T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yüksek Lisans Tezi

ÇALIŞANLARIN SİBER GÜVENLİK FARKINDALIKLARININ ARAŞTIRILMASI

Serdar MASUM

Enformatik Anabilim Dalı

Enformatik Programı

DANIŞMAN
Doç. Dr. Hulusi GÜLSEÇEN

II. DANIŞMAN
Doç. Dr. Muhammed Ali AYDIN

Haziran, 2022

İSTANBUL

Bu çalışma, 16.06.2022 tarihinde aşağıdaki jüri tarafından Enformatik Anabilim Dalı, Enformatik Programında Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Doç. Dr. Hulusi GÜLSEÇEN(Danışman)
İstanbul Üniversitesi
Fen Fakültesi

Doç. Dr. Çiğdem EROL
İstanbul Üniversitesi
Enformatik Bölümü

Dr. Öğr. Üyesi Özgür Can TURNA
İstanbul Cerrahpaşa Üniversitesi
Mühendislik Fakültesi

İntihal Programı Beyanı

20.04.2016 tarihli Resmî Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

Proje Destekleri

[ ]

Tezden Üretilmiş Yayınların Künye Bilgileri

[ ]

ÖNSÖZ

Tez çalışması sürecinde tecrübesi ve bilgisi ile bana yol gösteren, sabır ve desteğini hiç eksik etmeyen çok değerli danışman hocalarım Doç. Dr. Hulusi GÜLSEÇEN ve Doç. Dr. Muhammed Ali AYDIN' a sonsuz teşekkürlerimi sunarım.

Annem Şefika MASUM, babam Sürmeli MASUM sevgileri, üzerimdeki emekleri ve destekleri için teşekkür ederim.

Haziran 2022 Serdar MASUM

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Simgeler **Açıklama**

x^2 : Ki Kare Dağılımı

p : Olasılık Değeri

Kısaltmalar **Açıklama**

TDK **:** Türk Dil Kurumu
NATO **:** North Atlantic Treaty Organization
CL **:** Supervisory Control and Data Acquisition Systems
URL **:** Uniform Resource Locator
UDHB **:** Ulaştırma Denizcilik ve Haberleşme Bakanlığı
SOME **:** Siber Olaylara Müdahale Ekipleri

ÖZET

ÇALIŞANLARIN SİBER GÜVENLİK FARKINDALIKLARININ ARAŞTIRILMASI

YÜKSEK LİSANS TEZİ

Serdar MASUM

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Enformatik Anabilim Dalı

Danışman : Doç. Dr. Hulusi GÜLSEÇEN

II. Danışman: Doç. Dr. Muhammed Ali AYDIN

Bu araştırmanın amacı, çalışanların siber güvenlik farkındalıklarının incelenmesi ve sonuçların değerlendirmesidir. Bu amaç doğrultusunda çalışanların demografik özellikleri ile kişisel siber güvenlik sağlama durumları arasındaki ilişki analiz edilmiştir. Araştırmanın örneklemini Türkiye'de çalışmakta olan bireylerden oluşmaktadır. Örneklem ise, rastgele seçilen **457** erkek ve **413** kadın olmak üzere **870** çalışandan oluşturmaktadır. Çalışmada kullanılan anket, internet anketi türünde olup Google Forms kullanılarak hazırlanmış, katılımcılara elektronik ortamda ulaştırılmıştır ve internet ortamında yanıtlanmıştır. Araştırmada bağımsızlık için ki-kare testi veya χ^2 testi kullanılmıştır. Araştırma sonucunda erkek çalışanların kişisel siber güvenlik farkındalıklarının kadın çalışanlardan daha fazla olduğu görülmüştür. Bankacılık işlemleriyle kişilerin mali varlılarını başkalarının eline geçme konusunda tedirgin olmaları nedeniyle tüm

yaş grupların dikkatli oldukları anlaşılmıştır. Çalışanların her eğitim seviyesinde siber eğitim açığının olduğu görülmektedir.

Haziran 2022, 95 sayfa.

Anahtar kelimeler: Siber Güvenlik, Çalışanlar, Siber Saldırı, Farkındalık

SUMMARY

THESIS TITLE

M.Sc. THESIS

RESEARCHİNG EMPLOYEE'S CYBER SECURİTY AWARENESS

İstanbul University

Institute of Graduate Studies in Sciences

Department of Informatics

Supervisor : Assist. Prof. Dr. Hulusi GÜLSEÇEN

Co-Supervisor : Assist. Prof. Dr. Muhammed Ali AYDIN

The purpose of this research is to examine the cyber security awareness of employees and evaluate the results. For this purpose, the relationship between the demographic characteristics of the employees and their personal cyber security Deciency has been analyzed.The sample of the research consists of individuals working in Turkey. The sample consists of 870 randomly selected employees, 457 male and 413 female. The questionnaire used in the study is of the type of internet questionnaire, prepared using Google Forms, delivered to the participants electronically and answered on the internet. Chi-square test or χ^2 test was used for independence in the research. As a result of the research, it has been seen that male employees have more personal cyber security awareness than female employees. It has been understood that all age groups are cautious because people are uneasy about getting their financial assets into the hands

of others through banking transactions. It is seen that there is a cyber training gap at every education level of the employees.

June 2022, 95 pages.

Keywords: Cyber Security, Employees, Cyber Attack, Awareness

1. GİRİŞ

Teknolojinin çok hızlı bir şekilde ilerlemesi sebebiyle bu gelişimin çıktıya dönüşmesi de aynı derecede hızlı gerçekleşmektedir. Böylece dijital sistemler ifadesi yaşamımızın en güncel konusu durumundadır. Teknolojinin faydalı taraflarını kullanmak eğlenceli, hayatı kolaylaştırıcı ve düzenleyicidir. Ancak hem devlet hem şirket hem de kişisel olarak kullanılan sistemlerin siber uzayda yer aldığını hatırlamak gerekir. Çünkü siber uzay sandığımız derecede güvenli bir alan değildir ve iyi olmayan taraflarından ve tehlikelerinden korunmak lazımdır. Teknolojideki ilerlemeler ve internet kullanan aygıt adedindeki yükselişin bir aksi olarak yaşamımıza dahil olan dijitalleşme ifadesi çok hızlı bir sürede kabul almıştır. Sadece kişisel değil, devletler, kurumlar ve hem de her türlü global şirketlerin hepsi dijital dönüşüm halindedirler. Dijital sistemlere yapılan siber saldırıların adetleri ve sonuçları her geçen gün çoğalmaktadır.

Dijitalleşme, devlet ile kuruluşları güncel alanlara ve yeni dijital teknolojilerle altyapıyı modernize etmeye yönlendirmektedir. Dijital sistem bağlılığı gün be gün arttıkça bireyler, organizasyonlar ve sistemler de siber tehlikelere aynı oranda hassaslaşmaktadır. Güvenlik aygıtları ve bunların yetenekleri arttıkça siber korsanlar da buna paralel olarak organize ve karmaşık duruma gelmektedirler. İyi niyetli olmayan aygıtlara rahat bir şekilde erişim sağlamak, çoğalan riskin sebeplerinden birisidir. Organizasyonlar, siber riskin nasıl üstesinden geleceklerini ve bu siber tehditlerin sistemlerini ve süreçlerini ne türlü değiştirebileceğini kavramalıdırlar.

Kişisel veya sektörde yer alan diğer şirketlerde kullanılan sistemler ayırt edilmeksizin, internete erişimi bulunan veya bulunmayan tüm aygıtlar siber saldırıların ve iyi niyetli olmayan yazılımların odağındadırlar. Bilhassa bu siber saldırıların yaşamımızın sürdürülmesi için çok önemli olan su, elektrik, finans, sağlık, iletişim gibi alanlarda olduğu varsayılırsa, neticesi toplum için yıkıcı etkilere, can ve mal zayiatına ve çeşitli tahribatlara sebep oluşturabilecektir.

