilgisayarların ve dijital telekomünikasyon teknolojilerinin kullanımı konusunda eğitmesi, bilimsel verilere dayanması ve siber flört şiddeti mağduriyetinin yaygınlığı ve farklı biçimleri konusunda farkındalık yaratması önemli olacaktır. Siber flört şiddetine karşı savunmasız olan ergen kızların ve kadınların, özellikle ayrılık dönemlerinde, bu tür olumsuz davranışlara maruz kalabileceklerinin farkında olmaları ve gerekirse ailelerinden ve kolluk kuvvetlerinden yardım talep etmeleri gerektiği konusunda bilgilendirilmeye ihtiyaçları vardır.

Her ne kadar geleneksel şiddet ve siber şiddet arasında ilgili şiddetin dinamikleri de dahil olmak üzere pek çok benzerliğe sahip olsa da (örneğin, her iki durumda da tacizin öncesinde genellikle yakın partner şiddetinin damgasını vurduğu çalkantılı bir ilişkinin olması gibi), siber şiddetin kadın kurbanları, kendilerini daha az güvenilir hissetmektedirler. Bu nedenle bazı sosyal ve sağlık profesyonellerinden ihtiyacı olan desteği alamayabilirler (Fernet, Lapierre, Hébert, Cousineau, 2019). Çeşitli uygulama alanlarından (okul, toplum, sağlık ve sosyal hizmetler, polis, yargı) çalışanlar da siber flört şiddeti mağdurlarını desteklemeleri gereken durumlarla karşılaşmaktadırlar.

Siber flört şiddetinin sınıflandırılmasını doğrudan siber flört şiddeti ve dolaylı siber flört şiddeti olmak üzere iki genel biçimi vardır (Fernet, Lapierre, Hébert, Cousineau, 2019). Doğrudan siber flört şiddeti, saldırganlığın doğrudan ortağa yönelik olduğu, yakın bir partneri veya eski yakın partneri özel bir bağlamda istismar etmek için teknolojinin (örneğin cep telefonları, anlık mesaj hizmetleri, coğrafi konum uygulamaları) kullanılmasıdır. Bu

şiddet biçimini kullanırken fail, diğer kişilerin (mağdurun arkadaşları, tanıdıkları veya ailesi) saldırganlığa tanık olmasını beklemez. Aksine, dolaylı siber flört şiddetinde, mağduru dolaylı olarak hedeflemek amacıyla teknolojilerin kullanımı yoluyla mağdur dışındaki bir kişiye bilgi yayma eylemidir. Bu içerik mağdura ait veya mağdur hakkında sözler, fotoğraflar, videolar vb. olabilir ve cinsel nitelikte olabilir (mağdurun çıplak resimleri, cinsel ilişki videosu gibi). Bu içerik çevrimiçi olarak yayınlanabilir ve herkes tarafından, hatta yabancılar tarafından bile görüntülenebilir veya mağdurlar tarafından bilinen belirli bir hedef kitleye, örneğin e-posta listesi aracılığıyla meslektaşlarına gönderilebilir. Bu şiddet biçiminin özelliği, mağdur üzerinde bir tür kontrol sağlamak için mağdurun sosyal veya iş ağının kullanılmasıdır. Doğrudan siber flört şiddetine örnek olarak; takip ve kontrol (örneğin, durum güncellemelerini takip etmek, metin mesajlarını taramak, coğrafi konum belirleme) , taciz (örneğin, SMS ile tekrar tekrar iletişim kurmak) ve cinsel şiddet (örneğin, istenmeyen cinsel içerikli mesajlar veya resim göndermek) verilebilirken dolaylı siber flört şiddeti için: cinsel (örneğin, bir video paylaşım sitesinde mağdurun pornografik videosunu göndermek) ve cinsel olmayan şiddet (örneğin, mağdurun nerede ve kiminle birlikte olduğunu öğrenmek için akrabalarına çevrimiçi mesajlar göndermek) gibi davranışları saymak mümkündür.

Araştırmalarda 18-25 yaş arası, yani üniversite öğrencisi örnekleminde siber flört şiddetinin yaygınlık oranlarına ve mağduriyet biçimlerine bakıldığında, izleme ve tacizin en sık karşılaşılan ve en çok incelenen şiddet biçimleri olduğu görülmektedir (Brown ve Hegarty, 2018; Henry ve Powell, 2018). Kadın olmanın bir risk faktörü olduğu bilinmekte ve fiziksel şiddet mağduru olan kadınların siber şiddet mağduru olma olasılıkları daha yüksek görünmektedir.

Özetle siber IPV mağduriyeti, ergenlik ve yetişkinlik döneminde devam eden veya bir ilişki bittikten sonra yaşanan yaygın bir olgudur. IPV'nin bu biçimi mağdurlara doğrudan uygulanabilir (örneğin art arda istenmeyen SMS göndererek) veya dolaylı olarak arkadaşları ve akrabaları tanık olarak kullanılarak mağdura bir şey yapması için baskı uygulayabilir (örneğin mahrem resimlerin çevrimiçi olarak yayınlanması gibi). Bu durum, çevrimiçi mağduriyete odaklanan önleme ve müdahale programlarının geliştirilmesini ve kadına yönelik şiddeti hedefleyen mevcut önleme girişimlerinde çevrimiçi mağduriyete yönelik bir bileşenin de konuşulması gerektiğini gözler önüne sermektedir.

2.2.3. Siber terörizm

Terör eylemleri teknolojinin gelişmesi, internetin yaygınlaşmasıyla birlikte yeni yöntemler geliştirmiştir. Terör faaliyetleri siber dünyada da yaygınlaşmaya başlamıştır. Bu çerçevede ‘’Siber Terörizm’’, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere karşı kullanılmasıdır (Başeskioğlu, 2021). Ayrıca bir hükümetin veya toplumun yıldırılması, baskı altında tutulması amacıyla da kullanılmaktadır. Siber terörizmde, finans sektöründeki aktörlere saldırılar, kişilerin bankalardaki mevduatlarının ele geçirilmesi, devlete ait gizli sırların ele geçirilerek deşifre edilmesi, kamu internet sitelerinin çökertilmesi şeklinde farklı türden terör eylemleri yaşanabilmektedir.

2.2.4. Siber vandalizm

Siber vandalizm, dijital biçimde meydana gelen hasar veya yıkım olarak adlandırılır. Siber Vandallar bir web sitesini bozabilir, elektronik dosyaları veya normal kullanımı kesintiye uğratabilirler. Bilgisayar sistemini devre dışı bırakmak için bir disk sürücüsünü kaldıran kötü amaçlı yazılımlar oluştururlar. Siber vandalizm, müşterilerin, hizmetlere erişmesini engellemekle beraber finansal kayıp, markaya zarar vermek, itibara etkisi de dâhil olmak üzere işletmeleri önemli ölçüde etkilemektedir (Başeskioğlu, 2021).

2.2.5. E-dolandırıcılık

Kimlik avı, bir kişiyi, banka hesabı bilgileri gibi hassas bilgilerinin e-posta yoluyla ifşa edilmesi için kandırma işlemidir. Kötü niyetli kişiler banka ya da diğer finans kuruluşlarından gelen telefon, e-mail ya da sms gibi bilgi talebinde bulundukları bir mesajı göndererek karşısındaki kişinin kişisel bilgilerini ele geçirmeye çalışırlar. Mağdurdan hesap numarası, hesap şifresi vb. gibi hassas bilgileri kendilerine vermesini talep eder ve ele geçirdikleri bilgiler ile mağdurun hesabından kendilerine ait hesaplara para transferi yaparak hesaplarını boşaltırlar. Ülkemiz, telefon dolandırıcılığının en etkili kullanıldığı ülkeler arasındadır (Öztürk, 2018). Kendini savcı, hâkim, polis olarak tanıtan kişiler “Terör olaylarına karıştınız, hesaplarınızı kontrol ediyorlar’’ yalanıyla her gün binlerce kişiyi dolandırmaktadır. Bu mağdurlar arasında hâkim, doktor ve akademisyenler gibi eğitimli insanlar da olabilmektedir (Başeskioğlu, 2021).

2.2.6. Hacklemek (Bir bilgisayar veya sisteme sızarak ele geçirmek)

Bilgisayar korsanlığı, başkasının bilgisayarındaki verileri çalmak, değiştirmek veya yok etmek için o bilgisayara erişme eylemidir. Bilgisayar korsanlığı yapmanın ardındaki neden kazanç elde etmekle beraber politik ya da sosyal olabilmektedir.

2.2.7. Kötü amaçlı yazılım yaymak

Bilgisayar korsanları kötü amaçlı yazılımları yaymak için birçok web sitesi kullanmaktadırlar. Bunu kendilerini geliştirmek için yâda belirledikleri hedeflere ulaşmak için yaparlar. Kötü amaçlı yazılımlar, sistemleri çökerterek birey veya işletme için mali kayıplara neden olabilmektedir. Kayıplar, sistemin onarım maliyetini ve imha edilen verileri içerir (Başeskioğlu, 2021).

2.2.8. Siteler arası komut dosyası

Bazı saldırganlar, web sitesinin koduna gizli şekilde bir komut dosyası yerleştirir. Bu web sitesini ziyaret eden kullanıcı, bu komut dosyasını çalıştırır. Komut dosyası, kullanıcının bilgisayarındaki bilgilerini tarar. Saldırgan, komut dosyasını mağdurun bilgisayarına aktarmak için çerezleri kullanır. Bu sayede hassas bilgiler toplanır ve bu bilgiler saldırganın sistemine aktarılır. Saldırgan, bu bilgileri kullanıcının bilgisayarına veya bir web sitesindeki oturumlara erişmek için kullanır. Bu saldırı neticesinde kullanıcıyı finansal zarara uğratır (Başeskioğlu, 2021).

2.2.9. Spam yapma

Spam, genel olarak internet ortamında aynı mesajın sayısız kopyası çıkarılarak mesaj konusu ile ilgili talebi olmayan kişilere istekleri dışında gönderilmesi eklinde tanımlanmaktadır (İkizler ve Başar, 2006). İnternet üzerinden istenmeyen veya gereksiz e-postaları toplu olarak gönderme eylemi ‘’Spam’’ olarak adlandırılmaktadır. Türkçe ’de kavram bazen “yığın ileti” olarak da anılmaktadır. Spam e-postalar yalnızca kurbanın gelen kutusunu doldurmakla kalmaz, aynı zamanda tüm ağı da meşgul etmektedir. Yaygın olarak yalnızca istenmeden alınan elektronik postalara spam adı verilmekle birlikte web

sayfalarına, tartıma gruplarına eposta ile gönderilen reklamlar ve promosyon duyuruları gibi ağ ortamında yayılan istem dışı tüm gönderiler spam olarak sınıflandırılabilir. Spam yaymak isteyen kişi çok sayıda gruba üye olarak bunlara toplu mesaj gönderir ve böylece tüm üyelerin mesajı almalarını sağlar. Spam iletiler ilk zamanlar gönderici adresinin engellenmesi ile bir ölçüde azaltılabilmektedir. Ancak spam göndericiler günümüzde deneme amaçlı adresleri ya da kötü niyetli yazılımlarla kontrol edilen adresleri kullanmakta, bu durumda gerçek kaynağa ulaşılamadığı gibi internet ortamı bir kere kullanılıp terkedilmiş adreslerle dolmakta bu da önemli ve büyük maliyetlere neden olmaktadır. Kullanıcılar ise aynı mesajı her seferinde farklı göndericiden almaya devam etmekte ve göndericiyi yasaklamak kullanıcının yasak listesini kabartmaktan başka bir şeye yaramamaktadır.

Dünya üzerinde yüz milyondan fazla internet bağlantısı olduğu düşünülürse her bilgisayar için1 mega byte yer kapladığı varsayımı ile sadece yasaklanan adresler 10000 GB bir alanın boş yere kullanılması anlamına gelmektedir. Kaldı ki Anti-spam yazılımlarının kullandığı disk kapasitesi ve iletilerin bu programlar tarafından kontrol edilmesi sırasında harcanan bağlantı süreleri hesaplanırsa spam iletilerin zararlarının ne boyutlarda olduğu görülebilir. Spam, yalnızca ticari reklam için kullanılmamakta, zararlı düşünce ve akımların yayılması içinde en önemli reklam aracı haline gelmektedir. Ayrıca bu tür iletilerle ticari reklam yapmak sokaklarda ya da adreslere bildiri dağıtmak gibi görülse de reklamı yapılan materyalin kalitesi, kanunlara ve standartlara uygunluğu, tüketici haklarının güvenceye alınması gibi konularda reklam ile ürün arasında hukuksal bir bağ kurulamadığından spam ile yapılan reklamlarla sahtecilik ve dolandırıcılık yapılması riski çok yüksektir (İkizler ve Başar, 2006).

2.2.10. Siber işgal

Bir kişi ya da kuruma ait web alanının ya da sitesinin ismini, ticari markasını kendi adlarına kaydettirip daha sonra yüksek bir meblağa sahibine satmak amacıyla yapılan bir tür düzenbazlık eylemine siber işgal denilmektedir (Başeskioğlu, 2021).

2.2.11. Çevrimiçi açık artırma

İnternet üzerindeki çeşitli web siteleri çevrimiçi müzayedeler düzenlemekte ve siber suçlular bu web sitelerinden yararlanmaktadırlar. Web sitesini birebir kopyalayarak açık

artırma sırasında yapılan tüm para akışı, böylece bilgisayar korsanının hesabına geçmektedir (Başeskioğlu, 2021).

2.2.12. İnternet zaman hırsızlığı

İnternet saati hırsızlıkları çoğunlukla, bir kullanıcının ISS (İnternet Servis Sağlayıcısı) bilgilerinin çalındığı ve bu bilgilerin zamanın bedeli karşılığında internette gezinmek için kullanıldığı bir suç türüdür. Bu, kullanıcının internette geçirdiği süre için ücretlendirildiği anlamına gelmektedir.

2.2.13. Web krikosu

Web krikosu, bir saldırganın ilgili olmayan bilgileri görüntülemek için bir kuruluşun web sitesini ele geçirme yöntemidir. Bu durumu kuruluşun faaliyetleri hakkında farkındalığı yaymak için de kullanabilirler. Web krikosu politik, sosyal veya ekonomik çıkarlara hizmet etmektedir.

2.2.14. Hizmeti engelleme saldırısı (Distrubuted denial of service attack-DDoS)

Servis hizmet dışı bırakma saldırıları kullanıcıların uygulamalarına erişiminin/kullanımının engellenmesidir. Bu saldırılara Denial of service attack (DDoS) denilmektedir. Hizmet engelleme saldırıları bilgi güvenliği unsurlarından erişebilirliği hedef almaktadır. Bu saldırı ile saldırgan sistemin hafıza, ram, bant genişliği veya işlemcisini gereksiz bir şekilde kullanmaktadır. Kaynakları çok yoğun bir şekilde kullanılan bulut sistemi, kendi kullanıcılarına cevap veremez veya hızlı bir şekilde işlem yapmalarına olanak tanımaz. Bu şekilde sistem ya hizmet veremez duruma gelir veya çok düşük performanslar hizmet vermeye devam eder.

Çoğunlukla virüs bulaştırılarak zombi haline getirilen bilgisayarların, bir sunucu bilgisayara eş zamanlı ve mümkün olduğunca çok sayıda istek göndermesi, sunucunun kapasitesinin aşılması sonucunda da hizmet veremez hale getirilmesi ilkesine dayanır (Lo, Chi-Chun, Chun-Chieh Huang ve Joy Ku, 2010). Bulut sisteminin dağıtık ve çok kullanıcılı yapısı düşünüldüğünde, hizmet sağlayıcısının kısa bir süre için de olsa hizmet alıcılarına

hizmet verememesi, hizmet alıcıları için çok büyük maliyetli zararlara neden olabilir. Bu saldırılar çoğu zaman bir saldırı tespit sistemi yardımı ile belirlene bilmektedir (Salur, 2018).

2.2.15. E-posta sahtekârlığı

Bir e-postanın içeriğini değiştirerek yapılan saldırı şeklidir. Kaynağını gizleyerek, bankadan geliyormuş gibi izlenim vererek kişisel bilgileri çalmayı hedeflemektedir. Bu, alıcının hassas bilgileri vermesi için yapılmaktadır. Siber dolandırıcılar son zamanlarda işletmeleri ve çalışanlarını hedef alarak önemli zararlarla karşı karşıya bırakmaktadır. Siber dolandırıcılık kuruluşlara ciddi zararlar vermekte ve bu suçlar kısa sürede de tespit edilememektedir. Son yıllarda yapılan çalışmalarda bir siber ihlalin tespit edilebilmesinin ortalama 206 gün sürdüğü, kötü amaçlı yazılımların %95'inin e-posta yoluyla gönderildiği, işletmelerin %60'ından fazlasının kimlik avı ve sosyal mühendislik saldırılarına maruz kaldığı ve yüksek tutarlarda iş e-postası dolandırıcılık (BEC) kaybı yaşandığı tespit edilmiştir. BEC, bir kuruluşun kritik önem seviyesindeki bilgilerine erişilmesi, e-posta tabanlı bir dolandırıcılık yöntemi ile tasarlanan ve sonucunda da maddi bir kazanç sağlanan zararlı bir kimlik avı biçimi olarak tanımlanmaktadır (Erdoğan, 2021).

2.2.16. Salam saldırısı

Salam saldırısı, doğası gereği marjinal bir yapıdadır. Uzun süre fark edilmeden kalabilmektedir. Salam saldırısına örnek olarak, saldırganın birden fazla banka hesaplarından her gün 1 TL çekmeyi hedeflemesi verilebilir. Kullanıcılar bunun farkına varmayacaktır. Ancak birçok kullanıcının banka hesabından birkaç gün içinde elde edilen 1 TL, birkaç ay veya yıl içinde çok miktarda para birikimine neden olacaktır. Bankalar bu tür yasal olmayan işlemleri izleme noktasında ciddi önlemler alarak azaltmaya çalışmaktadırlar (Başeskioğlu, 2021).

2.2.17. Veri karıştırması

Verileri bir bilgisayar sistemine girmeden önce değiştirme eylemi, "Veri Karıştırma'dır.'' Örneğin, bir saldırgan maaş bordrosunu değiştirerek şirketten alması

gereken maaş miktarını değiştirebilmektedir. İşyerinden daha yüksek maaş alabilmekte ancak şirket raporlarında, kendisine ödenmesi gereken miktarın ödendiği görülmektedir.