Kuruluşlar açısından bakılırsa, iş sürekliliği en mühim noktadır. İyi niyetli olmayan uygulamaların ve siber atakların firma içine sızması, iş ortaklarının yitirilmesine, somut ve soyut hasarlara ve ileride üretimin durmasına sebep olabilmekte ve bu da önemli krizlere yol açabilmektedir. Bireysel bakış açısıyla yaklaşılacak olursak en sade şekilde tüm kişisel verilerimizin, banka hesap bilgilerimizin bulunduğu mobil cihazlar kişiler için çok kıymetlidir.

Buna ek olarak bilgisayarların kameralarına izinsiz erişim sağlanarak kişilerin takip edilmesi, izinsiz ses kaydı alınması gibi haller değerlendirildiğinde kişisel bir şekilde de siber güvenlik kavramının bilincinde olmamız gerekmektedir. Nihayetinde siber ve siber güvenliği iyi algılamaya, geçmişteki siber vakalardan ders çıkarmaya, bu kavramlara ilişkin bilinç oluşturmaya, bu hususlardaki incelemeleri değerlendirmeye, stratejileri oluşturmaya ve gerekli iş ve işlemleri gerçekleştirmeye ihtiyaç vardır.

Günümüzde kullanılmakta olan sistemlerin pek çoğu teknolojiden faydalanarak hizmetini sürdürmektedir. İnternet kullanan aygıtların her geçen gün artması ile birlikte dijital dönüşüm gerçekleşmekte ve bu da yaşamımızın bir parçası haline gelmektedir. Yaşadığımız bu dijital süreçlerin pek çok faydasının olduğu yadsınamaz. Ancak, bu süreçler maalesef ki göründüğü kadar iyi olmayabilir. Bilhassa internetin yaygınlaşmasına paralel olarak tehditler de o oranda artış göstermektedir. Kötü amaçlı yazılımlar, fidye, oltalama ve siber tehdit gibi kavramlar ortaya çıkmaktadır.

Her geçen gün teknoloji kullanımı artış göstermektedir. Bunlardan hangisini seçersek seçelim hepsinin de bir güvenlik durumu bulunmaktadır. Bireysel veya kurumsal olarak her kullanıcının güvenliğe ilişkin bir mesuliyeti vardır. Teknolojiden yararlanacak kişiler bunu güvenli bir biçimde yapmaya çalışırken, kurumlar da bunu güvenli bir biçimde sağlamaya çalışmaktadırlar. Kurumlar için hem finansal hem de kişilerin hayatına ilişkin pek çok konuda kötü sonuçlar ile karşılaşmamak adına güvenlik temelini oluşturmak ayrı bir ehemmiyete sahiptir. Çağımızda en kıymetli varlığımız olan bilgi, duyarlılık gösterilmesi gereken en kritik konudur. Bununla birlikte küçük ya da büyük her türlü bilginin muhafaza edilmesi gerekliliği doğmuştur. Bilgi Güvenliği kavramı da bundan dolayı değer kazanmıştır. Bilgi Güvenliliğinin temel yapı taşları ise bütünlük, gizlilik ve erişilebilirliktir.

Kötü amaçlı siber saldırılar ve bunların sonucu olarak oluşabilecek olumsuz durumlar, bireysel, kurumsal ve toplumsal olarak tüm kullanıcıların güvenlik yatırımları ve yönetim desteğini yoğunlaştırmasını gerektirmektedir. Fakat belirli bir plan ve program olmadan yapılan güvenlik yatırımları faydalı olmamaktadır.

Hızla büyüyen bilgi teknoloji sistemleri incelendiğinde değerinin hızlı artış kazandığı ortaya çıkmaktadır. Bu sistemlerin kendi içindeki ilişkisi arttıkça çalışma ve kamu hayatında muhtelif saldırılarla karşı karşıya kalınmaktadır. Bilginin yazılı, elektronik vb. pek çok ortamda yer alması, veri paylaşımının artması ve çeşitli pek çok usulle gerçekleştirilmesi saldırıların yöntem ve farklılığının da çoğalmasına neden olmaktadır. Verilerin paylaşılması ve devamlı olarak ulaşılabilmesi sebebi ile göndericiden alıcıya güvenli bir şekilde, değişmeden, kaybolmadan ve tam bir şekilde aktarılması bilgi güvenliğinin gerekliliği için başlıca ölçütlerdir.

Bu tezde istatistiksel analiz platformlarından biri olan SPSS ile çalışanların siber güvenlik farkındalıklarının analizi gerçekleştirilmiştir. Analiz aracı olarak SPSS programı seçilmenin sebebi başta anket analizleri olmak üzere sağlık bilimleri ve fen bilimleri alanlarında da elde edilen bazı ölçümlerin analiz etmesidir.

Bu tez çalışmasının GENEL KISIMLAR ana başlığı altında bilgi, bilgi ilgili kavramlar, bilgi güvenliği, bilgi güvenliğinin tarihsel gelişimi, bilgi güvenliği temel unsurları, siber, siber güvenlik, siber saldırı çeşitleri, hackerlar, Türkiye'de siber güvenlik durum analizi, siber güvenlik ilgili yapılan çalışmalar, kurumsal siber güvenlik, kurumsal siber güvenliğe yönelik tehdit ve önlemleri ile ilgili kavramlar yer verilmiş seçilen teknoloji olarak SPSS programın tanıtılmış ve literatürde SPSS ile yapılmış siber güvenlik çalışmaları incelenmiştir.

MALZEME ve YÖNTEM bölümünde tez çalışmasında kullanılan anket, internet anketi türünde olup Google Forms kullanılarak hazırlanmış, katılımcılara elektronik ortamda ulaştırılmıştır ve internet ortamında yanıtlanmıştır. Araştırmada anket maddelerinin katılımcılar tarafından doğru bir şekilde okunup anlaşıldığı, dürüst ve gerçeği tam yansıtacak şekilde yanıtlandığı varsayımından hareket edilmiştir. Anket sorularının detaylarına, kullanılan programlama araçlarına, anket sonuçlarını üzerinde yapılan işlemlere ve çalışmayı gerçekleştirmek uygulanan yöntemlere yer verilmiştir. Araştırmada bağımsızlık için ki-kare testi veya χ^2 testi kullanılmıştır.

BULGULAR çalışanların siber güvenlik farkındalığının, cinsiyet, yaş, gelir ve eğitim durumuna göre farklılaşıp farklılaşmadığı madde madde ki-kare testi veya χ^2 testi ile belirlenmiştir.

TARTIŞMA ve SONUÇ bölümünde tez çalışmasının diğer çalışmalardan farkı, bulguların yorumları, elde edilen sonuçların literatüre katkısı, gelecek çalışmaların neler olabileceği konularına yer verilmiştir.

2. GENEL KISIMLAR

Bu bölümde, bilgi, bilgi ilgili kavramlar, bilgi güvenliği, bilgi güvenliğinin tarihsel gelişimi, bilgi güvenliği temel unsurları, siber, siber güvenlik, siber saldırı çeşitleri, hackerlar, Türkiye'de siber güvenlik durum analizi, siber güvenlik ilgili yapılan çalışmalar, kurumsal siber güvenlik, kurumsal siber güvenliğe yönelik tehdit ve önlemleri ile ilgili kavramlar ele alınmıştır.

2.1.BİLGİ KAVRAMI

Toplumu ve toplumu meydana getiren bireyleri geliştiren ve dönüşüme uğratan bilgi kavramı günümüzde çok önemli bir yere sahiptir. Bilgi kavramı bu önemi ile bilgi toplumu, bilgi güvenliği, siber güvenlik kavramlarına ilişkisi nedeniyle bu kavramları da günümüzde ön plana çıkarmaktadır (Kaya ve Aldemir, 2020).

Bilgi kavramının tek bir tanımı bulunmamaktadır, çünkü bilgi ait olduğu alan ve kültüre göre değişkenlik göstermektedir. Bilgi kavramı her ne kadar değişkenlik gösterse de literatürde "mantıklı bir yargı ya da deneysel sonuç sunan, başkalarına sistemli bir iletişim aracılığıyla ulaştırılan, olgulara ya da düşüncelere ilişkin ifadeler dizisidir" olarak tanımlanmaktadır (Bell, 2013).

Farklı bir açıdan bakıldığında bilgi; bir mesajın iletilmesinde kullanılan, alıcının ve iletişim kanalının bir fonksiyonu olan, hatta kaynağında bir fonksiyonu olarak tanımlanan veri olarak ifade edilmektedir (Orkan, 1992).

Türk Dil Kurumana göre bilgi; insan aklının erebileceği olgu ve ilkelerin tümüne verilen ad olarak tanımlanmakta. Bunun yanı sıra bilgiyi; bir konu ya da iş konusunda öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek olarak da tanımlayabiliriz.

Günümüzde bilgi büyük güç haline gelmiştir. Bulunduğumuz çağda ise bilgi çok büyük bir güç haline gelmiştir. Kurumlar sahip oldukları bilgilerini en iyi şekilde yönetmelidirler ki rekabet edebilsinler, büyüyebilsinler yani çağa ayak uydurabilsinler ve yaşamlarını sürdürebilsinler. Bilgi, işletmelerde rekabet avantajı sağlamak ve bu avantajı sürdürülebilir hale getirmek için

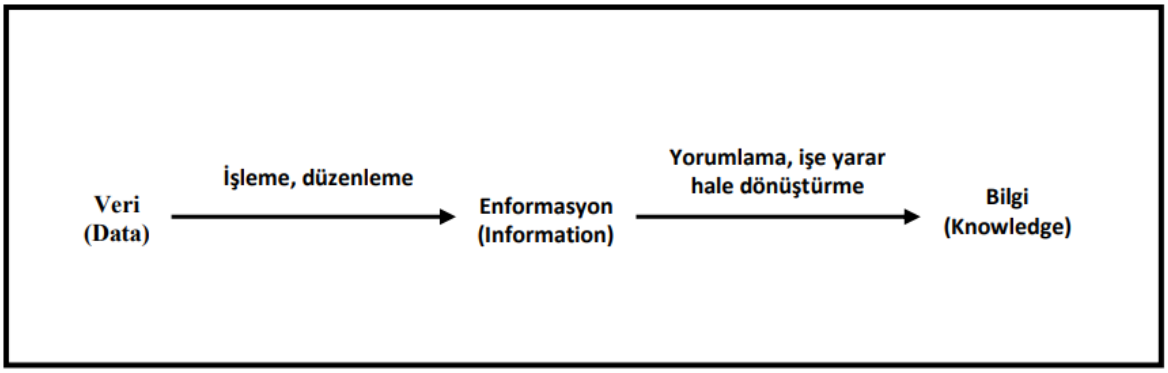
çok önemli bir kaynaktır. Günümüzde yapılan işlerin çoğu, bilgi temelli olmaktadır (Karaca, 2015).

2.1.1.Bilgi İlgili Kavramlar

Bilgi ile ilişkili olan veri kavramını açıklayacak olursak; veri bilgiyi oluşturmak için toparlanmış değerler bütünüdür. Bu açıdan bakılarsa veri; bir olguya ait, ağırlık, hacim, uzunluk gibi nicel ve sembol, resim, ses gibi nitel özellikler bütünüdür (Kitchin, 2014).

Ham verilerin anlamlı bir değere dönüştürülmesi ile bilgi elde edilir. Veriler belli bir amaç doğrultusunda bir araya getirilerek enformasyon oluşturulur. Veriler kısacası enformasyona dönüşecek basit bir olgudur ve veriler enformasyon ile beraber çalışıldığında bilgiye ulaşılacaktır.

Bilgi ve veri ile arasındaki ilişki kısaca açıklamak gerekirse; bilgi zihinsel değerlendirme, kurgulama, tahmin etme gibi değerlendirmeler sonucunda işlenmiş bir veri olan enformasyon kullanılabilir enformasyon olarak karşımıza çıkmaktadır (Kaya ve Aldemir, 2020).



Şekil 2. 1: Bilginin Oluşum Süreci (Güçlü ve Sotirofski, 2006).

2.2.BİLGİ GÜVENLİĞİ

Günümüzde veri ve bilgi kavramları öneminin artması ile bilgi güvenliği kavramı da aynı oranda önem kazanmıştır. Çünkü bilginin toplanması ve bu bilginin saklanması gerektiği gibi güvenliğinin de sağlanması gerekmektedir.

Toplanan bilgi ve veriler arttıkça bu bilgilerin güvenliği için verilen önemde artmaktadır. Günümüzde iletişim artık büyük oranda teknolojik alt yapılar ile sağlanmaktadır. İletişim için bu teknolojik alt yapı kanallarının kullanımı arttıkça kişisel verilerin bu kanallarda birikimi artmaktadır. Kısacası ne kadar çok teknolojik alt yapı kullanımı o kadar büyük veri boyutu saklanması demektir. Hızla ilerleyen bu süreçler hem kişisel ve hem de kurumsal olarak bilgi güvenliğinin önemini artırmaktadır (Alemdaroğlu, 2020).

2.3.BİLGİ GÜVENLİĞİNİN TARİHSEL GELİŞİMİ

Bilgi güvenliği sadece günümüzde değil geçmişte de önemli bir yere sahiptir. Birebir bilgi güvenliği olarak adlandırılmasa da geçmişte devletleri yönetenlerin aldığı tedbirler bilginin güvenliğine değer verildiğini göstermektedir.

Bu tedbirlere örnek olarak padişahların diğer devletlere gönderdiği mektupların ağzının mühürlemesi gösterilebilir. Bu yöntem ile mesajların aktarımı sırasında bilginin gizliliğinin ihlal edilmesi önlenmiştir (Alemdaroğlu, 2020).

Roma dönemine bakıldığında dönemin askeri komutanı olan Jül Sezar'ın kullandığı şifreleme yöntemi diğer kişiler tarafından deşifre edilememiş ve günümüze "Sezar şifreleme yöntemi" olarak gelmiştir.