2.2.18. Mantık hatası

Orijinal yazılımın içerisine gizlenen kötü amaçlı bir kod, mantık hatası olarak adlandırılmaktadır. Kötü amaçlı kod, kullanıcının gerçekleştirdiği bir işlemle tetiklenmektedir. Kötü amaçlı kod tetiklendiğinde, sistemdeki veriler yok edilebilmekte veya sistemi etkisiz hale getirebilmektedir.

Görüldüğü üzere bilişim teknolojilerindeki hızlı ilerlemeyle birlikte art niyetli insanlar tarafından çok sayıda farklı tür siber saldırı türleri geliştirilmeye devam edilmektedir.

2.2.19. Siber güvenlik ve bilgi güvenliğini tehdit eden unsurlar

Siber güvenlik ve bilgi güvenliğini tehdit eden unsurları; insan kaynaklı, fiziksel tehditler ve yazılım tehditleri olmak üzere üç farklı başlık altında incelemek mümkündür (Yılmaz, 2022).

2.2.19.1. İnsan kaynaklı tehditler

İnsan kaynaklı tehditler kendi içerisinde iki alt başlıkta incelenebilir:

- Art niyetli olmayan davranışlar sonucu oluşanlar: Bir kullanıcının, sistemi bilinçsiz ve bilgisizce, yeterli bilgiye sahip olmadan kullanması sonucunda sistemde ortaya çıkabilme ihtimali olan aksaklıklar.
- Art niyetli davranışlar sonucu oluşanlar: Sisteme hasar verebilmek amacıyla, saldırganlar tarafından sisteme yönelik yapılabilecek tüm art niyetli girişimlerden 16 kaynaklanan tehditlerdir. Bu tür tehditlerde kötü niyetli kullanıcılar tehdit kaynağından ve sistemdeki zafiyetlerden yararlanırlar.

Bu noktada cinsiyet cazibesini kullanılarak yapılan art niyetli davranışlardan da bahsetömek uygun olacaktır. Siber dolandırıcılar genellikle bazı ürünlerin çekiciliğini arttırmak amacıyla ürün tanıtımlarını yaparken cinsiyet cazibesinden istifade ederler. Örneğin internet üzerinden çevrimiçi olarak bahis oynatan web sitelerinin içeriklerinde çok

fazla kadın figürü vardır. Siber saldırganlar bazen kurbanlardan bir kadın ya da erkek ile görüşme karşılığında birtakım görevleri yapmalarını isteyebilirler (Dumanlı, 2011). Özellikle arkadaş bulma ve tanışma uygulamaları kullanıcıların karşı cins ile iletişim kurabilmesi veya gerçek hayatta buluşabilmesi için gold üyelik, premium üyelik vb. satın almalarını isteyebilir. Bu tür paraya dayalı üyelik sistemlerinde kullanıcıların kredi kartı gibi kişisel bilgileri çalınabilir veya kişilerin cinsel eğilimlerinden ötürü kullanıcılara konuşmalarının ifşa edilmemesi için belirli bir miktarda para ödemesi yapması gerektiği istenebilir. Ayrıca sistemlere erişmeyi amaçlayan siber saldırganlar kullanıcılara zararlı yazılımları indirtebilmek amacıyla genellikle erkek kullanıcılara kadın fotoğrafı göndermektedir. Fotoğraf açıldığında arka planda çalışan bir kod vasıtasıyla sisteme zararlı yazılımlar bulaşabilir veya kullanıcı içerisinde zararlı yazılım barındıran bir web sayfasına yönlendirilebilir (Yılmaz, 2023:42).

2.2.19.2. Fiziksel tehditler

Fiziksel tehditler, doğa olayları veya enerji kaynaklarında meydana gelen olumsuzluklar nedeniyle ortaya çıkmaktadır. Bu tür tehditlerin ne zaman meydana geleceği çoğu zaman önceden saptanamaz (Alguliyev, Imamverdiyev, ve Sukhostat, 2018 aktaran Yılmaz). Tehditler doğa olayı kaynaklı olmaları sebebiyle yeterli tedbirler alınmazsa genellikle engellenemezler. Fiziksel tehditler su baskınları, depremler, yangınlar, seller, ani ısı değişiklikleri, toprağın kayması, elektrik kesintileri vb. dir. Tehdidin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre iç tehditler, kurum içinde meydana gelebilecek olaylar, dış tehditler ise kurum dışında gerçekleşip etkisi kuruma yansıyan olaylar olarak tanımlanır.

2.2.19.3. Yazılım tehditleri

Donanımlar, onlar için üretilmiş özel yazılımlar (işletim sistemleri, uygulamalar, programlar vb.) olmadan bir işe yaramazlar. Donanımlar için üretilen bu yazılımların bilişim sistemlerinde kullanılmasıyla beraber bazı riskler meydana gelmektedir. Yazılımlar, art niyetli kişiler tarafından tahrip edilebilir, değiştirilebilir, silinebilir veya kaza ile işlevsiz hale gelebilir. Yazılımlara yönelik yapılan saldırılar çoğu zaman kolayca fark edilemezler (Pandey ve Misra, 2016). Örneğin, bir programı tasarlandığı özellikleriyle çalışıp bunun yanı

sıra art niyetli kişinin istediği diğer istekleri de yapabilecek tarzda manipüle etmek mümkündür. Bu tür durumlarda yazılımın manipüle edildiğinin farkına varmak zaman alabilir. Yazılımlar vasıtası ile ortaya çıkan tehditlere truva atları (trojan horse), rat (remote access trojan), keylogger, virüsler, wormlar, yazılımın tasarımcısından kaynaklanan arka kapı açıkları (Back Door) örnek olarak verilebilir (Yılmaz, 2022).

2.2.20. Siber saldırı kavramı

Siber saldırı ile ilgili birçok tanım bulunmaktadır. Uma ve Padmavathi (2013), siber saldırıyı yetkisiz veya güvenli bilgilere erişmek, casusluk yapmak, ağları devre dışı bırakmak ve hem veri hem de para çalmak amacıyla siber uzayın istismarı şeklinde tanımlamaktadır (Başeskioğlu 2021). Bilgisayar sistemlerini veya ağlarını veya üzerlerindeki bilgi veya programları değiştirme, bozma veya yok etme çabalarıdır. Günümüzde çok değişik şekillerde siber saldırılar yapılmaktadır. Siber saldırı türlerini bilmek onlara karşı önlem alabilmek için gereklidir. En önemli siber saldırı yöntemleri aşağıda sıralanmıştır.

2.2.20.1. Hizmet reddi saldırısı

Yetkili kullanıcıların sisteme erişimi veya tam tersi şekilde sistemin yetkili kullanıcılara erişimlerinin engellenmesidir. Bu tehlikeli bir elektronik saldırı formu olarak kabul edilir. Saldırgan bir noktadan hedef bilgisayarları çeşitli mesajlara daldırmaya ve yasal veri akışını engellemeye başlar. Bu, herhangi bir sistemin interneti kullanmasını veya diğer sistemlerle iletişim kurmasını engeller (Panimalar, Pai, ve Khan 2018 aktaran Yılmaz, 2023).

2.2.20.2. Kimlik avı

Genellikle toplum mühendisliğine dayanan bir yöntemdir. Kötü niyetli kişiler, kurbanlarını, kötü niyetli programlar içeren bir bağlantı açmaya motive eder ve bu nedenle, mağdurun ilgisini çekebilecek konuları içeren mesajlar göndererek veya kurbanın adını veya kötü amaçlı yazılımı kullanarak cihazlarına bulaşır. Mağdur bir mesajı açtığında, kötü niyetli kişi e-postalar, kişisel mesajlar ve hatta sosyal medya sitelerine yüklenen ve artık bu tür

tehditlere ve saldırılara karşı savunmasız hale gelen uygulamalar aracılığıyla korsanlık sürecine başlar (Alhayani, Abbas, Khutar ve Mohammed 2021 aktaran Yılmaz, 2023).

2.2.20.3. Ortadaki adam saldırısı

Bu, bilgisayar korsanının gönderici ve alıcı arasındaki bir iletişim iletim kanalına girmesiyle meydana gelen bir saldırıyı ifade eder. Bu tür saldırılar, oturumun ele geçirilmesine, gizlice dinlenmesine ve hatta meşru kullanıcılar arasında iletilen bilgilerin değiştirilmesine neden olur.

2.2.20.4. Mantıksal bomba

Bir programcının belirli bir olay olması durumunda programın otomatik olarak yıkıcı bir faaliyet gerçekleştirdiği bir programa kod girdiği başka bir saldırı türüdür.

2.2.20.5. Oltalama (Phishing)

Kimlik avcıları tarafından kullanılan bir stratejidir. Bu stratejiler, taklit saldırı, ileri saldırı ve açılır saldırı olarak üç gruba ayrılır. Kimlik avcıları, saldırıyı taklit ederek kurbanlarını, meşru bir kuruluştan gelen resmi bir e-postayı taklit eden e-posta yoluyla kişisel bilgilerini açıklamaları için cezbeder. İleriye dönük saldırı ve açılır pencere saldırıları, kimlik avcısının bir proxy web sitesi (ileriye yönelik saldırı) veya bir açılır pencere (açılır pencere) aracılığıyla kurbanın kişisel bilgilerini ele geçirdiği ve aldığı ortadaki adam (MITM) yöntemlerinin kullanımını içerir (Mohammad, Thabtah, ve McCluskey 2015 aktaran Yılmaz, 2023).

2.2.20.6. Koklayıcı (Packet Sniffer)

Yönlendirilmiş bilgileri gizlice dinleyen ve veri akışındaki her paketi inceleyerek şifreler gibi belirli bilgileri arayan bir programdır (Tomer, Lade, Kumar ve Patel, 2013 aktaran Yılmaz, 2023).

2.2.20.7. Solucan (Worm)

Solucanlar yerel sürücüde ya da ağda kendini tekrar tekrar kopyalayan bir programdır. Tek amacı sürekli kendini kopyalamaktır. Herhangi bir dosya ya da veriye zarar vermez ancak sürekli kopyalama yaparak sistemi meşgul eder ve performansı etkiler. Virüslerin aksine bir programa bulaşmaya ihtiyacı yoktur. İşletim sistemlerindeki açıklardan yararlanarak yayılırlar (Kara, 2015).

2.2.20.8. Truva atı (Trojan)

Truva atı bir virüs değildir. Gerçek bir uygulama gibi gözüken zararlı bir program türüdür. Trojan kendini çoğaltmaz ama virüs kadar yıkıcı olabilir. Truva atı bilgisayarda güvenlik açığı oluşturur ki bu da zararlı programların, kişilerin sistemine girmesi için bir yol açar. Bu şekilde kullanıcıların kişisel bilgileri çalınabilir. Tarihteki Truva savaşındaki olduğu gibi zararsız zannedilen Truva atı, sisteme girer ve Grek askerlerinin ordunun girmesi için kale kapılarını içeriden açması gibi zararlı yazılımların, hackerların sisteme girmesi için bir güvenlik açığı oluştururlar. Virüslerde olduğu gibi farklı amaçlara hizmet eden Trojan türleri de bulunmaktadır (Kara, 2015):

• Uzaktan kontrol yapan Truva atları: En yaygın trojan türlerinden biridir. Kötü niyetli kişilerin asıl kullanıcı bilgisayarın başındayken sistemde kullanıcıdan çok daha fazlasını yapabilmelerine olanak sağlar. Bu tarz bir trojan kullanan biri bilgisayardaki her veriye ulaşabilir.

• Şifre gönderen Truva atları: Bu trojanlar sistemde, tarayıcı hafızasında kayıtlı olan şifreleri, kullanıcı fark etmeden belli bir adrese mail atar. Web sayfalarında, uygulamalarda girilen tüm kullanıcı adı ve şifreleri alabilir.

• Keylogger: Bu Truva atı tipi yapı olarak oldukça basittir. Klavyede basılan her tuşun kaydını tutar ve belli aralıklarla belli bir mail adresine gönderir. Saldırgan bu kayıtları inceleyip sık tekrar eden girdileri tespit ederek kullanıcı adı ve şifrelerine ulaşır.

• Yıkıcı tip: Bu tür Truva atının tek işlevi dosyalara zarar vermek ve silmektir. Otomatik olarak sistem dosyalarını silebilir. Saldırgan tarafından aktifleştirilebilir ya da belli bir gün saatte çalışacak şekilde ayarlanabilir.

2.2.20.4. Botnet

Kötü amaçlı yazılımları dağıtmak, saldırıları koordine etmek ve istenmeyen postaları göndermek ve mesajları çalmak için kullanılan virüslü uzaktan kontrol sistemlerinden oluşan bir ağdır. Botnet'ler genellikle hedef bilgisayara gizlice yüklenir ve yetkisiz kullanıcının kötü niyetli hedeflerine ulaşmak için hedef sistemi uzaktan kontrol etmesine izin verir.

2.2.20.5. Virüs

Bilgisayar virüsleri, kendilerini çoğaltabilen ve kablolu veya kablosuz ağlar aracılığıyla yayılabilen kötü amaçlı kodlar veya programlardır (Yang, Yang, Zhu ve Wen, 2013). Virüsler, diğer programlara bağlanan ve kendini çoğaltarak sisteme bulaşan ve bu nedenle kullanıcı yetkilendirmesini virüse daha açık hale getiren ve kötü amaçlı programları yayarak tüm sistemi veya ağı sömürebilecek bir programdır.

2.2.20.6. Şifre kırılması

Kolay tahmin edilebilir parolaların tahminini ya da şifreli hallerine göre sözlük saldırısı yapma türüdür (Kara, 2015).

2.2.20.7. Tracking cookie

Cookie yani çerezler internette gezinilen siteler vb. ile ilgili veri barındıran basit metin dosyalarıdır ve bilgisayarda çerez klasöründe bulunurlar. Pek çok site de ziyaretçileri hakkında bilgi almak için çerezleri kullanırlar. Örneğin bir sitedeki ankette her kullanıcının bir oy kullanma hakkı bulunmaktadır. Bu web sitesi çerez bilgilerini kontrol ederek kişinin ikinci defa oy kullanmasına engel olabilir. Ancak çerezleri kötü niyetli kişiler de kullanabilir. Tracking cookie adı verilen bu çerez türü bulaştığı bilgisayarda internette yapılan tüm işlemlerin, gezilen sayfaların kaydını tutar. Hackerlar bu şekilde kredi kartı ve banka hesap bilgilerine ulaşabilirler (Kara, 2015).

2.2.20.8. IP aldatması

“IP adres yanıltmasıyla yapılan saldırı türüdür. IP paketlerinin kaynak IP'sini değiştirmekle sağlanmaktadır. Böylece paketi alan istemcinin, paketin geldiği gerçek kaynak adresini bilmesi engellenir. İstemci gelen paketin saldırgandan değil de kullanıcıdan geldiğini sanır (Turgut, 2009).

2.2.20.9. Konfigürasyon hatası

“Çok kullanılan programdaki kullanıcılardan kaynaklanan konfigürasyon hatalarından doğan açıklardır. Bu tür saldırı yönteminin kullanımı sistemin iyi şekillendirilmemesi veya yönetilmemesine dayanmaktadır. Saldırgan bu açıkları kullanarak sistem içindeki ayarlar ile oynar ve aslında normal olan fakat kullanılan sistemin şekline ya da konumuna bilgileri girerek sistemi çalışmaz veya ulaşılamaz duruma getirir. Bu yönteme verilecek olan en iyi örnek yönlendirici bilgilerinin değiştirilmesidir. Bu işlem sonucunda hedef alınan ağ tamamen yok edilir. Windows NT işletim sistemine sahip bilgisayarlarda sistem kütüğü (registry) üzerinde yapılacak olan değişiklikler sayesinde birçok servis devre dışı bırakılabilir (Turgut, 2009).

Güvenlik tehditlerinin azaltılması ve bilgi güvenliğinin korunması önemli bir kurumsal stratejik gündem haline gelmiştir. Çeşitli güvenlik tehditleri arasında, çalışanların bilgi güvenliği politikasını ihlal etmeleri, kuruluşlar için büyük bir endişe kaynağı olarak kabul edilmektedir (Chen vd., 2021; Luo vd., 2020; Moody vd., 2018; Siponen ve Vance, 2010 aktaran Xue, Xu, Luo, & Warkentin, 2021). Veri İhlali Araştırmaları Raporu 2020'ye göre, 81'den fazla ülkede 32.000'den fazla bilgi güvenliği olayı meydana gelmiş ve bunların %28'i kurum içinden kişilerin karıştığı olaylardır. Daha da kötüsü, PWC'ye (2018) göre, sektörler genelinde içeriden öğrenenlerin karıştığı vakalar ortalama 8,76 milyon ABD dolarına mal olmaktadır (Xue, Xu, Luo, & Warkentin, 2021).

2.2.21. Siber güvenlik farkındalığı

Siber güvenliğin sağlanması, siber suçların farkında olunarak bunlardan korunulması ve için en önemli stratejilerden biri, bireylerin ve kurumların maruz kalabilecekleri siber riskleri bilmek ve bu riskleri azaltarak ortadan kaldırabilmek için bir kamu bilincini

oluşturmaktır. Art niyetli kişiler, yazılım ve donanımdaki güvenlik açıklarından yararlanarak kişisel ya da kurumsal bilgilere izinsiz ele geçirerek büyük sorunlar yaşanmasına neden olabilmektedirler. Bir üst başlıkta kısaca değinilen siber saldırı türleri her geçen gün daha fazla kullanılmaya ve yeni saldırı türleri geliştirilmeye devam etmektedir. Her ne kadar sistemsel açıkları ortadan kaldırmak için büyük çabalar sarf edilse de hatta bu açıklar yok edilse de son kullanıcıdan kaynaklanan hata ve ihmaller saldırganların işlerini çoğu zaman kolaylaştırmaktadır. Parolalarını sık sık değiştirmeyen, antivirüs korumasını düzenli olarak güncellemeyen ve yalnızca korumalı kablosuz ağları kullanmak gibi temel siber güvenlik uygulamalarını takip etmeyen kişiler saldırganların birincil hedefleridir.

Siber güvenlik bilgisi, her geçen gün artan bilişim teknolojileri ve uygulamaları, sosyal medya platformlarının artması, bankacılık, danışmanlık gibi pek çok sektörde kurumların hizmetlerini artık online ortamda sunmaları, elektronik ticaret ve sanal alışveriş sitelerinin çok büyük hacimlere ulaşması, e-devlet uygulaması ile kamu hizmetlerinin online taşınması, e-nabız, online randevu sistemi gibi sağlık uygulamalarının yaygın şekilde kullanılması ve sosyal ağ ve bilgi ekonomisi gibi çevrim içi hizmetlerin yaygın kullanımı ile başa çıkmak için çok önemli hale gelmiştir.

Siber güvenlik kapsamında, veri güvenliğinden; verinin sahibi, veriyi kullanan, veri sistemini yöneten yani herkes sorumludur. Siber güvenlikte insanlar bireysel bazda bir halka iken kurumsal bazda bir zinciri oluştururlar. Dolayısıyla kurumun siber güvenliği zincirin en zayıf halkası kadar güçlüdür. Kullanıcılar zincirin halkaları olduğundan bilgi güvenliğinden doğrudan sorumludur. Saldırganlar zincirin en zayıf halkasına odaklanıp zarar verdiğinde zincir kırılacağı için siber güvenlik tam anlamıyla sağlanamayacaktır. Bu sebeple tüm sistemdeki kullanıcıların statü farkı gözetilmeksizin siber ortamdaki tehditlere karşı farkındalık düzeylerinin yüksek olması gerekmektedir (Thompson ve diğ., 2018).

Bu konudaki literatüre göz atıldığında siber güvenlik farkındalığına (SGF) dair birçok tanım olduğu anlaşılmaktadır. Abd Rahim ve diğerleri (2015) SGF'yi "İnternet kullanıcılarını çeşitli siber tehditlere ve bilgisayarların ve verilerin bu tehditlere karşı savunmasızlığına karşı duyarlı olmaları için eğiten bir metodoloji" olarak tanımlamıştır. Siber güvenlik, "çevrimiçi tüketicilerin kişisel bilgilerinin ve işverenlerinin internet özellikli cihazlarındaki bilgilerinin güvenliğini ve bütünlüğünü bir siber saldırıda ele geçirilmekten korumak için benimsemeleri gereken siber güvenlik uygulamaları" ile ilgilidir (Vishwanath ve diğerleri, 2020 aktaran Yılmaz, 2023).

Siber güvenlik bilincinin internet kullanıcılarını siber güvenlik riskleri hakkında uyarmak ve internet kullanıcılarının siber güvenlik riskleri hakkında farkındalık yaratmak olmak üzere iki temel amacı vardır. SGF, insan kaynaklı hataların veya güvenlik açıklarının azaltılması, güvenliğin kişisel veya kurumsal düzeyde iyileştirilmesinde kilit faktördür (Giannakas, Papasalouros, Kamburakis ve Gritzalis, 2019 aktaran Yılmaz, 2023). İnsan kaynaklı hataların veya güvenlik açıklarının azaltılması, için siber güvenlik ve gizlilik sorunları hakkında kullanıcı farkındalığı oluşturulmalıdır.

İnternet kullanıcı her bireyin yaşı, eğitimi, kültür seviyesi, öğrenme becerisi birbirinden farklı olduğundan bu tür bireysel farklılıklarının siber güvenlik davranışlarında da farklılıklar yaratmaktadır. Bu konuda eğitim verecek güvenlik uzmanlarının ve kuruluşların zayıf veya potansiyel olarak tehlikeli güvenlik uygulamalarına daha duyarlı kullanıcıları belirlemesine yardımcı olmak açısından kritik öneme sahiptir.

Fielding (2020), kurumlar için hayati önem taşıyan SG' yi sağlamak için gerekli olanları şu şekilde açıklamıştır:"Kuruluşların yapabileceği şey, tüm çalışanların karşılaştıkları risklerin ve ciddi veri kaybı ve hizmet kesintilerinin işverenleri üzerindeki etkilerinin farkında olduğu, güvenlik öncelikli bir kültür oluşturmaya yardımcı olmaktır" (Yılmaz, 2023). SG eğitimi ve farkındalığı artırma faaliyetleri SG'yi sağlamanın ilk adımıdır. Eğitim programları, geçici çalışanlar, yükleniciler, yarı zamanlı çalışanlar ve üst düzey yöneticiler dâhil olmak üzere tüm çalışanlara odaklanmalıdır. Her şey doğru türde bir program oluşturmakla ilgilidir. Gerçek dünya senaryolarını içeren simülasyon alıştırmalarının, özellikle kısa, 15 dakikalık aralıklarla- az ve sık sık- iletilirse, istenen etkiye sahip olma olasılığı yüksektir. Egzersizleri kendileri yapmak kadar önemli olan, bireylere performansları ve nerede iyileştirmelerin yapılması gerektiği konusunda geri bildirimde bulunmaktır. İnsanlara her şeyin neden olduğu gibi olması gerektiğini açıklamak ve neleri farklı yapmaları gerektiği konusunda onları eğitmek önemlidir. Unutulmaması gereken, bu belirsiz "yetiştirme" kavramıyla ilgili değildir. Farkındalık ile davranışları değiştirmektir. Bu herhangi bir programın değerlendirilmesi gereken özelliğidir (Yılmaz, 2023).

Dünyanın dört bir yanındaki insanların siber farkındalık düzeyleri yeterli seviyede olmadığı için, insanlar kimlik avı saldırı e-postalarını normal e-postalardan ayıramamakta ve potansiyel olarak kötü niyetli yazılımları cihazlarına indirmektedir (Hekim ve Başıbüyük, 2013). Üniversitelerde öğrencilere ve personele uygun eğitimler verildiği takdirde veri ihlallerinin ve başarılı oltalama saldırılarının sayısının hızla azalabileceğini söylemek

mümkündür. İnsan hatası, güvenlik olaylarının açık ara en büyük nedenidir ve bununla mücadele, saldırıları azaltmanın anahtarıdır (Yılmaz, 2022).

Eğitim ve farkındalık genellikle sosyal mühendislikle ilgili siber güvenlik saldırılarına karşı en iyi korumadır. Kişi, avlanma olaylarını proaktif olarak araştırabilir ve diğer insanların deneyimlerinden dolandırıcıların kendilerini nasıl etkilediğini veya olaya nasıl tepki verdiklerini öğrenebilir. Etkilenen bireylerin incelenmesi hasarın boyutunu değerlendirmeye yardımcı olacaktır. Kuruluşlar da kendi iç siber güvenlik farkındalık kampanyalarının bir parçası olarak eğitim sunmalıdır. Kullanıcılar, bir saldırganın hedef alacağı psikolojik güvenlik açıklarının farkında olmalı ve bu tür konuşmalara girmekten kaçınmalıdır.

Egelman ve Peer (2015) tarafından önerilen dört ana kullanıcı güvenlik davranışı kategorisine odaklanmak kullanıcıları sınıflandırmaya ve onların SGF davranışlarını incelemek için uygun bir yöntemdir (Yılmaz, 2023). Bu güvenlik davranışları cihaz güvenliği, parola oluşturma, proaktif farkındalık ve güncellemedir.

- Cihaz güvenliği, cihazları kilitlemek, otomatik cihaz veya ekran kilitlemeyi ayarlamak ve cihazları gözetimsiz bırakmadan önce manuel olarak güvenceye almak için PIN'lerin ve şifrelerin kullanılması anlamına gelir.
- Parola oluşturma, güçlü parolalar seçmeyi ve parolaları farklı hesaplar arasında yeniden kullanmamayı ifade eder.
- Proaktif farkındalık web sitelerinde veya e-posta mesajlarında URL çubuğu veya diğer tarayıcı göstergeleri gibi bağlamsal ipuçlarına dikkat etmeyi, web sitelerine bilgi gönderirken dikkatli olmayı ve güvenlik olaylarını bildirirken proaktif olmayı ifade eder.
- Son olarak güncelleme, kullanıcıların sürekli olarak güvenlik yamalarını ne ölçüde uyguladıklarını veya yazılımlarını başka bir şekilde güncel tuttuklarını ölçer (Gratian ve ark., 2018).

Kullanıcıların bireysel farklılıklarının ve kişilik özelliklerinin risk alma ve siber güvenlik önlemi almalarını nasıl etkilediğinin araştırmacılar tarafından derinlemesine incelenmesi bu açıdan önemlidir. Literatürde kullanıcıların uyumluluk, vicdanlılık, nevrotiklik, açıklık ve dışa dönüklük gibi kişilik özellikleri, cihaz güvenliği, parola oluşturma, proaktif farkındalık ve güncelleme konusundaki güvenlik davranışı niyetleriyle ilişkili olacağına dair çalışmalar mevcuttur,

Siber tehditler ve saldırılar her yaşta kullanıcıyı tehdit ederken çocuklar ve gençler önceki nesillere göre daha fazla maruz kalmaktadır. Dünyada yaşanılan Covid 19 pandemisi sırasında okulların ve üniversitelerin kapatılarak eğitimin online platformlar aracılığıyla verilmeye başlanması öğrencilerin daha fazla internette zaman harcamalarına sebep olmuş ve siber saldırılara ve kötü amaçlı yazılımlara maruz kalma olasılıklarını artırmıştır. 6 Şubat 2023 asrın felaketi denilen 11 şehri yıkan deprem felaketinden sonra da ülkemizde bazı illerde eğitim online hale gelmiş ve gençler yeniden sanal dünyaya gömülmüşlerdir.

Gençler özellikle internette özel verileri başkalarıyla paylaştıklarında sunulan kontrollerin olmaması nedeniyle tehlikeye atılabilir. Günümüzün bağlantılı dünyasında çocukların karşılaştığı tehlikeler ve riskler, yabancı tehlikesi, cinsel iletişim, siber zorbalık ve gelecekte kullanılmak üzere rutin olarak saklanan kişisel verilerin toplanmasına kadar geniştir (Dempsey ve ark., 2022). Çocuklar ve gençler, arkadaşları ve aileleriyle iletişim ve etkileşim kurmak, öğrenmek ve kendilerini geliştirmek için yoğun bir şekilde gündelik hayatlarında internet kullanmakta ve farklı uygulamaları aktif olarak kullanmaktadırlar. Bu durum savunmasız olan bu kişilerin daha fazla riskle karşılaşmalarına ve istenmeyen siber saldırılara, ihlalleri yaşamalarına yol açmaktadır. Bu nedenle özellikle aileler ve eğitimciler bu gençleri sanal dünyada yaşanabilecek olumsuz olaylar konusunda bilinçlendirmeli, sürekli uyarmalı ve kontrol etmelidir. Gençlerin internet kaynaklı riskleri yönetmelerine yardımcı olacak stratejiler geliştirilmeli ve onlara bilinçli bir eğitim çerçevesince verilmelidir.

2.2.22. Gençlere ve çocuklara yönelik siber güvenlik tehditleri ve siber güvenlik farkındalığı çalışmaları

Bu başlık altında yurtiçi ve yurtdışında gençler ve çocuklara yönelik siber güvenlik tehditleri ve siber güvenlik farkındalığı çalışmaları ayrıntılı olarak incelenerek konunun kuramsal çerçevesi oluşturulmaya çalışılmıştır.

Hamdan ve diğerlerinin (2013), 13-18 yaş aralığındaki 150 genç ile yürüttükleri çalışmalarında siber güvenlik tehditlerini araştırdıkları çalışmalarının sonucunda günlük 5 saat ve üstü internet kullanan gençlerin daha fazla siber saldırıya maruz kaldıkları ancak daha fazla siber güvenlik farkındalığına sahip olduklarını gözlemlemişlerdir.

Clemons ve Wilson, (2015), genç internet kullanıcılarının okul e-posta hesaplarının çevrim içi sosyal mühendisliğe ve çeşitli çevrim içi kaynaklardan bilgi bağlantılarına yönelik

tutumları ve tercihleri hakkında nitel araştırma gerçekleştirmiştir. Çalışma Amerika Birleşik Devletleri, Arjantin, Brezilya, Şili, Kolombiya, Almanya, Japonya ve Meksika'da çevrim içi olarak gerçekleştirilen veli ve öğrencilerle yapılan anketlere dayanmaktadır. Çalışma sonunda öğrenciler ve diğer genç nüfus arasında, kişisel mahremiyeti göz ardı etme ve ifade edilen tercihlerle tutarsız davranışlarda bulunma kararlarının neredeyse evrensel olduğu tespit edilmiştir (Yılmaz, 2023).

Alqathani (2022) tarafından, Suudi Arabistan'da üniversite öğrencileri ile yürütülen bir çalışma sonucunda, öğrencilerin bilgi güvenliği konusunun önemli olduğunu vurgulamalarına rağmen şifreleme, browser araçları ayarlamaları konularında birçok bilgi ve uygulama eksiklikleri olduğu sonucuna ulaşılmıştır (Demir ve Sarı, 2023). Bir başka çalışmada, Gabra ve diğ. (2020), Nijerya'da üniversite öğrencilerinin temel siber güvenlik ve bilgi güvenliği konularını bildiklerini fakat verileri korumayı nasıl gerçekleştirebilecekleri konusunda yetersiz oldukları sonucuna ulaşmıştır. Ayrıca öğrencilerin bu konulara yönelik herhangi bir eğitim almadıkları da görülmüştür (aktaran Demir ve Sarı, 2023).

Choong, Theofanos, Renaud, ve Prior (2019), çocukların şifre güvenliğinin çok önemli olduğu bir dünyaya daha etkili bir şekilde hazırlanmasına katkı sağlamak, şifre konusundaki bilgi ve deneyimlerini tespit etmek için bir anket geliştirmiş ve iki okuldan farklı düzeylerde 189 okul öğrenciden verileri toplamıştır. Çalışma sonucunda 6-8. sınıf öğrencileri şifreleriyle daha fazla zorluk yaşadıklarını bildirmişler ve şifrelerini korumak için daha fazla mücadele ettikleri ortaya çıkmıştır.

Siber güvenlik farkındalığını etkileyen faktörleri kuşaksal bir mercek aracılığıyla inceleyen Redekop (2016) 171 katılımcı üzerinde deneysel bir çalışma gerçekleştirilmiştir. Kuşaklar arasında siber güvenlik bilinci ve farkındalığı seviyeleri arasında farklılık olduğu sonucuna varmıştır. Bireylerin siber güvenlik farkındalık eğitimine ihtiyaç olduğu sonucu elde edilmiştir (Ünsal, 2022).

Görme engelli internet kullanıcılar üzerinde yapılan bir araştırmada, katılımcılara siber güvenlik tehditleri ve endişeleri sorulduğunda, büyük çoğunluğun endişeli veya çok endişeli olduklarını ifade ettikleri gözlemlenmiştir. Belirli konularla ilgili olarak, birileri tarafından veri hırsızlığı yapması (%70) veya finansal bilgilere erişmesi (%65) ve kişisel bilgilerin kamuya açıklanması (%65) gibi konularda da yüksek endişe duydukları ortaya çıkmıştır. Ayrıca bilgi işlem cihazına virüs bulaşma olasılığı veya kötü amaçlı yazılım

kurbanı olmak (%35) gibi konularda ise daha düşük endişe duyduklarını ifade etmişlerdir (İnan ve diğ., 2016).

Okullardaki siber güvenlik eğitimini ele alındığı bir araştırmada birçok nedenden ötürü siber güvenlik içeriğinin okul müfredatında yer almadığı ve eğitimcilerin de siber güvenlik konusunda yeterli donanıma sahip olmadıklarını belirtmektedir (Pye, 2016).

Kritzinger (2020) çalışmasında okullar ve öğretmenler için siber güvenlik kültürünü nasıl tasarlayabilecekleri, uygulayabilecekleri ve büyütebilecekleri de dahil olmak üzere siber güvenlik farkındalığı kılavuzları önermektedir (Ünsal, 2022).

Griffin (2021) araştırmasında siber güvenlik farkındalık eğitim programlarının etkisi ve programın kuruluşlarda ne kadar etkili ve verimli olduğu konusunda bilgi birikimine katkıda bulunmayı amaçlamıştır. Bu çalışmada ele alınan genel sorun, çalışanların ihmali ve etkisiz siber güvenlik farkındalığı eğitimi nedeniyle kuruluşlarda güvenlik ihlallerinin yaşanmasıdır. Araştırma sonucunda eğitim, güvenlik riskleri, güvenlik politikaları erişim kontrolleri ve liderlik farkındalığı olmak üzere dört farklı temanın ortaya çıktığı görülmüştür.

Benzer şekilde, Birleşik Krallık "Fair Trade Office" raporuna göre, yaklaşık Web kullanıcılarının %80'i çevrimiçi alışveriş yaparken ödeme ayrıntılarının güvenliğinden endişe duyduklarını ortaya koymaktadır. Bu endişeler, muhtemelen günümüzde artan e-ticaret hacmine paralel olarak daha yüksek olduğu tahmin edilebilir (İnan ve diğ., 2016).

Yetişkin öğrenme teorilerinde en iyi uygulamaların neler olduğunu ve bunların günümüz kurumsal siber güvenlik eğitim programlarında nasıl uygulanabileceğini incelendiği araştırmanın bulguları; harmanlanmış öğrenmenin yetişkinler için en iyi öğrenme yöntemi olduğunu iddia etmiştir (Jeffers, 2016).

Yurt içinde yapılan çalışmalarda siber güvenlik kavramının yanı sıra bilgi güvenliği kavramı üzerinde de araştırmaların yapıldığı saptanmıştır. Erol ve diğerleri (2015) "Siber Güvenlik Ölçeği" ni kullanarak yaptıkları araştırmalarının sonucunda öğrencilerin siber güvenlik farkındalık durumlarının orta düzeyde olduğunu ortaya koymuşlardır. Öğrencilerin güvenilmeyenden kaçınmakta ve güvenlik için önlem alabildikleri tespit edilmiş olup internet üzerinde gezinirken iz bırakmamaya dikkat ettikleri belirlenmiştir.

Bir çalışmada 2.449 ilköğretim ve lise öğrencisinin bilgi güvenliği ve bilgisayar farkındalık düzeylerini ortaya çıkarmak amaçlanmış ve sonuç olarak öğrencilerin bilgi güvenliği tehditleri ve bilgi güvenliği önlemleri hakkında çok az düzeyde bilgiye sahip oldukları ortaya çıkmıştır (Tekerek ve Tekerek, 2013). Ayrıca bu çalışmada kız öğrencilerin erkek öğrencilere oranla bilgi güvenliği farkındalığının yüksek olduğu, öğrenim seviyesi

arttıkça yine bilgi güvenliği farkındalığının arttığı, yerleşim yerine bakıldığında ise kırsalda olan öğrencilere nazaran ilçe merkezinde bulunan öğrencilerin farkındalığının anlamlı oranda yüksek olduğu tespit edilmiştir.