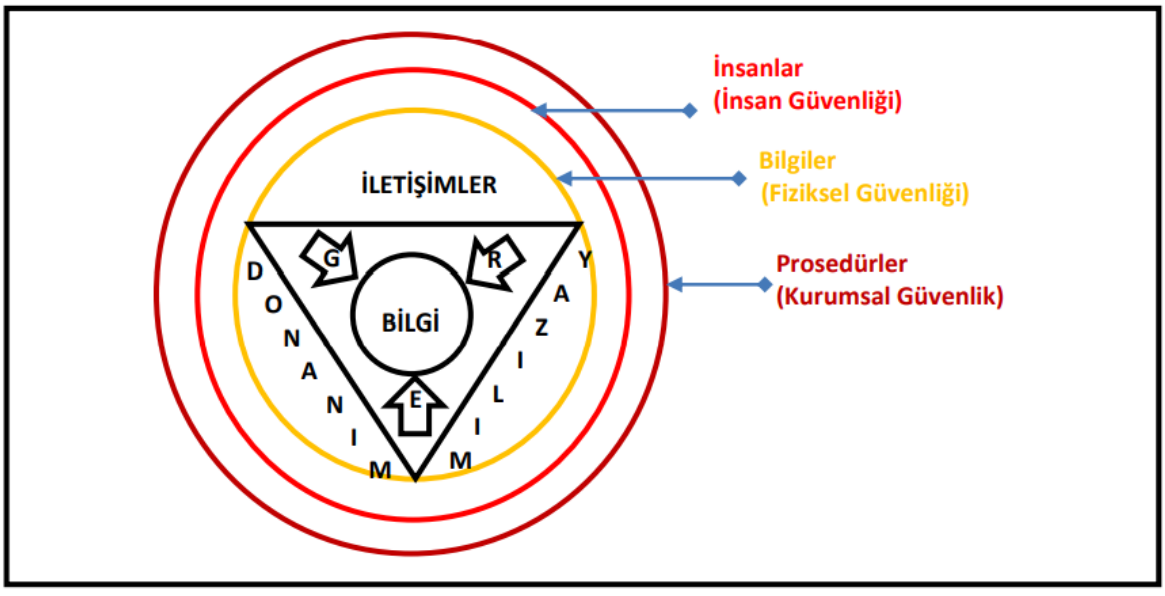
Eski Mısır döneminde ise özel alfabeler kullanılarak yazışmalar yapılmış böylelikle diğer kişilerin bu yazışmaları anlaması engellenmiştir. Bu özel alfabeler 19. Yüzyılda Fransız Jean-François Champollion tarafından çözümlenebilmiştir. Geçmişten verilen bu yöntemler aslında bilgi güvenliğininim sadece günümüzde değil geçmişte de büyük bir öneme sahip olduğunu göstermektedir. Günümüzle karşılaştırıldığında belki ilkel olarak gözükse de bu yöntemler ancak günümüz şartlarıyla karşılaştırıldığında önemli sonuçları olduğu görülmektedir (Güngör, 2015).

2.4.BİLGİ GÜVENLİĞİNİN TEMEL UNSURLARI

Bilgi güvenliği kavramı "verinin kendisi için oluşabilecek zararlardan uzakta tutulması, bilginin uygun teknoloji kullanılarak tüm alanlarda istenmeyen kişilerce ele geçirilmesinin önlenmesi" olarak tanımlanmaktadır (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliği daha ayrıntılı olarak şu şekilde de açıklanabilir; bilginin göndericiden alıcıya ulaşma aşamasında farklılaşmaması, diğer kişiler tarafından ele geçirilmemesi, zarar görmeden gizliliğini koruması bilgi güvenliği olarak ifade edilir. Bilgi güvenliğinin için üç temel öğe bulunmaktadır. Bu üç öğe şu şekilde sıralanabilir; gizlilik, bütünlük ve erişilebilirlik.

Bu üç temel öğeye ek olarak giriş denetimi, güvenlik, güven duyulması, inkâr edememe, kayıt altına alma, kimlik tespiti gibi kurullarda bilgi güvenliğinin ileri düzeyde kurulmasına sağlamaktadır (Sharp, 2004).



Şekil 2. 2: Gizlilik, Bütünlük, Erişilebilirlik Üçlü Nitelikleri (Ganbat, 2013).

2.4.1.Gizlilik

Bilginin sanal mecralarda aktarılırken yetkisiz kişiler ya da süreçler tarafından elde edilse bile yeterli bir biçimde anlamlandırılamaması gizlilik olarak ifade edilmektedir. Statik mecralardaki ya da ağ üstünden iletilen aktif mecralardaki veriler için gizliliğin sağlanması mecburidir.

Gizlilik olgusunda: yetkisiz kişiler tarafından kötü niyetli olarak veriler elde edilse bile bu verilerin kavranması ve çözümlenmesinin engelleyecek yöntemler ile bilginin anlaşılmamasının sağlanması amaçlanmaktadır. Şifreleme prosedürleri ve steganografi yollarından yararlanarak gizlilik kuralının devamlılığı sağlanır (Yerlikaya, 2019).

2.4.2.Bütünlük

Bilginin göndericiden iletilene kadar ulaşımı aşamasında zarar görmeden bir bütünlüğünü korumasını sağlayan güvenlik öğesi bütünlük ilkesidir. Bütünlük ilkesindeki amaç; iletişim sırasında bilginin iletilene ulaşana kadar değiştirilmemesi, yeni dataların eklenmemesi, belli bir parçasının ya da tümünün yeri değiştirilmemesidir. Özetleme algoritması ile bilginin bütünlüğünün devamlılığı sağlanır.

2.4.3.Erişilebilirlik

İhtiyaç duyulan bilgiye kullananların izni kapsamında zamanında ulaşımın sağlanması için tedbirlerin oluşturulması olarak ifade edilmektedir. İnformatik düzenleri kullanan bireyler veya süreçler için erişilebilirlik çok önemlidir. Çünkü informatik düzenlerden beklenilen görevleri zamanında gerçekleştirmeleri beklenir.

Erişilebilirlik hizmetinin amacı; kurum içinden ya da kurum dışından kaynaklanabilecek erişilebilirliği azaltıcı tehditlere karşı informatik sistemlerini korumaktır. Bu hizmetle verilere zamanında, hızlı bir şekilde güvenilir olarak kullanıcılar tarafından ulaşılabilir. Sistemlerin erişilebilirliğini negatif olarak etkileyen faktörler olarak doğal felaketler, yazılımlardaki uygun olmayan şifrelemeler, bilinçli olmayan çalışanlar sayılabilir. Erişilebilirliğin sağlanması için fiziki tedbirler alınmalı, casus önleyici yazılımlar, virüs önleyici programlar güncel bir şekilde kullanılmalıdır (Yerlikaya, 2019).

2.5.SİBER GÜVENLİK

Bilgisayar ya da ağ kavramlarının tanımı yapılabilmesi için siber ifadesi kullanılır. Sistem, donanım, yazılım gibi soyut ve somut alanı tarif etmek için siber alan kelimesinden yararlanılır.

Şahıs, kurum ya da devlet gibi yapıların bilgi sistemlerine ve önemli altyapılarına planlı olarak gerçekleştirilen saldırılara siber saldırı denilmektedir (Alkan, 2020).

Siber güvenlik terimi ilk olarak 1990larda bilgisayar mühendisleri tarafından kullanılmıştır. Bilgi gizliliği, bütünlüğü, erişilebilirliği siber dünyasının güvenliğini sağlamaktadır (Hansen ve Nissenbaum, 2009).

Siber tehditler sadece bilgisayar sistemlerine zarar olarak görülmemektedir. Siber tehditler artık ülkelerin çok önemli haberleşme ağlarına, enerji ya da ulaşım sistemlerine, askeri komuta sistemlerini bile zarar verecek boyutlarda asimetrik harp çeşidi olarak karşımıza çıkmaktadır. Tüm dünya olarak artık siber tehditler artık çok önemli tehdit olarak kabul etmektedir. Bu nedenle etkili savunma sistemlerinin kurulması ve acil durumlar için hazırlıkların yapılması gerekmektedir (Aytekin, 2015).

Saldırının oluştuğu anda tespit edilmesi, sanal veya fiziksel bariyer oluşturulmalı, bölgesel ve ulusal boyutta siber güvenlik politikalarının geliştirilmesi gerekmektedir. Bunun için siber saldırı farkındalığın yaratılması gerekmektedir (Goodman, 2008).

Günümüzde devletler, siber mecralara yönelik politikalar geliştirmektedirler. Bu politikalar oluşturulurken güvenli bir siber ortam sağlamak amaçlanmaktadır. Bu doğrultuda devletler siber bileşenleri siber saldırılara korumak, saldırı esnasında müdahale etmek, saldırıyı gerçekleştirilenleri cezalandırmak için yasal mevzuatlar düzenlemekte ve alt yapılara oluşturmaktadır (Çifci, 2013).

2016 yılında gerçekleştirilen Varşova Zirvesinde her geçen yıl siber saldırı sayısı arttığı ve bunun için siber savunmaya yönelik kaynak sağlanması gerektiği vurgulanmıştır. NATO'ya üye bir ülkede kritik bir alt yapıya gerçekleşen siber saldırının diğer ülkeleri de etkileyeceği belirtilerek durumun öneminden bahsedilmiştir (NATO, 2017).

Eski dönemlerdeki savaşlarda gerçekleşen füze saldırıları dakikaları alırken günümüzde bir siber saldırı ışık hızında gerçekleşebilmektedir. Teknoloji ne kadar ileri düzeyde olsa bile siber saldırılarının zamanının tahmini çok zordur. Bu nedenle bu tarz siber saldırılara karşı her zaman hazırlıklı olmak gereklidir. Bu hazırlıklar yapılırken siber saldırılara karşı tatbikatlar düzenlenir. Bu tatbikatlarda teoriden gerçeği görmek için gerçek saldırı ve savunma teknikleri kullanılmaktadır (VonKnop, 2008).

2.5.1.Siber Güvenlik ve Neden Önemlidir

Dünya; geçmiş yıllar ile kıyaslandığında teknolojiye daha fazla bağlı hale gelmiş ve bu durum dijital verilerin oluşturulmasında büyük bir artışa yol açmıştır. Oluşturulan veriler, şirketler, devlet kurumları, bireyler vb. tarafından bilgisayarlar aracılığıyla depolanmakta ve bu depolanan veriler günlük periyotlar halinde bir ağ üzerinden diğer bilgisayarlara aktarılmaktadır.

Ancak gerek bilgisayarlar gerekse de bağlı sistemlerde güvenlik açıkları bulunabilmekte, bu durum da bir saldırgan tarafından istismar edilebildiğinden oluşturulan yapının çökmesine sebebiyet vermektedir. Bundan dolayı siber güvenlik büyük ölçüde hayati önem taşımaktadır. 2010 yılının haziran ayında ortaya çıkan bilgisayar solucanının yayılma biçimi ile siyasi olarak kullanış şekli oldukça dikkat çekmiştir. Bahsi geçen bu solucan, Microsoft'un Windows tabanlı işletim sistemi aracılığıyla dağılarak Siemens'in S7 300 modüllerini hedef almıştır. Açılımı 'Supervisory Control and Data Acquisition Systems 'şeklinde olan SCADA yazılımı, Simatic WinCC SCADA kodludur (Başeskioğlu, 2021).

2.5.2.Siber Saldırılar ve Hackerler

1960'lı yıllarda ortaya çıkan ve bugün kullanmakta olduğumuz internetin erişimi belirtilen yıllarda az sayıda bilim adamı, araştırmacı ve savunma departmanı tarafından erişilebilir durumdaydı. O zamanlardaki internet veri yapısı birçok gelişim gösterdi ve siber suçun tanımı, bilgisayar ya da altyapısına fiziksel olarak verilen zarar olarak tanımlanmakta iken 1980'li yıllarda bu tanım bilgisayarın arızalanmasına yol açan bir eylem olarak değiştirildi. Genellikle savunma sanayi, büyük kuruluşlar ve araştırma topluluklarının kullanımı ile sınırlı olması nedeniyle siber suçun etkisi oldukça düşüktü. 1996 yılında halka açık olarak kullanılmaya başlanması ve insan hayatında büyük bir yer alarak popüler olması ile birlikte kullanıcıların işlevlerini ve özelliklerini anlamasını kolaylaştırmak amacıyla internet için grafik kullanıcı ara

yüzü basit bir şekilde tasarlandı. Böylece, kullanıcılar tarafından, arayıcılarındaki köprülere tıklayarak veya tarayıcıya URL'leri yazarak veriye ulaşılmakta ancak, verilere başkaları tarafından erişim sağlanıp sağlanmadığı, ulaştıkları verilerin izlenip izlenmediği ya da bir saldırgan tarafından izinsiz şekilde tahrif edilip edilmediği bilinmemekteydi. İlk başlarda sadece bilgisayara fiziksel olarak zarar verme olarak tanımlanan siber suç, internetteki gelişim ve kullanımdaki artışla verilere müdahale edilmesi sonucunda mali suçlar işlenmesine yönelmiştir (Başeskioğlu, 2021).

İnternet 2013 yılına kadar zirveye ulaşması sonucunda siber suçların oranı hızla artmış ve her saniye yirmi beş bilgisayar saldırıya uğrayarak aynı zamanda 900 milyon kullanıcı da siber suçların kurbanı olmuştur. Herkesin akıllı telefona sahip olmasıyla, kurbanların sayısı büyük ölçüde artmış, telefonlara güvenlik önlemleri alınmaması ve kullanıcı hataları ile birlikte bu durum milyar dolarlara varan saldırılara ve zararlara yol açmıştır (Başeskioğlu, 2021).

2.5.3.Siber Hacker Türleri

2.5.3.1.Siyah Şapkalı Hackerler

En zararlı ve en tehlikeli hackerlerdir. Saldırıları için ortak hackleme uygulamaları kullanırlar.

2.5.3.2.Beyaz Şapkalı Hackerler

En zararsız ve sistemin güvenlik açıklarını tespit edip ilgili personele aktarır. İyi niyetli siber güvenlik uzmanlarıdır.

2.5.3.3.Gri Şapkalı Hackerler

Sistem açıklarını tespit ederler Sisteme izinsiz giriş yaparlar ancak kullanıcılara herhangi bir zarar vermezler.

2.5.3.4.Yeşil Şapkalı Hackerler

Siber dünyada yenidirler. Diğer bilgisayar korsanlarını takip ederek bilgi sahibi olmaya çalışırlar.

2.5.3.5.Red Hat Hackerler

Siyah Şapkalı Hackerların çalışmalarını durdurmaya çalışırlar. Beyaz şapkalı Hackerlerden farkı sistem yöneticisine bildirmek yerine siyah şapka korsanını ortadan kaldırmaya inanırlar.

2.6.TÜRKİYE'DE SİBER GÜVENLİK DURUM ANALİZİ

Ülkemizde siber güvenliğe yönelik çalışmalar ilgili bakanlık olan Sanayi ve Teknoloji Bakanlığının koordinatörlüğünde Bilgi Teknolojileri ve İletişim Kurumu ile sivil toplum kuruluşları tarafından yürütülmektedir. 2012 yılında 28447 sayılı Resmî Gazetede "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" yayınlanmıştır (Yılmaz ve Sağıroğlu, 2013).

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında siber ortamı meydana getiren sistemlerinin korunması, siber ortamda işlenen verinin bütünlüğünün, gizliliğinin ve erişilebilirliğinin sağlanması, saldırılara karşı güvenlik mekanizmalarının oluşturulması ve siber saldırı sonrası sistemlerin geriye döndürülmesi tanımlanmıştır (UDHB, 2012).

Sonrasında 9 Eylül 2016 da Türkiye'nin 4 yıllık süreçte bu konuda yürüteceği çalışmaları belirten 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı tanıtılmıştır. Bu eylem planında; tüm kesimlerce siber güvenliğin ulusal güvenlikte çok önemli bir yere sahip olduğunun benimsenmesi, siber güvenliğin tüm mecralarda etkinliğinin sağlanması için gerekli idari ve teknolojik tedbirlerin alınmasıdır (STM, 2016).

Ülkemizde eylem planlarında yer alan amaçların gerçekleştirilmesi için kamu kurumlarına ve kritik sektörleri düzenleyip denetleyen kurumlara SOME (Siber Olaylara Müdahale Ekipleri) kurulması için görevler verilmiştir. Bu ekiplerle kamu ve özel kuruluşlar arasında bilgi alışverişi hızlanacaktır (Öğün ve Kaya, 2013).

Türkiye'de siber güvenlik alanında farkındalığın arttırılması için çeşitli çalışmalar yapılmaktadır.