Karacı vd. (2017) araştırmasında bilgisayar ve öğretim teknolojileri bölümü ve bilgisayar mühendisliği bölümü 170 öğrencinin siber güvenlik davranışlarını araştırmışlardır. Araştırma bulguları; öğrencilerin siber güvenlik davranış düzeylerinin yüksek olduğu ve erkek ve kadınlar arasında farklılık olmadığını göstermiştir. İş deneyimi ya da siber güvenlik dersi alan öğrencilerin daha olumlu davranışa sahip oldukları ve meslek lisesinden gelen öğrencilerin siber güvenlik davranışları açısından daha dikkatli oldukları gözlenmiştir.

Üniversite öğrencilerinin siber güvenlik ve siber suç farkındalıklarını incelemek maksadıyla 368 öğrenci ile nicel bir araştırma gerçekleştirilmiştir. Araştırma bulguları; öğrencilerin siber güvenlik farkındalık düzeylerinin düşük seviyede olduğu ve cinsiyete, yaşa, günlük internette geçirilen süreye göre anlamlı bir farklılık olduğunu ortaya koymuştur (Aksoğan ark., 2018).

Yalın ve Başfırıncı (2018) araştırmalarında üniversite öğrencilerinin siber güvenlik algılarını incelemişlerdir. 283 iletişim fakültesi öğrencisi üzerinde nitel bir yöntem ile araştırma gerçekleştirilmiştir. Araştırma sonuçları; iletişim fakültesi öğrencilerinin siber güvenlik farkındalık düzeylerinin yüksek olduğu fakat siber tehditlere karşı kendilerini güvende hissetmediklerini ve bu nedenden dolayı dikkatli davrandıklarını ortaya koymuştur.

Yakın tarihte ülkemizde yürütülen bir çalışmada öğrencilerin siber güvenliğe yönelik farkındalıklarının genel itibarıyla orta düzeyde olduğu ortaya çıkmıştır (Tokmak, 2023). Öğrencilerin spesifik olarak oltalama saldırılarının nasıl gerçekleştiği ile ilgili yeterli bilgi birikimine sahip olmadıkları gözlemlenmiş. Ayrıca siber güvenlik farkındalıkları bakımından cinsiyetin anlamlı bir fark yaratmadığı ancak kadın öğrencilerin siber ortamda saklanan verilerin güvenliğine daha şüpheci baktıkları görülmüştür. Katılımcıların okudukları bölümlerin siber güvenlik farkındalığı açısından anlamlı farklılıklar yarattığı müfredatlarında siber güvenlikle ilgili derslerin ve içerikleri olduğu bilişim sistemleri ile ilgili bölümlerin, diğer bölümlere nazaran siber güvenlik farkındalıklarının daha yüksek olduğu saptanmıştır.

Yiğit ve Seferoğlu (2019) araştırmalarında, üniversite öğrencilerinin siber güvenlik davranışlarının beş faktör kişilik özellikleri arasındaki ilişkiyi incelemişler ve araştırma farklı üniversite, bölüm ve sınıflardan 420 öğrenci üzerinde nicel bir yöntem ile

gerçekleştirilmiştir. Araştırma bulgularına göre; öğrencilerin siber güvenlik davranış düzeylerinin kabul edilebilir bir seviyede olduğu ve beş faktör kişilik boyutları arasında anlamlı bir ilişki olduğu sonucu elde edilmiştir. Siber güvenlik davranışlarıyla en güçlü ilişkiye deneyime açıklık, en zayıf ilişkiye ise dışadönüklük kişilik özelliklerinin sahip olduğu tespit edilmiştir.

Aydaner (2019) ise araştırmasında online ortamlarda alışveriş yapan genç tüketicilerin, sosyal mühendislik ile siber güvenlik farkındalıklarını incelemek amacıyla 693 öğrenci ile nicel bir çalışma gerçekleştirmiştir. Araştırma sonucunda; genç tüketicilerin sosyal mühendislik farkındalıklarında meydana gelen değişimin, çok güçlü bir oran olan %65'lik bir kısmının, öğrencilerin 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.

Aslanyürek, M. (2016) çalışmalarında, aktif internet kullanıcı sayısının 2,5 milyara ulaştığı günümüzde internet ve siber ortamda devletin gözetim teknolojilerini kullandığını belirtmiş ve internet servis sağlayıcılarının ve şirketlerin pazarlama faaliyetleri amacıyla çevrimiçi ortamda bulunan kişisel verileri topladığını ifade etmiştir. Ayrıca, bilgisayarkorsanlarının ise kötü amaçlı faaliyetleri nedeniyle internet güvenliği ve çevrimiçi gizlilik alanında birçok ihlale sebep olduğunu ortaya koymuştur. Bu bağlamda, çalışmasında ülkemizdeki internet kullanıcılarının internet güvenliği ve çevrimiçi gizlilik alanlarındaki ihlaller karşısında kanaatlerini ve farkındalıklarını değerlendirmeyi amaçlamıştır. Araştırma bulguları, çevrimiçi gizlilik ve güvenlik ihlalleri karşısında internet kullanıcılarının farkındalık boyutunun yüksek olduğunu, fakat bu ihlaller karşısında internet kullanımından vazgeçme eğilimlerinin düşük olduğunu ortaya koymuştur (Aslanyürek, 2016).

Cihan ve Yıldız (2021) çalışmalarında, sosyal medyanın yaygınlaşmasıyla birlikte toplumsal hayatta hızlı değişimler yaşandığını ve bu platformlarda kullanıcıların paylaşımlarının ve etkileşimlerinin güncel yaşamı doğrudan etkilediğini belirtmektedirler. Bu etkilerden biri de kriminal alanda gerçekleşmektedir ve suçlular, sosyal medyanın sunduğu imkanları kullanarak daha kolay ve daha az riskle suç işleme avantajına sahip olabilmektedirler. Ancak, sosyal medyanın denetiminde yaşanan güçlükler, güvenlik güçlerinin siber suçları takip etme konusundaki tecrübe eksikliği, uluslararası boyutta olan bazı suçların yargılama süreçleri ve ağ sağlayıcı firmaların duyarsızlığı, siber suçların takibini ve soruşturulmasını zorlaştırmaktadır. Bu çalışmada, sosyal medya aracılığıyla işlenen suç türlerini ve bu suçların bireysel ve sosyal yaşama etkilerini incelenmiştir. Facebook, Twitter ve Instagram gibi sosyal medya platformları

aracılığıyla işlenen suçların miktarı, oranları, çeşitleri, yaygınlığı ve sosyal yaşama etkileri araştırma kapsamında incelenmeye çalışılmıştır.

Özbek (2019) eğitim fakültelerinde öğrenim gören öğretmen adaylarının kişisel siber güvenlik sağlama durumlarını inceleyerek demografik özellikleri ile kişisel siber güvenlik sağlama durumları arasındaki ilişkiyi analiz etmiştir. Araştırma sonucunda öğretmen adaylarının kişisel siber güvenlik sağlama durumlarının orta düzeyde olduğu, bu durumun erkeklerde kadınlara oranla daha yüksek düzeyde olduğu, katılımcıların akademik başarı ve öğrenim gördükleri sınıf düzeylerine göre bu durumda bir farklılık olmadığı ve bu farkındalığın interneti daha sık kullananlarda yüksek düzeyde olduğu görülmüştür.

Altıner (2021) araştırmasında kadın öğretmenlerin erkek öğretmenlere nazaran internet ortamında daha bilinçli, dikkatli, temkinli davrandıkları ve siber güvenliklerini sağlama konusunda farkındalıklarının daha yüksek olduğuna da dikkat çekmektedir. Özellikle interneti yoğun olarak kullanan genç nesillere hitap eden onları yönlendirme ve farkındalık oluşturma şansı olan öğretmenlerin öncelikle kendi siber güvenliklerini sağlayabilmeleri önemlidir. Araştırmadan çıkan bu sonuca göre öğretmenlere siber güvenlik eğitimi verilmesi önerilebilir.

Benzer bir sonuç, Zwilling ve diğ. (2022) tarafından Türkiye, Polonya, Slovenya ve İsrail'deki üniversite öğrencileri ile gerçekleştirilen çalışmada da ortaya çıkmaktadır. Bu araştırma sonucuna göre katılımcıların siber güvenlik tehditlerine yönelik bilgilere sahip olmalarına rağmen güvenlik önlemleri almada ve çözüm üretmede yetersiz kaldıkları, basit ve en bilinen önlemleri uyguladıkları görülmüştür. Belirtilen araştırmalarda da vurgulandığı üzere; bilgi güvenliğine yönelik yaşanabilecek olumsuzluklara karşı alınabilecek ve en azından etkisini azaltabilecek en etkin yöntemlerinden birisi eğitimdir. Eğitim sürecinde en önemli adım eğitmen veya öğretmen eğitimleri olmaktadır.

Bu bağlamda Munzur Üniversitesi öğrencilerinin siber güvenlik farkındalık düzeyinin araştırılarak, bulgular doğrultusunda eğitimcilere ve gençlere öneriler sunmak amaçlanmıştır. Aşağıda bu konudaki alan çalışmasının ayrıntılarına yer verilmiştir.

3. UYGULAMA

Bu bölümde üniversite öğrencilerinin siber güvenlik farkındalık düzeylerini belirlemek amacıyla yürütülen bir alan çalışmasının ayrıntılarına yer verilmiştir.

3.1. Araştırmanın Amacı ve Önemi

Son 20 yıl içinde nesnelerin interneti (Internet of Things), bulut sistemleri, yapay zekâ vb. teknolojiler sayesinde gün içinde kullandığımız cihazlar (mutfak aletleri, arabalar, termostatlar, saatler vb.) gömülü sistemler aracılığıyla internete bağlanabilmektedir. Bu sayede insanlar, süreçler ve cihazlar arasında dijital verinin üretilmesi, işlenmesi, kaydedilmesi, depolanması ve dağıtılması sağlanmaktadır. Dijital veri biçimleri günümüz dünyasında benzeri görülmemiş bir ölçekte üretilmekte ve işlenmektedir (Selwyn, 2015). Cihazların birbirleriyle haberleşmeleri ve verilerin dijital olarak işlenmesi son kullanıcılar için kolaylık sağlasa da ağa bağlı cihazların sayısının artması ve cihazlar arasında daha fazla dijital veri paylaşılması, verilerin çalınması, değiştirilmesi ya da paylaşılması olasılığını da artırmaktadır. İnternette yapılan her işlemin ardında zamanla biriken bir veri izi bıraktığı dikkate alındığında, siber güvenlik tehdidinin ne kadar büyük olduğu da ortaya çıkmaktadır. Bu nedenle ağların ve dijital verilerin korunmasına ihtiyaç duyulmaktadır.

Elektronik cihaz ve internet kullanımı günlük hayatımızı kolaylaştırsa da verilerimizin güvenliği açısından ciddi riskler oluşturmaktadır. Kullanıcıların internet ortamında karşılaştıkları ihlal ve riskler yıllara ve değişen teknoloji nedeniyle farklı tanımlamalarda bulunulmuştur. 2004-2010 yılları arasında yaşanan bu ihlaller bilgi güvenliği ve bilgisayar güvenliği kavramları kullanılmış, 2016 yılında Siber Güvenlik (Cyber Security) kavramının kullanımıyla birlikte diğer kavramların kullanımında azalma görülmüştür. 2021 yılı itibariyle alana hâkim kavram siber güvenlik olmuştur. Literatürde siber güvenlik kavramına karşılık çevrimiçi güvenlik, internet güvenliği gibi terimler kullanılmakta internet ortamındaki güvenlik endişelerini belirtmek için birbirlerinin yerine kullanılmaktadır (Quayyum, Cruzes ve Jaccheri, 2021). Siber güvenlik, internet güvenliği, bilgi güvenliği ve bilgisayar güvenliği ile ilişkilendirilen genel bir terimdir. Ancak kapsamı, uygulamayı ve doğru kullanımını anlamak önemlidir. Siber güvenlik, birçok kişi tarafından yanlış anlaşıldığı gibi, bilgisayarların sadece internet üzerindeki güvenliğini sağlamakla sınırlı değildir. Siber güvenlik, donanım, yazılım, veri ve bilgilerin her türlü ihlalden

korunması olarak tanımlanabilir. Siber güvenlik, veri koruma ve bilgi güvenliğinin uygulanması için kurum ve kuruluşlar için en yüksek önceliği, bireyler için ise gizlilik, erişim kontrolü ve güvenlik olarak tanımlanabilir (Tirumala, Sathu ve Naidu, 2015; Toch ve ark., 2018). Şu anda, siber güvenliğin kapsamı, bireyleri siber zorbalığa karşı korumaya ve gelişmiş makine öğrenimi teknikleri kullanarak siber savaşı tanımlamaya yönelik olarak genişletilmiştir (Tirumala, Valluri ve Babu, 2019).

Dünyada siber güvenliğin sağlanmasına yönelik gerek devlet gerekse özel sektör tarafından ayrılan yüksek bütçe ve geliştirilen güvenlik önlemlerine rağmen siber saldırıların sayısı her geçen yıl artmaktadır. Donanım ve yazılım alanına yönelik güvenlik teknolojilerindeki gelişmeler sıradan kullanıcılar kaynaklı siber güvenlik ihlallerinin önüne geçilmesine imkân tanımamaktadır. Yapılan araştırmalar sonucu çoğu güvenlik ihlallerinin sıradan kullanıcılar olduğu tespit edilmiştir (Tuğal, Almaz ve Sevi, 2021). Sistemler donanım ve yazılımsal olarak güvenli olsa da siber saldırılara neden olan ihlallerin büyük bir kısmı "Son Kullanıcı Hatası" nedeniyle ortaya çıkmaktadır. Yaşanan güvenlik açıklarının %80' ini son kullanıcı hataları oluştururken siber güvenlik faaliyetleri sistem araçları ve teknolojiyi geliştirmek üzerine olmuştur. Hükümetler ve şirketler teknolojik olarak en güvenilir siber savunma teknolojisine sahip olsa dahi, son kullanıcı hatası, kişisel siber güvenlik bilgisi ve farkındalık eksikliği nedeniyle birçok kayıp yaşanmasının önüne geçememektedirler.

Dolayısıyla kullanıcıların gizlilik ve güvenlik risklerini ve kendilerini siber saldırılardan nasıl koruyacaklarını anlamaları modern yaşamda temel bir ihtiyaçtır. Siber güvenlik farkındalığı, "internet kullanıcılarını çeşitli siber tehditlere ve bilgisayarların ve verilerin bu tehditlere karşı savunmasızlığına karşı duyarlı olmaları için eğiten bir metodoloji" olarak tanımlanmaktadır (Abd Rahim, ark., 2015). Siber güvenlik farkındalığını "kullanıcıların bilgi güvenliğinin önemini, kuruluşun verilerini ve ağ sistemlerini güvende tutmak için yeterli düzeyde bilgi kontrolü uygulama sorumluluklarını anlama derecesi" olarak tanımlamıştır.

Yukarıdaki tanımlara dayanarak, siber güvenlik farkındalığının iki temel amacı vardır: son kullanıcıları siber güvenlik riskleri hakkında uyarmak ve siber güvenlik risklerini anlamalarını, internet kullanımı sırasında güvenliği benimsemeye yeterince adamak için geliştirmektir. Son kullanıcıdan kaynaklı hataların veya güvenlik açıklarının azaltılması, güvenliğin kişisel veya kurumsal düzeyde iyileştirilmesinde kilit bir faktördür (Giannakas, vd. 2019). Bu nedenle siber güvenlik hakkında kullanıcı farkındalığının artması gereklidir.

Ülkemizde siber güvenlik ile ilgili olarak Millî Eğitim Bakanlığı (MEB) ve Yüksek Öğretim Kurumuna (YÖK) bazı müfredatlarında yer vermelerine rağmen yeterli düzeyde olmadığı düşünülmektedir.

İnsanlar günümüzde teknolojiye her zamankinden daha fazla bağımlı hale gelmiş bulunmaktadır. Toplumun modern gelişmelere ilişkin olumlu algısına rağmen, teknolojinin getirdiği siber güvenlik tehditleri de gerçek bir tehlikedir. Pandemi dönemi bilgi ve iletişim teknolojilerinin kullanımının artmasıyla birlikte siber saldırı sayısı da artmıştır. Yaşı ne olursa olsun tüm kullanıcılar internette zaman geçirirken çeşitli güvenlik risklerine maruz kalmaktadır. Bu risklere en fazla maruz kalan son kullanıcılar ise özellikle küçük yaştaki kullanıcılardır. Bu nedenle kullanıcıların siber güvenlik farkındalığı kazanması oldukça önemlidir. Genç kullanıcıların mevcut siber güvenlik farkındalıklarını analiz etmek için siber güvenlik farkındalığı ölçeğine ihtiyaç duyulmaktadır.

3.2. Araştırmanın Modeli

Bu araştırma nicel araştırma yaklaşımı ile ilişkisel tarama modelinde tasarlanmıştır. İlişkisel tarama modelleri, iki veya daha çok sayıdaki değişken arasındaki birlikte değişimin varlığı veya derecesini belirlemeyi amaçlar (Karasar, 2016). Araştırmada bağımsız değişken olarak sosyo-demografik özellikler, bağımlı değişken olarak siber güvenlik farkındalığı kullanılacaktır.

Kuramsal çerçeve doğrultusunda, bu çalışmanın amacı; üniversite öğrencilerinin farklı değişkenler açısından siber güvenlik farkındalıklarını incelemek amaçlanmıştır.

Üniversite öğrencilerinin siber güvenlik farkındalıkları toplam puan ve alt boyutlarda;

a) Cinsiyet değişkenine göre farklılaşmakta mıdır?

b) Sınıf düzeyi değişkenine göre farklılaşmakta mıdır?

c) İnternet ve bilişim teknolojileri kullanma sürelerine göre farklılaşmakta mıdır?

d) Öğrenim görülen okul türüne göre farklılaşmakta mıdır?

e) Öğrenim görülen bölüme göre farklılaşmakta mıdır?

3.3. Araştırmanın Evreni ve Örneklemi

Munzur Üniversitesinin Aktuluk kampüsünde aynı binada eğitim gören İİBF ve Güzel Sanatlar Fakültesinde eğitim gören toplam 368 öğrenci çalışmanın ana evrenini oluşturmaktadır. Kolayda örnekleme yöntemiyle 125 öğrenciye anket formu dağıtıldı ve eksik ve baştan savma doldurulmuş formlar elenerek 101 katılımcıdan veri toplanmıştır.

3.4. Araştırmanın Sınırlılıkları ve Varsayımları

Araştırma, sadece bir kamu üniversitesinin tek bir fakültesinde eğitim gören öğrencilere uygulanmıştır. Bu çalışmanın en büyük kısıtı; araştırmanın bir fakülteyi kapsıyor olması, diğer fakülteleri, akademik birimleri veya diğer kamu üniversitelerini ve vakıf üniversitelerini kapsamıyor olmasıdır. Araştırmanın ikinci kısıdı kolayda örneklemeye gidilmiş olmasıdır.

Araştırma öz-raporlama (self-report) yöntemine dayandığından, katılımcıların verdikleri cevapların doğru olduğu, gerçek durumu yansıttığı varsayılmaktadır. Araştırmada kullanılan soru formunun ölçülmek istenen konuyu tam olarak ölçtüğü varsayılmaktadır.

3.5. Veri Toplama Araçları

Bu çalışmada anket veri toplama tekniği kullanılacaktır. Anket verileri yüz yüze görüşmelerde form doldurtularak toplanmıştır.

Anket düzenlemesi için çalışmanın amacına uygun olarak geçerliliği ve güvenirliliği gösterilmiş ölçüm aracı kullanılacaktır. Anketin birinci bölümünde katılımcıların sosyo-demografik özelliklerini tespit etmek için sorular yer almaktadır. İkinci bölümde siber güvenlik farkındalık ölçeği kullanılacaktır. Ölçek Yılmaz (2023) tarafından geliştirilmiş olup yazardan gerekli izinler alınmıştır. Ölçek 25 madde ve 4 alt boyuttan (Şifre Güvenliği, Önleyici Tedbirler, Kötü Amaçlı Yazılım Farkındalığı ve Kişisel Gizliliği Koruma) oluşmakta olup, orijinal çalışmada ölçeğin tamamına ilişkin Cronbach'ın alfa değeri 0,87 olmakla birlikte Şifre Güvenliği Alt Boyutu 0,92, Önleyici Tedbirler Alt Boyutu 0,82, Kötü Amaçlı Yazılım Farkındalığı Alt Boyutu 0,85 ve Kişisel Gizliliği Koruma Alt Boyutu 0,83' tür. Ölçek ifadelerinden bazıları şu şekildedir. "Şifre oluştururken özel karakterler, rakam ve harf kullanılması gerektiğini bilirim.", "Parolamı en az 8 karakterden oluşması gerektiğini

bilirim.", "Tanımadığım kişilerden gelen e-postada samimi ifadeler varsa (sevgili beyefendi/ hanımefendi vb.) dikkatli olmam gerektiğini bilirim." Ve "Bir e-postadaki veya sosyal medya gönderisindeki bağlantılara tıklama konusunda dikkat ederim."

Ölçek 1- Hiç Katılmıyorum 2- Katılmıyorum 3- Kararsızım (fikrim yok) 4- Katılıyorum 5- Tamamen Katılıyorum şeklinde derecelendirmesi yapılan 5"li likert tipi ölçeklerdir.

3.6. Verilerin Değerlendirilmesi

Araştırmada elde edilen verilerin değerlendirilmesinde Statistical Package for Social Science for Windows (SPSS) 24.0 paket programı kullanılmıştır.

Araştırmadan elde edilen verilerin analizinde;

- Katılımcıların tanıtıcı özelliklerinin frekans ve yüzde dağılımları,
- Siber Güvenlik Farkındalık ölçeğinin güvenirlik çalışması kapsamında, tüm ölçeklerin cronbach alpha iç tutarlılık katsayısı,
- Siber Güvenlik Farkındalık ölçeğinin geçerlik çalışması kapsamında, faktör analizi yapılmıştır.
- Siber Güvenlik Farkındalık ölçeğine katılma düzeylerini belirlemek amacıyla ortalama ve standart sapma değerleri incelenmiştir.
- Siber Güvenlik Farkındalık ölçeğine katılma düzeylerinin, araştırmaya katılanların demografik özellikleri açısından farklılıklarını belirlemek amacıyla bağımsız örneklem t testi, tek yönlü varyans analizi, Tukey ve LSD testleri uygulanmıştır.

4. BULGULAR

Araştırmanın bu bölümünde öncelikle betimleyici istatistiklere yer verilecektir. Daha sonra geçerlilik ve güvenilirlik analizleri ve kurulan hipotezlerin test edilmesi için bağımsız örneklem t testi ve tek yönlü varyans analizleri (ANOVA) yapılacaktır.

4.1. Demografik Bulgular

Tablo 4.1'de araştırmaya katılanların demografik özelliklerinin frekans ve yüzde dağılımlarına yer verilmiştir.

Tablo 4.1. Katılımcıların demografik özelliklerine yönelik bulgular

Değişkenler	Kategori	Frekans	Yüzde (%)
Cinsiyet	Kadın	68	67,3
	Erkek	33	32,7
Yaş	18-25	89	88,1
	26-33	7	6,9
	34 ve üzeri	5	5,0
Bölüm	Finans ve Bankacılık	30	29,7
	Sağlık Yönetimi	24	23,8
	Siyaset Bilimi ve Kamu	21	20,8
	Yönetimi	11	10,9
	Uluslararası Ticaret ve	6	5,9
	İşletmecilik	9	8,9
	Müzik		
	Mimarlık		
Sınıf	1. Sınıf	51	50,05
	2. Sınıf	35	34,7
	3. Sınıf	9	8,9
	4. Sınıf	6	5,9
Günlük İnternet	1 Saatten Az	5	5,0
Kullanımı	1- 3 Saat Arası	22	21,8
	3 -5 Saat Arası	43	42,6
	5 Saatten Fazla	31	30,7
Bireyin Siber Saldırıya	Evet	15	14,9
Maruz Kalma Durumu	Hayır	71	70,03
	Fikrim Yok	15	14,9
Ailenin Siber Saldırıya	Evet	10	9,9
Maruz Kalma Durumu	Hayır	61	60,4
	Fikrim Yok	30	29,7
Siber Güvenliği	Evet	42	41,6
Sağlayabilecek Bilgi ve	Hayır	29	28,7
Beceri Durumu	Fikrim Yok	30	29,7

Araştırmaya katılan 101 üniversite öğrencisinin demografik özellikleri incelendiğinde;

- 68 kişinin (%67,3) kadınlardan oluştuğu,
- 89 kişinin (%88,1) 18-25 yaş aralığında olduğu,
- 30 kişinin (%29,7) Finans ve Bankacılık bölümü öğrencisi olduğu,
- 51 kişinin (%50,05) üniversite 1. sınıf öğrencisi olduğu
- 43 kişinin (%42,6) günlük internet kullanımının 3-5 saat aralığında olduğu,
- 71 kişinin (%70,03) siber saldırıya maruz kalmadığı,
- 61 kişinin (%60,4) ailesinin veya yakın çevresinin siber saldırıya maruz kalmadığı,
- 42 kişinin (%41,6) siber güvenliği sağlayabilecek bilgi ve beceriye sahip olduğu görülmektedir.

4.2. Normallik Analizi

Farklılık analizleri, korelasyon ve regresyon analizleri gibi parametrik testleri yapabilmek için verilerin normal dağılım göstermesi gerekmektedir. Bu sebeple normallik testi yapılmaktadır. Normal dağılım analizinde "Tests of Normality" kısmında yer alan Kolmogorov-Smirnov significant değeri 0,05'den büyük olmalıdır. Ancak sosyal bilimlerde özellikle 5'li likertli çalışmalarda bu değerin 0,05'den büyük olması oldukça zordur. Bu sebeple parametrik testlerin yapılabilmesi için Skewness ve Kurtosis (Çarpıklık ve Basıklık) değerlerine de bakılmaktadır. Bu değerlerin "-2" ve "+2" aralığında olması, verilerin normal dağılım gösterdiği anlamına gelmektedir (George ve Mallery, 2010).

Tablo 4.2. Normallik analizi bulguları

Ortalamalar	**Skewness (Çarpıklık)**	**Kurtosis (Basıklık)**
Siber Güvenlik	1,200	1,490
*Şifre güvenliği	0,844	1,093
*Önleyici tedbirler	1,427	1,308
*Kötü amaçlı yazılım farkındalığı	1,307	1,973
*Kişisel gizliliği koruma	0,850	0,247

Tablo 4.2 incelendiğinde, siber güvenlik (Skewness= 1,200; Kurtosis=1,490), şifre güvenliği (Skewness= 0,844; Kurtosis= 1,093), önleyici tedbirler (Skewness=1,427; Kurtosis= 1,308), kötü amaçlı yazılım farkındalığı (Skewness=1,307; Kurtosis=1,973) ve kişisel gizliliği koruma (Skewness= 0,850 ; Kurtosis= 0,247) değerlerinin "-2" ve "+2" aralığında olduğu görülmektedir. Dolayısıyla elde edilen verilerin normal dağılım gösterdiği kanıtlanarak parametrik testlerin uygulanmasına karar verilmiştir.

4.3. Güvenilirlik Analizi

Yapılan araştırmada kullanılan ölçeğin güvenirliğinin ölçülmesinde Alfa Değeri (Cronbach Alpha) testinden yararlanılmıştır. Alfa katsayısının yorumlanmasında araştırmacılar tarafından belirli ölçütler dikkate alınmaktadır. Bu ölçütlere göre Cronbach Alfa katsayısı (α) değerleri şu şekildedir:

- $0,00 \leq \alpha < 0,40$ aralığında güvenilir değildir
- $0,40 \leq \alpha < 0,60$ aralığında düşük güvenilirliktedir
- $0,60 \leq \alpha < 0,80$ aralığında oldukça güvenilirdir
- $0,80 \leq \alpha < 1,00$ da yüksek güvenilirliktedir (Büyüköztürk, 2011).

Araştırmada kullanılan ölçeğin güvenilirlik Cronbach Alfa katsayısı değerleri Tablo 3'de gösterilmektedir.

Tablo 4.3. Güvenilirlik analizi bulguları

Değişkenler	**α değeri**
Siber Güvenlik	0,921
Şifre güvenliği	0,688
Önleyici tedbirler	0,894
Kötü amaçlı yazılım farkındalığı	0,778
Kişisel gizliliği koruma	0,691

Tablo 4.3 incelendiğinde;

- "Şifre güvenliği", "kötü amaçlı yazılım farkındalığı" ve "kişisel gizliliği koruma" alt boyutlarının güvenilir olduğu,
- "Siber Güvenlik Farkındalık Ölçeği" ve "önleyici tedbir" alt boyutunun yüksek güvenilirlikte olduğu görülmektedir.

4.4. Faktör Analizi

Faktör analizi, aynı yapıyı ölçen çok sayıda değişkenlerden az sayıda ve tanımlanabilir nitelikte anlamlı değişkenler elde etmeye yönelik bir veri analizidir. Faktör analizinin uygunluğunu belirlemek için KMO (Kaiser- Meyer- Olkin) ve Barlett testleri uygulanmaktadır. KMO testinin değeri 0 ile 1 aralığında olmalıdır. 0,8 üstü değerler mükemmel sayılabilir. Faktör yük değerlerinin ise 0,45 ya da daha yüksek olması iyi bir ölçüdür. Ancak uygulamadaki az sayıda önerme için bu sınır değeri, 0,30'a kadar indirilebilir (Büyüköztürk, 2011). Tablo 4'de ölçek maddelerinin faktör yüklerine, KMO ve Barlett testi değerlerine yer verilecektir.

Tablo 4.4. Siber güvenlik farkındalık ölçeğinin faktör analizi bulguları

Madde Sırası	**Faktör Yükleri**
11. madde	0,834
10. madde	0,805
8. madde	0,778
12. madde	0,756
18. madde	0,738
19. madde	0,731
6. madde	0,684
17. madde	0,674
4. madde	0,662
14. madde	0,653
13. madde	0,651
16. madde	0,649
25. madde	0,629
15. madde	0,615
1. madde	0,603
2. madde	0,579
23. madde	0,571
5. madde	0,544
22. madde	0,502
3. madde	0,603
7. madde	0,542
20. madde	0,413
Kaiser-Meyer-Olkin Measure of Sampling Adequacy (**KMO**): 0,851 **Bartlett's Test of Sphericity**: Approx. Chi-Square: 1587,737; df: 300; sig: 0,00	

Tablo 4.4 incelendiğinde KMO değeri 0,851 olarak hesaplanmıştır. Bu veri ölçeğe faktör analizi uygulayabilmek için örneklem büyüklüğünün yeterli olduğunu

göstermektedir. Faktör yükleri 0,413-0,834 arasında değişkenlik göstermektedir. Siber güvenlik farkındalık ölçeği faktör analizi bulguları, ölçeğin faktör yapısını ve geçerliliğini desteklemektedir. Buna karşın, faktör analizi sonucunda işlemeyen 3 madde ölçekten çıkarılmış ve faktör yükleri .40 üzerinde olan 22 madde ölçeğe alınmıştır.

4.5. Tanımlayıcı İstatistikler

Ölçek ortalama puanlarına bakılırken aritmetik ortalamalar hesaplanmaktadır. Likert tipi ölçeklerin ortalama puanlarının yorumlanmasında aşağıdaki puan aralıkları dikkate alınmaktadır.

Tablo 4.5. 5'li likert tipi ölçek puanları

Puan Aralığı	**Ölçekteki Karşılığı**
1,00-1,80	Kesinlikle Katılıyorum
1,81-2,60	Katılıyorum
2,61-3,40	Kararsızım
3,41-4,20	Katılmıyorum
4,21-5,00	Kesinlikle Katılmıyorum

Tablo 4.5 esas alınarak siber güvenlik farkındalık ölçeği ve alt boyutlarının ortalama, standart sapma ve ortalamanın ölçekteki karşılık puanına yer verilecektir.

Tablo 4.6. Katılımcıların siber güvenlik farkındalıklarına ilişkin bulgular

Değişkenler	**Ortalama**	**Standart Sapma**	**Ortalamanın Ölçekteki Karşılık Puanı**
Siber Güvenlik	1,67	0,60	1
*Şifre güvenliği	1,84	0,67	2
*Önleyici tedbirler	1,53	0,70	1
*Kötü amaçlı yazılım farkındalığı	1,59	0,63	1
*Kişisel gizliliği koruma	1,74	0,74	1

Tablo 4.6 incelendiğinde siber güvenlik farkındalık ölçeği ve önleyici tedbirler, kötü amaçlı yazılım farkındalığı ve kişisel gizliliği koruma alt boyutlarının ortalama puan değerlerinin "kesinlikle katılıyorum" seçeneğine denk geldiği; şifre güvenliği alt boyutunun ise "katılıyorum" seçeneğine denk geldiği tespit edilmiştir. Dolayısıyla araştırmaya dahil olan katılımcıların siber güvenlik farkındalıklarının oldukça yüksek olduğu sonucuna ulaşılmıştır.

4.6. Farklılık Analizleri

Farklılıkları incelemeye yönelik analizler, ölçek puanlarının katılımcıların demografik özelliklerine göre anlamlı farklılıklar gösterip göstermediğini tespit etmek için yapılmaktadır. İki değişkenli sorular için bağımsız örneklem t testi; üç ve üzeri değişkenli sorular içinse tek yönlü varyans analizi (ANOVA) analizi uygulanmaktadır.

Bu bölümde üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri; cinsiyet, yaş, bölüm, sınıf, günlük internet kullanımı süresi, bireyin siber saldırıya maruz kalma durumu, bireyin ailesinin veya yakın çevresinin siber saldırıya maruz kalma durumu ve bireyin siber güvenliği sağlayabilecek bilgi ve beceriye sahip olma durumuna göre incelenmiş ve bulguları aşağıda sunulmuştur.

4.7. Bağımsız Örneklem T Testi

Tablo 4.7'de katılımcıların siber güvenlik farkındalıklarının cinsiyete göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.7. Katılımcıların siber güvenlik farkındalık düzeylerinin cinsiyete göre farklılıkları

Değişkenler	Cinsiyet	Sayı	Ortalama	Standart Sapma	t	F	p
Siber Güvenlik	Kadın	68	1,65	0,55	-,634	3,391	0,528
	Erkek	33	1,73	0,68			
*Şifre güvenliği	Kadın	68	1,85	0,64	,107	1,777	0,915
	Erkek	33	1,83	0,73			
*Önleyici tedbirler	Kadın	68	1,46	0,63	-1,467	3,407	0,146
	Erkek	33	1,68	0,81			
*Kötü amaçlı yazılım farkındalığı	Kadın	68	1,59	0,63	,127	0,004	0,900
	Erkek	33	1,58	0,65			
*Kişisel gizliliği koruma	Kadın	68	1,70	0,67	-,900	3,268	0,370
	Erkek	33	1,84	0,87			

Tablo 4.7 incelendiğinde üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin cinsiyete göre istatistiksel olarak anlamlı farklılık göstermediği tespit edilmiştir ($p > 0,05$).

4.8. Tek Yönlü Varyans Analizi (ANOVA)

Tablo 4.8'de üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin yaş aralığına göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.8. Katılımcıların siber güvenlik farkındalık düzeylerinin yaş aralığına göre farklılıkları

Değişkenler	Yaş Aralığı	Sayı	Ortalama	Standart Sapma	F	p
Siber Güvenlik	18-25	89	1,66	0,59	0,300	0,741
	26-33	7	1,83	0,78		
	34 ve üzeri	5	1,75	0,52		
*Şifre güvenliği	18-25	89	1,81	0,64	1,130	0,327
	26-33	7	2,20	0,97		
	34 ve üzeri	5	1,91	0,61		
*Önleyici tedbirler	18-25	89	1,52	0,68	0,699	0,499
	26-33	7	1,81	1,06		
	34 ve üzeri	5	1,37	0,44		
*Kötü amaçlı yazılım farkındalığı	18-25	89	1,59	0,65	0,129	0,879
	26-33	7	1,47	0,46		
	34 ve üzeri	5	1,63	0,54		
*Kişisel gizliliği koruma	18-25	89	1,71	0,73	0,990	0,375
	26-33	7	1,77	0,80		
	34 ve üzeri	5	2,20	0,84		

Tablo 4.8 incelendiğinde üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin yaş aralığına göre istatistiksel olarak anlamlı farklılık göstermediği tespit edilmiştir ($p > 0,05$).