"Fulya Aslay (2017) tarafından yapılan çalışmasında STM Mühendislik Teknoloji Danışmanlık firmasının yayınladığı Temmuz Eylül Dönemi Siber Tehdit Durum Raporuna (STM, 2016) göre yine aynı yıl yayımlanan Fortinet firmasına ait rapora göre Türkiye zararlı yazılım (malware) ve istismar kiti (exploit kit) tespit edilen ülkeler sıralamasında ilk 5 de yer aldığı belirtilmiştir.

Trend Micro firması tarafından yayınlanan rapor incelendiğinde 2016 yılında tüm dünyada fidye yazılım saldırısının arttığı ve Türkiye'nin de Avrupa bölgesinde bu zararlı saldırıları en fazla yaşayan ülke olduğu görülmüştür. Ayrıca Trend Micro raporuna göre on-line bankacılık alanında yaşanan siber saldırılar ülkemizi oldukça etkilemekte ve Avrupa bölgesinde bu tür online saldırıları yaşayan ülkeler arasında ilk sırada Türkiye yer almaktadır. Ülkemizden sonra ise Almanya ve Fransa gelmektedir. Bu tür siber saldırıların miktarları arttıkça ülkelerin bunlara karşı aldıkları önlemler için yaptıkları harcamalar aynı oranda artmaktadır. Cybersecurity Ventures firmasında yer alan bilgilere göre 2015 yılında 3 trilyon dolar olan siber suçlar maliyetinin 2021 de 6 trilyon olması beklenmektedir. Bu tür saldırıların fazla olması nedeniyle kurumlar bilgi güvenliği danışmanlığı hizmeti veren şirketlerden danışmanlık almaktadırlar. Bu kapsamda da siber güvenlik harcamaları gün geçtikçe artmaktadır.

2.7.SİBER GÜVENLİKLE İLGİLİ YAPILAN ÇALIŞMALAR

"Cengiz Gündüz Alp (2021) tarafından yapılan çalışmanın amacı Türkiye'deki üniversitelerin bilgi işlem daire başkanlıklarında çalışanların dijital veri güvenliği ve siber güvenliği sağlama farkındalıklarını belirlemektir. Araştırmanın örneklemi güvenlik konusunda Türkiye'deki 174 üniversitedeki 410 çalışandan oluşmaktadır. Çalışma kesitsel tarama modeli ile yürütülmüştür. Araştırma sonucunda üniversitelerin bilgi işlem daire başkanlıklarındaki çalışanların dijital veri güvenliği ve kişisel siber güvenliği sağlama farkındalıklarının yüksek ve bu farkındalıklar üzerinde cinsiyet, yaş, mesleki deneyim, öğrenim durumu ve üstlenilen görevinde etkili olduğu anlaşılmıştır."

"Abdullah Karakaya (2020) tarafından yapılan çalışmanın amacı Karabük Üniversitesi çalışanlarına yönelik kişisel siber güvenlik araştırmasıdır. Araştırmada, üniversite de görev yapan idari ve akademik personelin siber güvenliğe dair algıları ölçülmüştür. Araştırma sonucunda çalışanların bilgi güvenliğine yönelik eğilimlerinde konum, cinsiyet ya da yaş farklılıklarının çalışanların algılarında ayırıcı bir özellik teşkil etmediği anlaşılmıştır. Bu noktada çalışanların desteklenmesi yönü ile sağlanabilecek bilgi güvenliği eğitimlerinin, çalışanları aynı yönde geliştireceği düşünülmektedir."

"Avcı ve Oruç (2020) tarafından yapılan çalışmanın amacı üniversite öğrencilerinin siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesidir. Bu çalışmaya,

Türkiye'de özel bir üniversitede Eğitim ve Mühendislik Fakültesi'nde okuyan 88 öğrenci katılmıştır. Bu çalışmada karma araştırma yöntemlerinden yakınsak paralel tasarım kullanılmıştır. Bu çalışmanın sonucunda öğrencilerin kişisel siber güvenliği sağlama ve bilgi güvenliği farkındalıklarının genel olarak yüksek olduğu görülmektedir. Öğrencilerin sosyal ağlarda alışveriş yaparken, şifre belirlerken, kişisel bilgileri paylaşırken, bilinmeyen adreslerden gelen postları yanıtlarken dikkatli olduklarını belirttikleri görülmektedir. Öğrencilerin kişisel gizliliği koruma ve ödeme bilgilerini koruma davranışlarında farkındalıklarının oldukça yüksek olduğu tespit edilmiştir."

"Yiğit ve Seferoğlu (2019) tarafından yapılan çalışmanın amacı üniversite öğrencilerinin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve cinsiyet, sınıf düzeyi, bölüm, bilişim güvenliği eğitimi alma durumu ve haftalık internet kullanım süresi değişkenlerine göre incelenmesidir. Çalışmaya farklı üniversite, bölüm ve sınıflardan 420 öğrenci katılmıştır. Verilerin analizi Pearson korelasyon katsayısı, bağımsız örneklemler t-testi ve tek yönlü varyans analizi (ANOVA) gibi istatistiksel teknikler kullanılarak yapılmıştır. Bu çalışmanın sonucunda öğrencilerin siber güvenlik davranış düzeylerinin kabul edilebilir bir seviyede olduğunu göstermiştir. Ayrıca öğrenciler kendilerini uyumlu, sorumlu ve deneyime açık kişiler olarak değerlendirirken, dışadönük konusunda kararsız bir görüş bildirmişlerdir."

"Aksoğan ve diğer (2018) tarafından yapılan çalışmanın amacı İletişim Fakültesinde öğrenim gören öğrencilerin siber suçlar ve siber güvenlik hakkındaki farkındalıklarını incelemektir. Çalışmaya İnönü Üniversitesi İletişim Fakültesinde, farklı bölüm ve sınıflarda öğrenim gören toplam 357 öğrenci katılmıştır. Veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Siber Güvenlik Farkındalığı Anketi" kullanılmıştır. Veriler betimleyici ve anlam çıkarıcı istatistikler kullanılarak analiz edilmiştir.

Araştırma sonuçlarına göre genel anlamda siber güvenlik konularında farkındalıklarının olmadığını belirten azımsanmayacak sayıda öğrenci bulunmaktadır. Cinsiyete, yaşlara ve internette günlük geçirilen süreye göre verilen cevapların bazılarında anlamlı farklılıklar gözlemlenirken, katılımcıların okudukları bölüme göre verilen cevaplar arasında anlamlı bir fark bulunmamıştır. İletişim Fakültesi öğrencileri için iyi hazırlanmış ve etkili bir bilişim güvenliği eğitimi verilmesi önerilmektedir."

“Ali Semerci (2019) tarafından yapılan çalışmanın amacı eğitim fakültesi öğrencileri ile diğer fakültelerdeki öğrencilerin siber güvenlik farkındalıklarının karşılaştırılması araştırmasıdır. Araştırmaya 2018-2019 eğitim-öğretim yılında üç farklı devlet üniversitesinde öğrenim gören 448 üniversite öğrenci katılmıştır. Veriler, anket formu ve “Kişisel Siber Güvenliği Sağlama Ölçeği” kullanılarak toplanmıştır. Araştırma bulguları, katılımcıların kişisel siber güvenlik farkındalıklarının orta ve üzeri düzeyde olduğu, eğitim fakültesi öğrencilerinin siber güvenlik farkındalık düzeyleri ile diğer fakültelerdeki öğrencilerin farkındalık düzeyleri ve cinsiyet arasında anlamlı farklılık bulunmadığı sonucuna ulaşılmıştır. Öğrencilerin siber güvenlik farkındalıkları ile sınıf düzeyi ve günlük internet kullanım süreleri arasında farklı etki düzeylerinde anlamlı farklılık bulunmuştur.”