Tablo 4.9'da katılımcıların siber güvenlik farkındalık düzeylerinin üniversitede okudukları bölüme göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.9. Katılımcıların siber güvenlik farkındalık düzeylerinin okudukları bölüme göre farklılıkları

Değişkenler	Bölüm	Sayı	Ortalama	Standart Sapma	F	p
Siber Güvenlik	Finans ve Bankacılık	30	1,58	0,50		
	Sağlık Yönetimi	24	1,71	0,54		
	Siyaset Bil. ve Kamu Yön.	21	1,64	0,60	1,691	0,144
	Uluslararası Tic. ve	11	1,58	0,88		
	İşletmecilik	6	1,51	0,25		
	Müzik	9	2,19	0,66		
	Mimarlık					
*Şifre güvenliği	Finans ve Bankacılık	30	1,67	0,53	3,097	**0,012**
	Sağlık Yönetimi	24	1,92	0,48		
	Siyaset Bil.ve Kamu Yön.	21	1,85	0,64		
	Uluslararası Tic. ve	11	1,64	0,99		
	İşletmecilik	6	1,61	0,52		
	Müzik	9	2,55	0,80		
	Mimarlık					
*Önleyici tedbirler	Finans ve Bankacılık	30	1,40	0,53		
	Sağlık Yönetimi	24	1,62	0,74		
	Siyaset Bil. ve Kamu Yön.	21	1,56	0,69	1,927	0,097
	Uluslararası Tic. ve	11	1,48	0,82		
	İşletmecilik	6	1,07	0,11		
	Müzik	9	2,06	0,95		
	Mimarlık					
*Kötü amaçlı yazılım farkındalığı	Finans ve Bankacılık	30	1,62	0,63		
	Sağlık Yönetimi	24	1,55	0,63		
	Siyaset Bil. ve Kamu Yön.	21	1,56	0,62	0,093	0,993
	Uluslararası Tic. ve	11	1,57	0,94		
	İşletmecilik	6	1,55	0,51		
	Müzik	9	1,70	0,41		
	Mimarlık					
*Kişisel gizliliği koruma	Finans ve Bankacılık	30	1,66	0,59		
	Sağlık Yönetimi	24	1,75	0,84		
	Siyaset Bil. ve Kamu Yön.	21	1,55	0,70	2,161	0,065
	Uluslararası Tic. ve	11	1,67	0,86		
	İşletmecilik	6	1,93	0,50		
	Müzik	9	2,44	0,76		
	Mimarlık					

Tablo 4.9'da yer alan analiz sonucuna göre katılımcıların siber güvenlik farkındalıklarının okudukları bölüme göre anlamlı farklılık göstermediği saptanmıştır ($p > 0,05$).

Siber güvenlik farkındalığının alt boyutları incelendiğinde, "şifre güvenliği" alt boyutunun müzik bölümünde okuyan öğrenciler lehine anlamlı bir farklılık gösterdiği saptanmıştır ($p < 0,05$). Bu bağlamda müzik bölümünde okuyan öğrencilerin şifre

güvenliğini sağlama düzeylerinin daha yüksek olduğu sonucuna ulaşılabilir. "Önleyici tedbirler", "kötü amaçlı yazılım farkındalığı" ve "kişisel gizliliği koruma" alt boyutlarını ise öğrencilerin okudukları bölüme göre anlamlı bir farklılık göstermediği belirlenmiştir (p> 0,05).

Tablo 4.10'da katılımcıların siber güvenlik farkındalıklarının sınıf düzeylerine göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.10. Katılımcıların siber güvenlik farkındalıklarının sınıf düzeyine göre farklılıkları

Değişkenler	Sınıf	Sayı	Ortalama	Standart Sapma	F	p
Siber Güvenlik	1. Sınıf	51	1,72	0,63	2,355	0,077
	2. Sınıf	35	1,49	0,45		
	3. Sınıf	9	2,02	0,82		
	4. Sınıf	6	1,81	0,37		
*Şifre güvenliği	1. Sınıf	51	1,89	0,63	3,850	**0,012**
	2. sınıf	35	1,61	0,56		
	3. Sınıf	9	2,38	1,00		
	4. Sınıf	6	2,02	0,42		
*Önleyici tedbirler	1. Sınıf	51	1,59	0,70	2,560	0,059
	2. Sınıf	35	1,36	0,60		
	3. Sınıf	9	2,01	0,96		
	4. Sınıf	6	1,30	0,42		
*Kötü amaçlı yazılım farkındalığı	1. Sınıf	51	1,65	0,71	0,712	0,549
	2. Sınıf	35	1,46	0,52		
	3. Sınıf	9	1,70	0,69		
	4. Sınıf	6	1,61	0,49		
*Kişisel gizliliği koruma	1. Sınıf	51	1,75	0,78	2,902	**0,039**
	2. Sınıf	35	1,56	0,60		
	3. Sınıf	9	1,93	0,91		
	4.Sınıf	6	2,46	0,53		

Tablo 4.10'da yer alan analiz sonucuna göre katılımcıların siber güvenlik farkındalıklarının okudukları sınıf düzeyine göre anlamlı farklılık göstermediği saptanmıştır (p> 0,05).

Siber güvenlik farkındalığının alt boyutları incelendiğinde, "şifre güvenliği" ve "kişisel gizliliği koruma" alt boyutlarının 2. sınıfta okuyan öğrenciler lehine anlamlı bir farklılık gösterdiği saptanmıştır (p< 0,05). Bu bağlamda 2. sınıfta okuyan öğrencilerin şifre güvenliğini sağlama ve kişisel gizliliği koruma düzeylerinin daha yüksek olduğu sonucuna ulaşılabilir. "Önleyici tedbirler" ve "kötü amaçlı yazılım farkındalığı" alt boyutlarının ise

öğrencilerin okudukları sınıf düzeyine göre anlamlı bir farklılık göstermediği belirlenmiştir (p> 0,05).

Tablo 4.11'de katılımcıların siber güvenlik farkındalıklarının günlük internet kullanım sürelerine göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.11. Katılımcıların siber güvenlik farkındalıklarının günlük internet kullanım sürelerine göre farklılıkları

Değişkenler	Günlük İnternet Kullanımı	Sayı	Ortalama	Standart Sapma	F	p
Siber Güvenlik	1 saatten az	5	1,52	0,48		
	1-3 saat arası	22	1,77	0,64	0,895	0,447
	3-5 saat arası	43	1,73	0,66		
	5 saatten fazla	31	1,55	0,48		
*Şifre güvenliği	1 saatten az	5	1,68	0,46		
	1-3 saat arası	22	2,00	0,75	1,562	0,204
	3-5 saat arası	43	1,92	0,71		
	5 saatten fazla	31	1,65	0,52		
*Önleyici tedbirler	1 saatten az	5	1,45	0,50		
	1-3 saat arası	22	1,53	0,77	0,836	0,477
	3-5 saat arası	43	1,65	0,78		
	5 saatten fazla	31	1,39	0,54		
*Kötü amaçlı yazılım farkındalığı	1 saatten az	5	1,46	0,50		
	1-3 saat arası	22	1,70	0,68	0,413	0,744
	3-5 saat arası	43	1,60	0,69		
	5 saatten fazla	31	1,52	0,55		
*Kişisel gizliliği koruma	1 saatten az	5	1,48	0,50		
	1-3 saat arası	22	1,88	0,73	0,561	0,642
	3-5 saat arası	43	1,76	0,75		
	5 saatten fazla	31	1,67	0,78		

Tablo 4.11 incelendiğinde üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin günlük internet kullanım sürelerine göre istatistiksel olarak anlamlı farklılık göstermediği tespit edilmiştir (p > 0,05).

Tablo 4.12'de katılımcıların siber güvenlik farkındalık düzeylerinin, siber saldırıya maruz kalma durumuna göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.12. Katılımcıların siber güvenlik farkındalık düzeylerinin siber saldırıya maruz kalma durumuna göre farklılıkları

Değişkenler	**Siber Saldırıya Maruz Kalma Durumu**	**Sayı**	**Ortalama**	**Standart Sapma**	**F**	**p**
Siber Güvenlik	Evet	15	1,54	0,62		
	Hayır	71	1,67	0,56	0,736	0,482
	Fikrim Yok	15	1,81	0,74		
*Şifre	Evet	15	1,78	0,82		
güvenliği	Hayır	71	1,83	0,61	0,262	0,770
	Fikrim Yok	15	1,95	0,78		
*Önleyici	Evet	15	1,42	0,79		
tedbirler	Hayır	71	1,51	0,64	1,061	0,350
	Fikrim Yok	15	1,77	0,86		
*Kötü amaçlı	Evet	15	1,37	0,42		
yazılım	Hayır	71	1,60	0,65	1,239	0,294
farkındalığı	Fikrim Yok	15	1,73	0,71		
*Kişisel	Evet	15	1,60	0,70		
gizliliği	Hayır	71	1,76	0,74	0,340	0,713
koruma	Fikrim Yok	15	1,78	0,81		

Tablo 4.12 incelendiğinde üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin siber saldırıya maruz kalma durumuna göre istatistiksel olarak anlamlı farklılık göstermediği tespit edilmiştir ($p > 0,05$).

Tablo 4.13'te katılımcıların siber güvenlik farkındalık düzeylerinin, aile veya yakın çevrenin siber saldırıya maruz kalma durumuna göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.13. Katılımcıların siber güvenlik farkındalık düzeylerinin, aile veya yakın çevrenin siber saldırıya maruz kalma durumuna göre farklılıkları

Değişkenler	Aile veya Yakın Çevrenin Siber Saldırıya Maruz Kalma Durumu	Sayı	Ortalama	Standart Sapma	F	p
Siber Güvenlik	Evet	10	1,88	0,55		
	Hayır	61	1,59	0,58	1,739	0,181
	Fikrim Yok	30	1,78	0,63		
*Şifre güvenliği	Evet	10	2,01	0,72		
	Hayır	61	1,73	0,65	2,235	0,112
	Fikrim Yok	30	2,01	0,66		
*Önleyici tedbirler	Evet	10	1,80	0,73		
	Hayır	61	1,43	0,67	1,799	0,171
	Fikrim Yok	30	1,65	0,73		
*Kötü amaçlı yazılım farkındalığı	Evet	10	1,58	0,41		
	Hayır	61	1,55	0,65	0,387	0,680
	Fikrim Yok	30	1,67	0,66		
*Kişisel gizliliği koruma	Evet	10	2,16	0,82		
	Hayır	61	1,65	0,70	2,046	0,135
	Fikrim Yok	30	1,78	0,77		

Tablo 4.13 incelendiğinde üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin aile veya yakın çevrenin siber saldırıya maruz kalma durumuna göre istatistiksel olarak anlamlı farklılık göstermediği tespit edilmiştir ($p > 0,05$).

Tablo 4.14'te katılımcıların siber güvenlik farkındalık düzeylerinin, siber güvenliği sağlayabilecek bilgi ve beceriye sahip olma durumuna göre farklılık gösterip göstermediğine yönelik bulgular yer almaktadır.

Tablo 4.14. Katılımcıların siber güvenlik farkındalık düzeylerinin, siber güvenliği sağlayabilecek bilgi ve beceriye sahip olma durumuna göre farklılıkları

Değişkenler	Siber Güvenliği Sağlayabilecek Bilgi ve Beceriye Sahip Olma Durumu	Sayı	Ortalama	Standart Sapma	F	p
Siber Güvenlik	Evet	42	1,56	0,49		
	Hayır	29	1,76	0,68	1,377	0,257
	Fikrim Yok	30	1,75	0,63		
*Şifre güvenliği	Evet	42	1,68	0,56		
	Hayır	29	1,99	0,76	2,296	0,106
	Fikrim Yok	30	1,93	0,72		
*Önleyici tedbirler	Evet	42	1,41	0,55		
	Hayır	29	1,65	0,80	1,131	0,327
	Fikrim Yok	30	1,60	0,78		
*Kötü amaçlı yazılım farkındalığı	Evet	42	1,52	0,59		
	Hayır	29	1,64	0,72	0,365	0,695
	Fikrim Yok	30	1,63	0,62		
*Kişisel gizliliği koruma	Evet	42	1,64	0,72		
	Hayır	29	1,77	0,78	0,779	0,462
	Fikrim Yok	30	1,86	0,73		

Tablo 4.14 incelendiğinde üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin, siber güvenliği sağlayabilecek bilgi ve beceriye sahip olma durumuna göre istatistiksel olarak anlamlı farklılık göstermediği tespit edilmiştir ($p > 0,05$).

5. SONUÇ VE ÖNERİLER

İnternetin hayatımızın vazgeçilmez bir parçası olduğunu kabul ederek çocuk ve gençleri internet kullanımını sınırlamak yerine bilinçli kullanımını öğretmek gerekmektedir. Çoğu durumda, ebeveynler, çocuklarının izinsiz erişimlerinin ve uygunsuz çevrim içi sitelere maruz kalmalarının farkında değiller ve bu da çocukları siber güvenlik tehdidine maruz bırakmaktadır (Yılmaz, 2023). İnternetin faydalarından yararlanırken, çocukların artık daha erken yaşlarda internet erişimine sahip olması nedeniyle, ebeveynlerin veya çocukların siber zorbalık gibi potansiyel risklerin farkında olması ve güvenlik önlemleri alması önemlidir. Bu nedenle, çocukluktan başlayarak gençleri siber güvenlik farkındalığı kazandırmak gerekmektedir. Okul öğrencileri, etkili farkındalık programları ve eğitim yoluyla kendi siber güvenliklerinin sorumluluğunu almaya teşvik edilmeli ve donatılmalıdır (Kritzinger, Bada ve Nurse, 2017'den akt.,Yılmaz, 2023).

Ülkemizde siber güvenlik eğitimleri MEB ve YÖK'e bağlı akademik kurumların müfredatlarında yer almasına rağmen yeterli düzeyde değildir. Bilgi Güvenliği Derneği (BGD), Türkiye Bilişim Derneği (TBD) sivil toplum kuruluşları (STK) ya da özel organizasyonlar tarafından da verilen bu eğitimler kullanıcılarda siber güvenlik farkındalığının oluşturulması ve toplumun geneline yayılması için en önemlidir (Yılmaz, 2023). Siber güvenlik alanında farkındalık ve eğitim çalışmaları ilkokuldan itibaren verilmeli ve eğitim sisteminin her kademesinde ilgili ders müfredatı ile ilişkilendirilmelidir. Gelecek nesillerde "Siber Vatandaş" bilinci oluşturulmalıdır (Ünver, 2012). Siber saldırıları ve riskleri azaltmak için siber güvenlik farkındalığının artırılması gerekmektedir.

Bu çalışmada üniversite öğrencilerinin siber güvenlik farkındalıklarının incelenmesi amaçlanmıştır. Üniversite öğrencilerinin siber güvenlik farkındalıkları siber güvenliğin; şifre güvenliği, önleyici tedbirler, kötü amaçlı yazılım farkındalığı ve kişisel gizliliği koruma alt boyutlarıyla birlikte incelenmiştir. Üniversite öğrencilerine, demografik ve siber güvenlik farkındalığına yönelik sorular olmak üzere toplam 33 ifade yöneltilmiştir. Katılımcıların demografik özelliklerine göre siber güvenlik farkındalık düzeylerine bakıldığında;

- Üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin yüksek olduğu belirlenmiştir.
- Üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri; günlük internet kullanım süresi, bireyin siber saldırıya maruz kalma durumu, aile veya yakın

çevrenin siber saldırıya maruz kalma durumu ve siber güvenliği sağlayabilecek bilgi ve beceriye sağlayabilme durumuna göre anlamlı bir farklılık göstermemektedir.

- Siber güvenlik farkındalık düzeylerinde demografik değişkenlere göre (cinsiyet, yaş, bölüm, sınıf) anlamlı bir farklılık tespit edilmemiştir.
- Siber güvenliğin "şifre güvenliği" alt boyutunun müzik bölümünde okuyan öğrenciler lehine anlamlı bir farklılık gösterdiği saptanmıştır. Bu bağlamda müzik bölümünde okuyan öğrencilerin şifre güvenliğini sağlama düzeylerinin daha yüksek olduğu sonucuna ulaşılmaktadır.
- Siber güvenliğin "şifre güvenliği" ve "kişisel gizliliği koruma" alt boyutlarının 2. sınıfta okuyan öğrenciler lehine anlamlı bir farklılık gösterdiği saptanmıştır. Bu bağlamda 2. sınıfta okuyan öğrencilerin şifre güvenliğini sağlama ve kişisel gizliliği koruma düzeylerinin daha yüksek olduğu sonucuna ulaşılmaktadır.

Ebeveynlere ve gençlere siber güvenlik önlemleri açısından bazı tavsiyeler verilebilir.

- Araştırmalar ailelerin çocuklarının bilgi güvenliğini sağlama konusunda çocuklarına sadece uyarılarda bulunmakla yetindikleri, çocuklarına bilgi güvenliği konusunda yardımcı olmada yetersiz kaldıkları, tam olarak çocuklarına bilgi güvenliği konusunda bilgi veremediklerini gözler önüne sermektedir.
- Ülke genelinde yürütülecek programlarla toplumun her kesimine siber güvenlik farkındalığı ve siber güvenlik bilinci oluşturulması gerekmektedir.
- Ülkemizdeki ebeveynlerin bilgi güvenliği konusundaki farkındalıklarının tespit edilmesi sonrasında anne-babalara siber güvenlik ve bilgi mahremiyeti konusunda seminerler verilebilir.
- Özellikle siber saldırılara açık olan çocuklar ve gençlere evlerinde aileleri okullarda ise öğretmenler tarafından siber güvenlik kavramı ve siber suçlar hakkında düzenli eğitimler verilmelidir. Bu bağlamda ders müfredatlarına yeni bir konu olarak siber güvenlik eklenebilir, daha üst sınıflarda seçmeli siber güvenlik dersi konulabilir.
- Anne ve babalar çocuklarına daha erken yaştan itibaren bilgi mahremiyeti ve internet ortamında yaşayabilecekleri olumsuz olayları anlatarak bilinçlendirmeleri gerekmektedir.
- Hayatımızın bir parçası haline gelen mobil cihazları güvenli kullanabilmek için siber güvenlik sorunlarını, riskleri ve siber tehditlerin belirlenip gerekli önlem planlarının oluşturulması gerekmektedir.

- Bireyler kullandıkları tüm cihazlara sadece güvenilir kaynaklardan uygulamalar indirmeli olası siber saldırılara karşı uyanık olmalıdır.
- İndirilen uygulamaların cihazda ne tür verilere eriştiğini ve fonksiyonu itibariyle çalışması için gerçekten bu verilere erişmesi gerekip gerekmediğini sorgulanmalıdır.
- Internet bankacılığını kullanan bireylerin bu hususta eğitilmeleri, bazı zararlı yazılımlar vasıtasıyla siber saldırıların gerçekleştiği, hatta bu zararlı yazılımların kendilerini kullanıcıların bilgisayarında kullanmış oldukları anti-virüs yazılımlarından gizledikleri, siber saldırıların internet bankacılığı kullanan kullanıcıların sistemlerini çalışamaz hale getirdikleri, bu nedenle farklı boyutlarda önlem alınması gerekmektedir.
- Kişiler gelen mailde ya da mesajda, sahte e-posta adresleri ve isimler gibi bir saldırının emaresi olabilecek işaretlerin bulunup bulunmadığına dikkat etmelidir. E-posta içerisindeki yönlendirme bağlantılarının üzerine imleç getirilmeli ve birkaç saniye bekledikten sonra ekranda çıkan bağlantının tam adresi kontrol edilmelidir. Bir e-postadaki bağlantının üzerine imleci getirmek, bağlantının tam adresini ortaya çıkarttığı unutulmamalıdır.
- İnternet alışverişlerinde sanal kredi kartı teknolojisini kullanılarak limiti o an değiştirilebilen bir sistem kullanılmalıdır. İnternet 55 tarayıcısında ya da alışveriş yapılan web sitelerinde kart bilgileri saklanmamalıdır. Kredi kartlarının kullanılmadığı zamanlarda çevrimiçi alışverişe kapatılması önem arz etmektedir. Aynı zaman da 3D secure olmayan web sitelerinde alışveriş yapılmamalıdır.
- Kişisel bilişim sistemlerinin güvenliği bağlamında işletim sistemi güncellemelerinin zamanında yapılması, lisanslı anti virüs yazılımlarının kullanılması, güvenilirliği doğrulanmamış internet sitelerine giriş yapılmaması, elektronik postalara tanınmayan kaynaklardan gelen maillerin ve eklentilerinin açılmaması ve kullanılmadığı zamanlarda bilgisayarların kapalı tutulması, havaalanı kafe vb. yerlerde şifresiz olarak herkesin kullanımına açılan Wi-Fi ağlarına bağlanılmaması, internet üzerinden yapılan alışverişlerde sanal kart teknolojisinin kullanılması, internetten crack ya da patch gibi eklentiler kullanarak indirilen lisanslı olmayan programların kullanılmaması gibi önlemler almak mümkündür (Yılmaz, 2022).
- Hatırlanması gereken belki de en önemli kural, kişisel veya iş bilgilerinin asla telefonda paylaşılmaması gerektiğidir. Siber suçluların tipik olarak kullandığı farklı vishing saldırı türlerinin farkında olunmalıdır.

- İnternete bağlanan cihazların kullanılmadığı zamanlarda internet bağlantılarının kapatılması uygun olacaktır. Ayrıca akıllı cihazların parolaları varsayılan ayarda bırakılmamalı, sadece kendi kullanıcısının bildiği güçlü bir parola belirleyerek kullanılması son derece önemlidir. Cihazların Wi-Fi broadcast yayınları kapatılarak sadece seçilen kablosuz ağa manuel olarak bağlanması sağlanmalıdır.
- Parolalar cihazlar ve internet ortamında sunulan hizmetlerde alınan en temel güvenlik önlemidir. Parolaların ele geçirilmesi farklı kişiler tarafından kişisel verilerin istismar edilmesiyle sonuçlanabilir ya da bir başkası adına suç işlenmesine mahal verebilir. Bu sebeple parolalar cihazların üzerinde ya da internet tarayıcılarında saklanmamalıdır. Kullanılan her cihaz ya da platformda aynı parolayı kullanmak bir hesabın ele geçirilmesinden ötürü diğer hesapları da tehlikeye sokacağından, her platformda farklı parola kullanılmalıdır.
- Parolalar bir başkasıyla paylaşılmamalı kişisel olmalıdır. Parola oluştururken sadece rakam ya da harf kullanılmasından kaçınılmalı, iki büyük harf, iki küçük harf, iki rakam ve iki özel karakterden oluşan en az sekiz karakter uzunluğunda olacak şekilde belirlenmelidir. Kullanılan şifrelerde ad, soyad, doğum tarihi ve memleket bilgisi içeren bilgiler kullanılmamalıdır. Özetle parolalar diş fırçaları gibidir; her gün kullanılır, sıklıkla değiştirilir ve bir başkası ile paylaşılmaz (Yılmaz, 2022:48).

Yapılan araştırmalar ve sonuçlar dahilinde şu önerilerde bulunulabilir:

- Literatür analizleri, siber güvenlik sorununun sadece bilişim sistemini kullanan bireyin güvenlik sorunu olmaktan öte, ulusal ve uluslararası bir sorun olduğu, bu nedenle, siber güvenliğin kamuda, özel sektörde ve toplumun tüm kesimlerinde düzenli ve aksamadan yürütülebilmesi ve bilişim sistemini kullanan tüm bireylerin kullandıkları bilişim sistemlerinde siber güvenliğinin sağlanması noktasında gerek ulusal hukuk gerekse uluslararası hukuk düzeninin etkisinin çok büyük olduğu vurgulanmaktadır (Yılmaz ve Sağıroğlu, 2013). Dolasıyla ülkemizde ve dünyada siber güvenliğin sağlanması konusunda ulusal hukuk ve uluslararası hukuka çok büyük görevler düşmekte olup yasa yapıcıların siber suçlarla ilgili yeni düzenlemeler yapmaları gerekmektedir.
- Ülkemizde kamu kurumlarında ve özel sektörde bilişim sistemlerinde yaşanabilecek olası siber saldırıları önlemek için siber güvenlik konularında ileri boyutta siber güvenlik tedbirleri alınması için hukuki altyapının da hazırlanması gerektiği, Türk Ceza Kanunu (TCK) ve Ceza Muhakemeleri Kanununda (CMK) siber suçlarla

mücadele konusunda gerekli hukuki mevzuatın yapılması ve yasaların düzenlenmelere ihtiyaç duyulmaktadır (Hekim ve Başıbüyük, 2013).

- Üniversite öğrencilerinin siber güvenlik farkındalıklarının arttırılabilmesi için siber güvenlik uzmanları tarafından çeşitli eğitimler ve konferanslar verilmelidir. Hatta öğrenciler arasında siber güvenlik farkındalığının oluşturulabilmesi için bütün bölümlerde siber güvenlik konusuna yönelik zorunlu bir ders okutulmalıdır.
- Herhangi bir siber saldırı durumunda öğrencilerin nasıl tepkiler verdiğinin gözlemlenebilmesi ve nasıl müdahalede bulunulması gerektiği konusunda pratik deneyimler kazanılabilmesi için üniversitelerde siber güvenlik simülasyonları düzenlenmelidir.
- Toplumun farklı kesimleri için siber güvenlik, bilgi mahremiyeti ve siber suçlar gibi konularda eğitimler, seminerler verilebilir. Bu konulardaki kamu spotları, TV programları, afiş ve broşürler artırılabilir.
- Bu alandaki bilim insanlarının ileriki dönemlerde öğrencileri siber saldırılara karşı savunmasız bırakan ve siber güvenlik davranışını olumsuz etkileyen faktörlerin neler olduğu ortaya çıkartacak araştırmalara yönelmesi uygun olacaktır.
- Öğrenciler siber güvenliği tehdit eden unsurlara karşı bilinçli olmalıdırlar. Siber güvenliğin sağlanabilmesi için güçlü ve karmaşık şifreler oluşturulmalı ve iki adımlı doğrulama faktörü kullanılmalıdır. Güvenilir olmayan siteler ve bağlantılar tıklanmamalı ve önemli veriler düzenli olarak yedeklenmelidir.
- Bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmelerle birlikte uluslararası çatışmalar artık siber savaşlar yoluyla yapılmaktadır. Bu sebeple olası bir siber saldırıya karşı güvenliği sağlayabilmek için siber güvenlik uzmanlığı, güvenlik mühendisliği ve etik hackerlık gibi siber güvenlik mesleklerine gereken önem verilmelidir. Ayrıca üniversite tercih döneminde olan öğrencilere, siber güvenlik alanında uzmanlık gerektiren meslekleri seçmeleri konusunda tavsiyelerde bulunulmalıdır.
- Yerli yazında siber güvenlik konusuna yönelik daha kapsamlı araştırmalar yapılmalıdır. Siber güvenlik farkındalığının öneminin daha net bir şekilde anlaşılabilmesi için konunun farklı ana evrenlerde ve farklı değişkenlerle birlikte incelenmesi gerekmektedir.
- Siber güvenlik farkındalığı ve bilinci sektörden sektöre değişkenlik gösterebilmektedir. Bu sebeple hangi sektörde siber güvenlik bilincinin daha yüksek

olduğunun saptanabilmesi için siber güvenlik farkındalığına ilişkin sektörler arası araştırmanın yapılması gerekmektedir. Böylece siber güvenlik bilinci düzeyinin sektörden sektöre neden değişkenlik gösterdiği de ortaya çıkartılabilir.

6. KAYNAKLAR

Abd Rahim, N. H., Hamid, S., Kiah, M. L. M., Shamshirband, S., Furnell, S., 2015. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes,* 44(4):606-622.

Acılar, A., Baştuğ, A., 2016. Social engineering: Anformation secrity threat in enterprises. *Press Academia Procedia*, 2(1): 289-297.

Akça, E.B., Sayımer, İ., 2017. Siber zorbalık kavramı, türleri ve ilişkili olduğu faktörler: Mevcut araştırmalar üzerinden bir değerlendirme. *AJIT-e: Academic Journal of Information Technology*, *8*(30): 7-19.

Aksoğan, M., Bayer, H., Gülada, M. O., Çelik, E., 2018. İletişim fakültesi öğrencilerinin siber güvenlik farkındalığı: İnönü Üniversitesi örneği. *Kesit Akademi Dergisi*, (13): 271-288.

Altıner, İ., 2021. Öğretmenlerin kişisel siber güvenlik farkındalık düzeylerinin farklı değişkenlere göre değerlendirilmesi. *Yüksek Lisans Tezi,* Ankara Üniversitesi, Ankara.

Alzahrani, L., 2021. Statistical analysis of cybersecurity awareness issues in higher education institutes. *International Journal of Advanced Computer Science and Applications,* 12(11): 630-637.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior,* 69:437–343.

Arce, I., 2003. The weakest link revisited. *IEEE Security and Privacy,* 1(2): 72–76.

Atkinson, S., Furnell, S., Phippen, A., 2009. Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security,* 7: 13-19.

Aydaner, G., 2019. Genç tüketicilerin sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisinin ölçülmesi. *Yüksek Lisans Tezi,* Bandırma Onyedi Eylül Üniversitesi, Balıkesir.

Başeskioğlu, M. Ö., 2021. Siber güvenlik, bilgisayar ağları, kimlik avı, kötü amaçlı yazılım, fidye yazılımı, sosyal mühendislik biçiminde korsanlıktan korunmaya yönelik incelemeler ve bir uygulama. *Yüksek Lisans Tezi,* Yalova Üniversitesi, Yalova.

Baykara, M., Daş, R., 2019. Saldırı tespit ve engelleme araçlarının incelenmesi. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi,* 10(1): 57-75.

Bhattacherjee, A., Sanford, C., 2006. Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly,* 30(4): 805–825.

Bordeleau, F., Felden, C., 2019. Digitally transforming organisations: A review of change models of industry 4.0. In Pro-ceedings of ECIS 27.

Borrajo E, Gámez-Guadix M, Pereda N, Calvete E., 2015, The development and validation of the cyber dating abuse questionnaire among young couples. Computers in Human Behavior, 48:358365.

Bouncken, R.B, Fredrich, V., 2016. Learning in coopetition: Alliance orientation, network size and firm types. *Journal of Business Research*, 69(5): 1753-1778.

Brown, C., Hegarty, K., 2018. Digital dating abuse measures: A critical review. *Aggression and Violent Behavior,* 40: 44–59.

Büyüköztürk, Ş., 2011. Veri analizi el kitabı. Pegem Yayıncılık: Ankara.

Canbek, G., Sağıroğlu, Ş., 2007. Çocukların ve gençlerin bilgisayar ve internet güvenliği. *Gazi Üniversitesi Politeknik Dergisi,* 10(1): 33-39.

Choong, Y. Y., Theofanos, M. F., Renaud, K., Prior, S., 2019. Passwords Protect My Stuff A Study Of Children's Password Practices. Journal of Cybersecurity, 5(1): 1-15.

Connolly, J. A., McIsaac, C., 2009. Romantic relationships in adolescence. In R. M. Lehner, & L. Steinberg (Eds.). Handbook of adolescent psychology (pp. 479–523). Hoboken, NJ, USA: John Wiley & Sons.

D'Arcy, J., Herath, T., Shoss. M.K., 2018. Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems,* 31(2):285-318.

Daud, M., Rasiah. R., George, M., Asirvatham, D. Thangiah, G., 2018. Bridging the gap between organizational practices and cyber security compliance: Can cooperation promote compliance in organizations? *International Journal of Business & Society,* 19(1): 161-180.

Değirmenci, N., Demiral, D.G., 2023. Bilgi güvenliği farkındalığı üzerine üniversite öğrencilerine yönelik araştırma. *Karadeniz Sosyal Bilimler Dergisi*, 15(29): 613-635.

Demir, Ü., Sarı, B., 2023. Okul öncesi ve çocuk gelişimi bölüm öğrencilerinin bilgi güvenliği ve dijital okuryazarlık durumlarının incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, *20*(3): 760-769.

Dempsey, J., Sim, G., Cassidy, B., Ta, V. T., 2022. Children designing privacy warnings: Informing a set of design guidelines. *International Journal of Child Computer Interaction,* 31, 100446.

DiMaggio, P., Powell, W.W., 1983. The iron cage revisited: Collective rationality and institutional isomorphism in organizational fields. *American Sociological Review,* 48(2): 147-60.

Dimitropoulos, L, Patel, V, Scheffler, S., Posnack, S., 2011. Public attitudes toward health information exchange: Perceived benefits and concerns. *The American Journal of Managed Care,* 17 (12): 111-126.

Ding, S., Tukker, A., Ward, H., 2023. Opportunities and risks of internet of things (IoT) technologies for circular business models: A literature review. *Journal of environmental management*, *336*, 117662.

Dumanlı, D., 2011. Reklamlarda toplumsal cinsiyet kavramı ve kadın imgesinin kullanımı; bir içerik analizi. *Yalova Sosyal Bilimler Dergisi,* 1(2): 132-149.

Erdoğan, M., 2021. İşletmelerin kâbusu: İş e-postası dolandırıcılığı (BEC). *İşletme Akademisi Dergisi*, *2*(2): 208–219.

Ernest Chang, S., Ho, C.B., 2006. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3):345–361.

Erol, O., Şahin, Y. L., Yılmaz, E., Haseski, H. İ., 2015. Personal cyber security provision scale development study. *International Journal of Human Sciences,* 12(2): 75-91.

Fernet, M., Lapierre, A., Hébert, M., Cousineau, M. M., 2019. A systematic review of literature on cyber intimate partner victimization in adolescent girls and women. *Computers in Human Behavior*, *100*, 11-25.

Gao, X., Zhong, W. A., 2016. Differential game approach to security investment and information sharing in a competitive environment. *IIE Transactions,* 48(6): 511-26.

Gelderblom, O., Trivellato, F., 2019. The business history of the preindustrial world: Towards a comparative historical analysis. *Business History,* 61(2): 225-259.

George, D., Mallery, M., 2010. SPSS for windows step by step: A simple guide and refrence. 17.0 update, Boston: Pearson.

Giannakas, F., Papasalouros, A., Kambourakis, G., Gritzalis, S., 2019. A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, *28*(3): 81-106.

Gopal, A., Gosain, S., 2010. The role of organizational controls and boundary spanning in software development outsourcing: Implications for project performance. *Information Systems Research,* 21(4): 960–982.

Güldüren, C., Çetinkaya, L., Keser, H., 2016. Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online*, *15*(2): 682-695.

Gyde, M., 2017. Organisations must disrupt cyber attacks before. Bahrain This Week. Retrieved from, https://www.bahrainthisweek.com.

Hamdan, Z., Obaid, I., Ali, A., Hussain, H., Rajan, A. V., Ahamed, J., 2013. Protecting teenagers from potential internet security threats. International Conference on Current Trends in Information Technology, Dubai, United Arab Emirates.

Hasan, S., Ali, M., Kurnia, S., Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

Hekim, H., Başıbüyük, O., 2013. Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi,* 4(2): 135-158.

Henry, N., Powell, A., 2018. Technology-facilitated sexual violence: A literature review of empirical research. Trauma, *Violence, & Abuse,* 19(2), 195–208.

Hinduja, S., Patchin, J. W., 2011. Electronic dating violence: A brief guide for educators and parents. Retrieved from http://cyberbullying.org/electronic_dating_violence_fact_sheet.pdf.

Hsu, C., Lee, J.N, Straub, D.W., 2012. Institutional influences on information systems: Security innovations. *Information Systems Research,* 23(3): 918-939.

Huang, Y., Chou, C., 2010. An analysis of multiple factors of cyberbullying among junior high school students in Taiwan. *Computers in Human Behavior,* 26, 1581-1590.

Hwang, K., Choi, M., 2017. Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. *Government Information Quarterly,* 34(2): 183-198.

Livari, J., Huisman, M., 2007. The relationship between organizational culture and the of systems development Methodologies. *MIS Quarterly*, 31(1): 35-58.

Inan, F. A., Namin, A. S., Pogrund, R. L., Jones, K. S., 2016. Internet use and cybersecurity concerns of individuals with visual impairments. *Educational Technology & Society,* 19 (1): 28-40.

Iswaran, S., 2020. MCI's response to PQ on training cybersecurity experts for Singapore. Parliament QAs. Retrieved from https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/10/mciresponse-to-pq-on-training-cybersecurity-experts-for-singapore?page=15.

ITU (International Telecommunication Union)., 2005. ITU internets reports 2005: The Internet of Things. pp. 4-5.

İkizler, M., Başar, S., 2006. Spam'in zararları ve spam ile hukuki mücadele: ABD örneği ve Türk Avrupa Birliği Hukukları ile karşılaştırılması. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *8*(2), 91-114.

İnan F. A., Akbar S. Namin, Rona L. Pogrund., Keith S. Jones., 2016, Use and cybersecurity concerns of individuals with visual impairments, *Journal of Educational Technology & Society* 19(1): 28- 40.

Jensen, T., Hedman, J., Henningsson, S., 2019. How tradeLens delivers business value with blockchain technology. *MISQuarterly Executive,*18(4): 221-243.

Kankanhalli, A., Teo, H.H., Tan, B.C., Wei, K.K., 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2):139-154.

Kaplan, R.S., Norton, D. P., 1992. The balanced-scorcard: Measures that drive performance. *Harvard Business Review,* 71–99.