2.8.KURUMSAL SİBER GÜVENLİK

Siber güvenlik hem ulusal hem uluslararası bir ihtiyaç olarak gözükse de, temel amacın toplumu, Kurum ve Şirketleri hatta bireyleri siber saldırılara karşı korumanın amaçlanması, daha kalıcı sonuçlar olacağından temel hedef olmalıdır. Bununla birlikte siber saldırıların birincil hedefi olan Kurum ve Şirketler için kurumsal siber güvenlik kaçınılmaz hale gelmiştir.

Kurum ve Şirketlerin siber saldırılardan korunabilmek için yeterli alt yapıyı oluşturması, çalışanları bilinçlendirmesi ve bilişim sistemlerinde yeterli ve tecrübeli personele sahip olması, saldırılara karşı olası riskleri belirlemesi, oluşan siber saldırılarda kök nedenleri araştırarak kalıcı önlemler alması, donanımları, altyapıları, internet sağlayıcıları, uygulamaları, her türlü bilgiyi güvenlik bir alt yapı ile koruması gerekmektedir.

2.8.1.Kurumsal Siber Güvenliğe Yönelik Tehditler

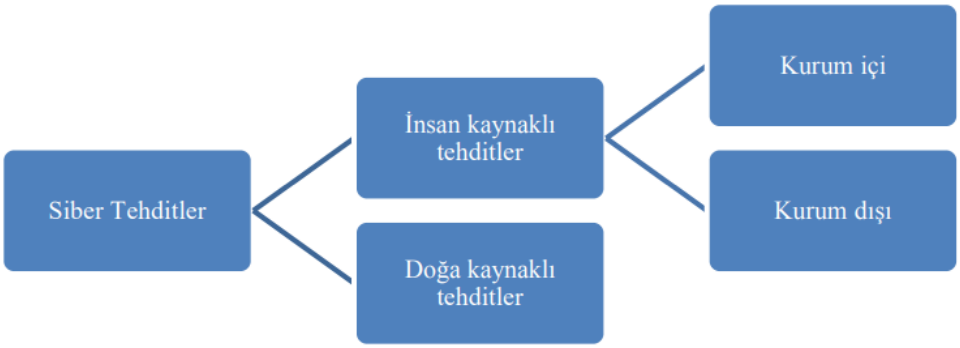
Kurumların siber ortamdaki verilerine yönelik siber tehditler, siber ortamdaki güvenlik açıklarının kullanılması ile meydana gelebilmektedir. Bu tehditler, insan kaynaklı ya da doğal kaynaklı tehditlerdir (Yaşar ve Çakır, 2015).

İnsan kaynaklı tehditler:

- *Kurum içi*: Bilinçsiz, eğitimsiz personel, sistemsel hatalar…

- *Kurum dışı*: İnternet ortamından gelen oltalama mailleri, izinsiz erişim, hırsızlık…

Doğa kaynaklı tehditler: Sel, yangın, deprem vb.… doğal afet



Şekil 2. 3: Siber Tehditlerin Sınıflandırılması

2.8.2.Kurumsal Siber Güvenliğe Yönelik Önlemler

Günlük hayatın vazgeçilmez bir parçası haline gelen teknoloji ve internet kullanımının artması ile birlikte bilgi ve iletişim teknolojisinde oluşan tehditlere karşı siber güvenlik olarak tanımlanan bir ihtiyaç doğmuştur. Siber saldırılara günümüzde en fazla Kurum ve Şirketler maruz kalmakta olup bu saldırıların artmasına yol açan sebepler aşağıda sıralanmıştır (Yaşar ve Çakır, 2015).

- İnternet kullanıcıların siber güvenlik konusunda yeterli bilgiye sahip olmaması,
- Kurum ve Şirketlerinin altyapılarının internet tabanlı olması,
- Şirketlerin üst düzey yöneticilerin konuya gerekli önemi vermemesi,
- Siber güvenlik konusunda gerekli yapılandırmanın olmaması,
- Bilgi işlem birimlerindeki personelin yetkin ve tecrübeli olmaması,
- Saldırılara konusunda Kurumların iş birliği içerisinde olmaması,
- Maruz kalınan saldırıların Şirketlerce gizli tutulması ve sebeplerinin yeterince araştırılmaması,

- Donanım ya da yazılımlarda güvenli üretimlerin olmaması vb.

Geçmişte yapılan saldırılar sadece erişimi sağlamaya yönelikken günümüzde yapılan siber saldırılar Kurum ve Şirketler için büyük tehditler oluşturmakta, erişim sağlanan verilerin kullanımı ile birlikte maddi zararlara da yol açmaktadır. Bu durumdaki Kurum ve Şirketler müşteri kayıpları yaşamakta ve itibar zedelenmesi ile karşı karşıya kalmaktadır.

Gelinen aşamada Kurum ve Şirketler için büyük tehdit oluşturan bu siber saldırılardan korunmak için siber güvenlik çalışmalarının yürütülmesi kaçınılmaz hale gelmektedir. Bu çalışmaların neredeyse tamamının ulusal ve uluslararası boyutta olduğu ve amaçlarının sistemsel ve karmaşık bir hale gelen bu saldırılardan korunmak. (Yaşar ve Çakır, 2015).

3. MALZEME VE YÖNTEM

Bu bölümde araştırmanın modeli, araştırma evreni ve örneklemi, veri toplama araçları, verilerin toplanması ve çözümlenmesinde kullanılan istatistiksel yöntem ve teknikler yer almaktadır.

Bu araştırmada, çalışanların siber güvenlik farkındalıklarının analizi incelemek amacıyla, bir ölçme aracı kullanılmıştır. Araştırmada bağımsızlık için ki-kare testi veya χ^2 testi kullanılmıştır.

Wikipedia göre **Ki-kare testi** veya **χ^2 testi** istatistik bilimi içinde bir sıra değişik problemlerde kullanılan bazıları parametrik olmayan sınama ve diğerleri parametrik sınama yöntemidir. Bu çeşit istatistiksel sınamalarda test istatistiği için "örnekleme dağılımı", sıfır hipotez gerçek olursa ki-kare dağılımı gösterir veya sıfır hipotez "asimptotik olarak gerçek" olursa, eğer sıfır hipotez gerçekse ve eğer örnekleme hacmi istenilen kadar yeterli olarak büyük ise bir ki-kare dağılımına çok yakın olarak yaklaşım gösterir.

Bağımsızlık için ki-kare testi ki-kare testinin uygulandığı değişik kategorik değerler taşıyan (satır için değişkende r tane kategorili bir değişken ve sütun için değişkende c tane kategorili değişken) iki tane rassal değişken bulunduğu kabul edilir. Bu iki kategorik rassal değişkenin birbirinden "bağımsız" olup olmadıkları araştırma sorusu için uygulanır. Bu tip testte, sıfır hipotez satır rassal değişkeni ile sütun rassal değişkeninin birbirinden "bağımsız" olduğudur ve "alternatif hipotez" "satır değişkeni ile sütun değişkeni birbirinden "bağımsız değildir" önerisidir. Dikkat edilirse bu testin sonucu simetrik değildir; hatta "zayıftır". Eğer sıfır hipotez test ile kabul edilirse sonuç "güçlü “dür ve uygulanmalara katkı yapabilir. Ama sıfır hipotez test ile reddedilirse, yani iki rassal değişken "bağımsız değil" ise, sonuç "zayıftır ve ne derecede iki değişkenin ne derecede bağımlı oldukları bu testle gösterilmez.

Bu araştırmada, istatistiksel analiz platformlarından biri olan SPSS ile çalışanların siber güvenlik farkındalıklarının analizi gerçekleştirilmiştir. Analiz aracı olarak SPSS programı seçilmenin sebebi başta anket analizleri olmak üzere sağlık bilimleri ve fen bilimleri alanlarında da elde edilen bazı ölçümlerin analiz etmesidir.