Kaplan, Ö., Kaplan, A., Mucuk, S., 2023. Gençlerde siber flört istismarının yalnızlıkla ilişkisi. *YOBÜ Sağlık Bilimleri Fakültesi Dergisi*, *4*(2): 150-160.

Kara, İ., 2015. Türkiye'de zararlı yazılımlarla mücadelenin uygulama ve hukuki boyutunun değerlendirilmesi. *Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi*, (52), 87-98.

Karacı, A., Akyüz, H. İ., Bilgici, G., 2017. Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi,* 25(6): 2079-2094.

Karasar, N., 2016. Bilimsel araştırma yöntemi kavramlar teknikler ilkeler. Nobel Akademik Yayıncılık: Ankara.

Kasperskylab., 2018. KSN Report: Ransomware and malicious cryptominers 2016-2018. Retrieved from Kaspersky Business Hub, https://cloud.kaspersky.com.

Kianpour, M, Øverby, H., Kowalski, S.J., Frantz, C., 2019. Social preferences in decision making under cybersecurity risks and uncertainties. *In: International Conference on Human-Computer Interaction.* Cham: 149–63.

Kling, R., 1980. Social analysis of computing: Theoretical perspectives in recent empirical research. *Computing Surveys,*12(1): 61-110.

Knapp, K.J., Marshall, T.E., Rainer, Jr. R.K., Morrow, D.W., 2006. The top information security issues facing organizations: What can government do to help? *Information Systems Security,* 15(4):51-68.

Knowles, W., Prince, D., Hutchison, D., Disso, JFP, Jones, K. A., 2015. Survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection,* 9:52-80.

Kong, H. K., Kim, T. S., Kim J., 2012. An analysis on effects of information security investments: A BSC perspective. *Journal of Intelligent Manufacturing,* 23(4): 941–953.

Köprülü, M., 2023. Üniversite öğretim elemanlarının kişisel siber güvenlik farkındalık durumlarının belirlenmesi: Yıldız Teknik Üniversitesi örneği, *Yüksek Lisans Tezi,* Gazi Üniversitesi, Ankara.

Kritzinger, E., Smith, E., 2008. Information security management:An information security retrieval and awareness model for industry. *Computer and Security,* 27, 224-231.

Kumari L., Debbarma, S., Shyam, R., 2011. Security problems in campus network and its solutions. *International Journal of Advanced Engineering & Application,* 1(1): 98–101.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45:13-24.

Lindsay, M., Booth, J. M., & Messing, J. T., 2016. Experiences of online harassment among emerging adults: Emotional reactions and the mediating role of fear. *Journal M. Fernet, et al. of Interpersonal Violence,* 31(3): 3174–3195.

Lo, Chi-Chun, Chun-Chieh, Huang., Oy, Ku., 2010. A cooperative intrusion detection system framework for cloud computing networks." Parallel processing workshops (ICPPW), 2010 39th international conference on. IEEE.

Looi, H.C., 2005. E-commerce adoption in brunei darussalam: A quantitative analysis of factors influencing its adoption. *Communications of the Association for Information Systems,* 15(1):3.

McAfee, Inc., 2014. Net Losses: Estimating the global cost of cybercrime: Economic impact of cybercrime II. Santa Clara, CA: Center for Strategic and International Studies. Retrieved from http://www.mcafee.com/tw/resources/reports/rp-economic-impactcybercrime2.pdf.

McCumber, J., 2005. Assessing and managing security risk in IT systems. Washington: CRC Press.

Melville, N. P., Robert, L., Xiao, X., 2023. Putting humans back in the loop: An affordance conceptualization of the 4th industrial revolution. *Information Systems Journal*, *33*(4): 733-757.

MIIT (Ministry of Industry and Information Technology)., 2012. Internet of things "twelfth five-year" development plan. http://www.gov.cn/zwgk/2012-02/14/content_2065999.htm.

Miller, B., Miller, K., Zhang, X., Terwilliger, M. G., 2020. Prevention of phishing attacks: A three-pillared approach. *Issues in Information Systems*, *21*(2).

Mohebbi S, Li X., 2015. Coalitional game theory approach to modeling suppliers' collaboration in supply networks. *International Journal of Production Economics,* 69:333-342.

Morgan, S., 2020. Top 5 Cybersecurity facts, figures, predictions, and statistics for 2020 to 2021. March. 2020. Retrieved from Cybercrime Magazine, https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for -2019-to-2021/.

Nagurney, A., Shukla, S., 2017. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, 260(2):588-600.

Njenga, K., Jordaan, P., 2016. We want to do it our way: The neutralization approach to managing information systems security by small businesses. *African Journal of Information Systems.*8(1):41-63.

Oliveira, T., Martins, M.F., 2011. Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation,* 14(1):110.

Öğün, M. N., Kaya, A., 2013. Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri Dergisi,* 18, 145-181.

Öztürk, M.S., 2018. Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi,* 208-232.

Pandey, R. K., Misra, M., 2016. Cyber security threats—Smart grid infrastructure. In 2016 National power systems conference (NPSC) (pp. 1-6). IEEE.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers and Security,

Pearson, N. A., 2014. Larger problem: financial and reputational risks. *Computer Fraud & Security,* 4:11–3.

Peltier, T. R., 2005. Implementing an information security awareness program. *Information Systems Security,* 14(2): 37-49.

Penmetsa, M. K., 2010. A methodology for measuring information security maturity in Norwegian and Indian MSME's with special focus on people factor. *Master's Thesis,* Gjovik University, College Department of Computer Science and Media Technology, Hogskolen.

Powell, W. W., 1987. Explaining technological change. *The American Journal of Sociology,* 93(1):185-197.

Puhakainen, P., Siponen, M., 2010. Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *MIS Quarterly,* 34(4):757–78.

Pye, K., 2016. Teaching cybersecurity in K-12 schools (Order No. 10155676). Available from ProQuest Dissertations ve Theses Global. (1836799123). Retrieved from https://www.proquest.com/dissertations-theses/teaching-cybersecurity-k-12-schools/docview/1836799123/se-2?accountid=8319.

Quayyum, F., Cruzes, D. S., Jaccheri, L., 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343.

Quigley, K., Burns, C., Stallard, K., 2015. Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection. *Government Information Quarterly*, 32(2): 108-117.

Rajendran, S. D., Wahab, S. N., Yeap, S. P., 2020. Design of a smart safety vest incorporated with metal detector kits forenhanced personal protection. *Safety and Health at Work,* 11(4): 537-542.

Ravichandran, T., Rai, A., 2000. Quality Management in Systems Development: An Organizational System Perspective. *MIS Quarterly*, 24(3):381-415.

Rezgui, Y., Marks, A., 2008. Information security awareness in higher education: An exploratory study. *Computer and Security,* 27, 241-253.

Rhee, H.S., Kim C, Ryu., 2009. YU. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security,* 28(8):816–826.

Rogers, R.W., 1983. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychophysiology: A sourcebook 153–76.

Rojas-Solís JL., Guzmán-Toledo RM., Sarquiz-Garcia GC., GarcíaRamírez FD., Hernández-Cruz S., 2021. Ciber-violencia en parejas de jóvenes universitarios durante la pandemia por Covıd-19 (Cyber dating violence in college students during pandemic due Covıd-19). *Eureka 2021,* 18(2):227-243.

Rombach, R., Blattmann, A., Lorenz, D., Esser, P., Ommer, B., 2022. High-resolution image synthesis with latent diffusionmodels. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 10684–10695

Romkey, J., 2017. Toast of the IoT: the 1990 interop internet toaster. IEEE Consum. Electron. Mag. 6 (1), 116–119.

Ruivo, P,, Oliveira, T., Neto, M., 2014. Examine ERP post-implementation stages of use and value: Empirical evidence from portuguese SMEs. *International Journal of Accounting Information Systems,* 15(2):166-84.

Saffo, P., 1997. Sensors: the next wave of innovation. Commun. ACM 40(2):92–97.

Salur, M.U., 2018. Bulut Bilişimde Güvenlik, Çevrimiçi,: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ab.org.tr/ab16/bildiri/131.pdf

Saprikin, O.S., 2021. Models and methods for diagnosing Zero-Day threats in cyberspace. Current information technology bulletin 4.2: 155-167.

Sayar, T. E., 2022. Türkiye'de dijital oyun sektörü ve okuryazarlık faaliyetlerine ilişkin bir değerlendirme. *Medya Okuryazarlığı Araştırmaları Dergisi,*1(1): 41-50.

Schwabe, H., Castellacci, F., 2020. Automation, workers' skills and job satisfaction. *PLoS One,*15(11), e0242929.

Selwyn, N., 2015. Data entry: Towards the critical study of digital data and education. *Learning, Media and Technology*, *40*(1), 64-82.

Semerci, A., 2019. Nomophobia as the predictor of secondary school students' smartphone addiction. *Bartın University Journal of Faculty of Education*, *8*(3): 947-965.

Smith, S., Winchester, D., Bunker, D., Jamieson, R., 2010. Circuits of power: A Study of mandated compliance to an information systems ecurity" De Jure" Standard in a Government Organization. *MIS Quarterly*, 34(3):463–486.

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security,* 22(1):42-75.

Stonard, KE., Bowen, E., Lawrence TR., 2014. Price SA. The relevance of technology to the nature, prevalence and impact of adolescent dating violence and abuse: A research synthesis. *Aggression and Violent Behavior,* 9:390-417.

TDK., 2022, Türk Dil Kurumu Sözlüğü.

Tekerek, M., Tekerek, A., 2013. Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education,* 2(3), 61-70.

Ten C.W., Manimaran G., Liu C.C., 2010. Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans 40(4):853-865.

Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Patsourakos, K., 2018. Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice,* 1:5.

Tirumala, S. S., Sathu, H., Naidu, V., 2015. Analysis and prevention of account hijacking based incidents in cloud environment. In *2015 International Conference on Information Technology (ICIT)* (pp. 124-129). IEEE.

Tirumala, S. S., Valluri, M. R., Babu, G. A., 2019. A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., Lepri, B., 2018. The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys (CSUR)*, *51*(2): 1-27.

Tokmak, M., 2023. Öğrencilerin siber güvenlik farkındalık düzeylerinin makine öğrenmesi yöntemleri ile belirlenmesi. *Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *28*(2): 451-466.

Tsou, HT., Hsu, SHY., 2015. Performance effects of technology–organization–environment openness, service co-production, and digital-resource readiness: The Case of the IT Industry. *International Journal of Information Management,* 35(1):1–14.

Tuğal, İ., Almaz, C., Sevi, M., 2021. Üniversitelerdeki siber güvenlik sorunları ve farkındalık eğitimleri. *Bilişim Teknolojileri Dergisi*, *14*(3): 229-238.

Turgut, Z., 2009. Ağ güvenliğinde solucan yayılımlarının incelenmesi ve yeni model yaklaşımları, Yüksek Lisans *Tezi,* Kocaeli Üniversitesi, Kocaeli.

TÜİK., 2020. Hane halkı bilişim teknolojileri (BT) kullanım araştırması. https://data.tuik.gov.tr/Bulten/Index?p=HanehalkiBilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679

TÜİK., 2023. Hane halkı bilişim teknolojileri (BT) kullanım araştırması. https://data.tuik.gov.tr/Bulten/Index?p=HanehalkiBilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2022-45587

Ünal, C., Sezer, C., 2023. Sağlık hizmetlerinde bilgi mahremiyeti endişesi ve korunma davranışlarını etkileyen faktörler. *Gümüşhane Üniversitesi Sağlık Bilimleri Dergisi,* 12(4): 1498-1517.

Ünsal, N. Ö., 2022. Harmanlanmış siber güvenlik eğitiminin kolluk kuvvetlerinin motivasyonuna ve algısına etkisi. *Doktora Tezi,* Gazi Üniversitesi, Ankara.

Ünver, M., 2012. Ulusal siber güvenliğin sağlanmasında farkındalık çalışmaları. *Mimar Mühendisler Dergisi,* (60), 1-8.

Varkan Kavas, Z., Özbudak, S., Çetkin, E., 2022. Öğretmenlerin siber güvenliklerinin incelenmesi. *International Social Sciences Studies Journal,* 8,106; 4505-4510.

Veiga, A. D., 2008. Cultivating and assessing information security culture. *Doctoral dissertation,* University of Pretoria, Faculty of Engineering, Built Environment and Information Technology, Pretoria.

Wall, J.D., Lowry, P.B., Barlow, J.B., 2016. Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems,* 17(1):39-76.

Wixom, B.H., Watson, H. J., 2001. An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly,* 25(1):17-41.

Xue, B., Xu, F., Luo, X., Warkentin, M., 2021. Ethical leadership and employee information security policy (ISP) violation: exploring dual-mediation paths. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 5-23.

Yalın, B. E., Başfırıncı, Ç. Ş., 2018. Cybersecurity perceptions of university students in Turkey. *Karadeniz Teknik Üniversitesi İletişim Araştırmaları Dergisi*, *8*(2): 2-14.

Yavanoğlu, U., Sağıroğlu, Ş., Çolak, İ., 2012. Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi,* 15(1): 15-27.

Yılmaz, F., 2023. Ortaokul öğrencilerinin siber güvenlik farkındalıklarının belirlenmesi. *Yüksek Lisans Tezi*, Amasya Üniversitesi, Amasya.

Yılmaz, M.Y.B., 2022. Son kullanıcılarda siber güvenlik farkındalığı. *Yüksek Lisans Tezi*, Sivas Cumhuriyet Üniversitesi, Sivas.

Yılmaz, S. ,Sağıroğlu, Ş., 2013. Siber güvenlik risk analizi, tehdit ve hazırlık seviyeleri, 6. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, 20-21.

Yılmaz, V., Sağıroğlu, Ş., 2008. Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2): 507-522.

Yiğit, M. F., Seferoğlu, S. S., 2019. Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, *15*(1): 186-215.

Zeytin, M., Akkaş, H., 2023. Siber güvenlik farkındalığının satın alma niyetine etkisi: Kuşak farklılığı ve kültürel değerler açısından incelenmesi. *Pazarlama & Pazarlama Araştırmaları Derneği*, *16*(3): p759.

Zhu, K., Kraemer, K.L., Dedrick, J., 2004. Information technology payoff in e-business environments: An international perspective on value creation of e-business in the financial services industry. *Journal of Management Information Systems,* 21(1):17-54.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H. N. 2022. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1): 82-97.

EK

‘’Siber Güvenlik Farkındalıklarının Belirlenmesi” adlı tez çalışmasına ilişkin hazırlanmıştır. Cevaplarda bireylerle ilgili bilgiler kesinlikle gizli tutulacak olup, elde edilecek sonuçlar sadece akademik amaçlı kullanılacaktır. İlginiz için teşekkürlerimi sunar, çalışmalarınızda başarılar dilerim. Saygılarımla

Fatma ÇAKAN

1. Cinsiyetiniz : Kadın ( ) Erkek ( )

2. Yaşınız : 18-25( ) 26-33( ) 34 ve üzeri ( )

3. Okuduğunuz bölüm:

4. Sınıfınız: 1( ) 2( ) 3 ( ) 4()

5. Günlük İnternet Kullanımınız kaç saattir?

1 Saatten Az ( ) 1-3 Saat Arası ( ) 3-5 Saat Arası ( ) 5 Saatten Fazla( )

6. Hiç siber saldırıya maruz kaldınız mı? Evet ( ) Hayır ( ) Fikrim Yok ( )

7. Ailenizde veya yakın çevrenizde siber saldırıya maruz kalan kişiler var mı?

Evet ( ) Hayır ( ) Fikrim Yok ( )

8. Kişisel siber güvenliğinizi sağlayabilecek bilgi ve becerilere sahip olduğunuzu düşünüyor musunuz? Evet ( ) Hayır ( ) Fikrim Yok ( )

		Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Şifre Güvenliği	1.Şifre oluştururken özel karakterler, rakam ve harf kullanılması gerektiğini bilirim.					
	2.Parolamı en az 8 karakterden oluşması gerektiğini bilirim.					
	3 Kişisel bilgilerimin yer aldığı şifre oluşturmakta sakınca görmüyorum. (T)					
	4 Şifremi kimseyle paylaşmam.					
	5 Şifrelerimi sıklıkla değiştiririm.					
	6 İki faktörlü kimlik doğrulamanın ne olduğunu bilirim.					
	7. Herhangi bir işlem yapmadığım halde e-postama gelen parola sıfırlama iletilerini dikkate almam.					
Önleyici Tedbirler	8 Gelen e-postalarda isim ve e-posta adresini kontrol ederim.					
	9.Tanımadığım kişilerden gelen e-postada samimi ifadeler varsa (sevgili beyefendi/ hanımefendi vb.) dikkatli olmam gerektiğini bilirim.					
	10 Bir e-postadaki veya sosyal medya gönderisindeki bağlantılara					

	tıklama konusunda dikkat ederim.					
	11 Bir e-posta ekini açmadan önce, ekteki dosya adının anlamlı olup olmadığını kontrol ederim.					
	12 Acil, önemli başlığıyla gelen e-postalara şüpheyle yaklaşırım.					
	13 Bağlantının güvenli olduğunu teyit etmek amacıyla bağlantı adresinin https:// olup olmadığını kontrol ederim.					
	14 Bir e-postayı okumadan önce e posta konusunun anlamlı ve gönderenin gerçek bir kişi olup olmadığına bakarım.					
Kötü Amaçlı Yazılım Farkındalığı	15 Cihazlarımda gerekli yazılım güncellemelerini yaparım.					
	16 Solucan ve virüsün farkını bilirim.					
	17 Kötü amaçlı yazılım kullanılarak uzaktan bağlantı ile bilgisayarımın ele geçirilebileceğini düşünürüm.					
	18 Bilgisayarıma saldırı olabilecek kötü amaçlı yazılım türlerinin farkındayım.					
	19 Kötü amaçlı yazılımların internete erişmeme engel olabileceğini düşünürüm.					
	20. Cihazımın/cihazlarımın verilerinin yedek kopyalarını oluştururum.					
Kişisel Gizliliği Koruma	21 Sosyal medyada adıma hesap açılmasının kimlik hırsızlığı olduğunu bilirim.					
	22 Tanıdığım kişiden gelen e-postada kişisel bilgilerim istenirse paylaşırım. (T)					
	23 E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.					
	24.Sosyal medya servislerinde kişisel bilgilerimi koruyan özellikler olduğunu bilirim.					
	25. Kimlik avının ne olduğunu bilirim.					

* (T): Ters maddeleri belirtmektedir.