Bu konuda daha önce yapılan makale ve tez çalışmalarında katılımcıların öğrencilerin ağırlıklı olduğu ve 100- 400 kişi arasında yapılmıştır. Bu çalışmada farklı sektörlerde çalışan 870 katılımcı arasında yapılmıştır. Daha önceki çalışmalar belirli il ve kurumlarda yapılmış olup bu çalışmada böyle bir kısıtlamaya gidilmeden farklı il farklı kurumlardaki katılımcılar çalışmaya dahil edilmiştir. Diğer çalışmalarda SPSS analizinde yer alan Anova Testi, Faktör Analizi yapılmıştır. Bu çalışmada diğer çalışmalardan farklı olarak ki kare testi yapılmıştır.

Tez çalışmasında kullanılan anket, internet anketi türünde olup Google Forms kullanılarak hazırlanmış, katılımcılara elektronik ortamda ulaştırılmıştır ve internet ortamında yanıtlanmıştır. Araştırmada anket maddelerinin katılımcılar tarafından doğru bir şekilde okunup anlaşıldığı, dürüst ve gerçeği tam yansıtacak şekilde yanıtlandığı varsayımından hareket edilmiştir.

Araştırmada çalışanların, cinsiyet, yaş, eğitim düzeyi ve gelir durumu gibi değişkenlerin siber güvenlik farkındalıklarının biçimleri ile ilişkisi incelenmiştir. Araştırmaya katılan katılımcıların, değişkenlerle ilgili algıların belirlenmesi için bağımsızlık için ki-kare testi veya χ^2 testi kullanılmıştır.

3.1.EVREN VE ÖRNEKLEM

Araştırmanın evreni, Türkiye'de çalışmakta olan bireylerden oluşmaktadır. Örneklem ise, rastgele seçilen 870 çalışanlardan oluşmaktadır. Araştırmaya katılan çalışanların cinsiyete göre dağılımları **Tablo 3.1. '**de gösterilmiştir.

Tablo 3.1: Araştırmanın katılımcılarına ait demografik bilgiler

Değişkenler		N	%
Cinsiyet	Kadın	413	47,5
	Erkek	457	52,5

Tablo:3.1 İncelendiğinde araştırmaya katılan çalışanların cinsiyetleri açısından erkek çalışanların örneklemin **%52,5** (n=457), kadın çalışanların **%47,5**'sini (n=413) oluşturmaktadır. Araştırmaya katılan çalışanların yaş aralıklarına göre dağılımları **Tablo:3.2**' de gösterilmiştir.

Tablo 3.2: Araştırmanın katılımcılarına ait yaş dağılımı

Değişkenler		N	%
Yaş	18-25	89	10,2
	26-33	235	27,0
	34-40	303	34,8
	41-50	176	20,2
	50 yaş ve üstü	67	7,7

Tablo 3.2 İncelendiğinde katılımcıların yaş dağılımında **%34,8**'lik oranla en çok kullanıcının 34-50 yaş aralığında olduğu, 26-33 yaş aralığında bulunanların **%27,0'** lik ikinci sırada yer aldığı**, %10,2**'sinin 18-25 yaş arasında, 41-50 yaş arasında ve **%7,7**'sinin 50 yaş ve üzerinde olduğu gözlenmiştir.

Tablo 3.3: Araştırmanın katılımcılarına ait eğitim düzeyi dağılımı

Değişkenler		N	%
Eğitim düzeyi	Ortaokul	6	0,7
	Lise	68	7,8
	Ön lisans	64	7,4
	Lisans	520	59,8
	Yüksek lisans	191	22,0
	Doktora	21	2,4

Tablo:3.3 İncelendiğinde araştırmaya katılan çalışanların eğitim düzeyi incelendiğinde Katılımcıların **%0,7**'sinin ortaokul, **%7,8**'inin lise, **%7,4**'ünün ön lisans, **%59,8**'inin lisans, **%22**'sinin yüksek lisans ve **%2,4**'ünün doktora mezunu olduğu gözlenmiştir.

Tablo 3.4: Araştırmanın katılımcılarına aylık gelir dağılımı

Değişkenler		N	%
Aylık Geliriniz	0 – 4000 TL	100	11,5
	4001 – 8000 TL	297	34,1
	8001 – 12000 TL	335	38,5
	12000 TL ve üstü	138	15,9

Tablo 3.4 Araştırmaya katılan çalışanların eğitim düzeyi incelendiğinde katılımcıların **%11,5**'inin 0-4000 TL, **%34,1**'inin 4001-8000 TL, **%38,5** 'inin 8001-12.000 TL ve **%15,9**'unun 12.000 TL ve üstü olduğu gözlenmiştir.

Tablo 3.5: Araştırmanın katılımcılarına ait internette geçen süre dağılımı

Değişkenler		N	%
İnternette günlük geçirilen süre	1-3 Saat	366	42,1
	3-5 Saat	277	31,8
	5-7 Saat	138	15,9
	7 Saat ve üstü	89	10,2

Tablo 3.5 İncelendiğinde araştırmaya katılan çalışanların **%42,1**'inin 1-3 saat, **%31,8**'inin 3-5 saat, **%15,9**'unun 5-7 saat ve **%10,2**'sinin 7 saat ve üstü olduğu gözlenmiştir.

Tablo 3.6: Araştırmanın katılımcılarına ait internet kullanım nedeni dağılımı

Değişkenler		N	%
İnternet kullanım nedeni	Genellikle iş için kullanırım	252	29,0
	Genellikle sosyal medya için kullanırım	429	49,3
	Genellikle eğitim ve araştırma için kullanırım	189	21,7

Tablo 3.6 İncelendiğinde araştırmaya katılan çalışanların katılımcıların **%29,0**'unun genellikle iş için kullanırım, **%49,3**'ünün genellikle sosyal medya için kullanırım, **%21,7**'sinin genellikle eğitim ve araştırma için kullanırım şeklinde nedenleri olduğu gözlenmiştir.

3.2.VERİ TOPLAMA ARAÇLARI VE VERİLERİN TOPLANMASI

Araştırmanın amacı, çalışanların siber güvenlik farkındalıklarının farklı değişkenlere göre belirlenmesi ve incelenmesidir. Araştırma verileri internet anketi türünde olup Google Forms kullanılarak hazırlanmış, katılımcılara elektronik ortamda ulaştırılmıştır ve internet ortamında yanıtlanarak toplanılmıştır.

3.3.KİŞİSEL BİLGİ FORMU

Kişisel bilgiler formunda, demografik bilgiler yer almaktadır. Çalışanların; cinsiyet, yaş aralığı, eğitim düzeyi, aylık geliri, internet kullanım sıklığı ve interneti kullanma nedeni ile ilgili bilgiler toplanmıştır.

Tablo 3.7: Kişisel bilgi formu

I.KISIM	
KİŞİSEL BİLGİLER	
CİNSİYETİNİZ	( )Erkek ( )Kadın
YAŞINIZ	( )18-25 ( )26-33 ( )34-40 ( )41-50 ( )50 Yaş Üstü
EĞİTİM DÜZEYİNİZ	( )Ortaokul ( )Lise ( )Ön lisans ( )Lisans ( )Yüksek Lisans ( )Doktora
AYLIK GELİRİNİZ	( )0.TL-4.000TL ( )4.001TL-8.000TL ( )8.001TL-12.000TL ( )12.0000 ÜSTÜ
İNTERNETTE GÜNLÜK GEÇİRDİĞİNİZ SÜRE	( )1-3 Saat ( ) 3-5 Saat ( ) 5-7 Saat ( )7 Saat Üstü
İNTERNETİ KULLANMA NEDENİNİZ	( )Genellikle iş için kullanırım. ( ) Genellikle sosyal medya için kullanırım. ( ) Genellikle eğitim ve araştırma için kullanırım.

3.4.SİBER GÜVENLİĞİ SAĞLAMA ÖLÇEĞİ

Ölçek 5'li likert tipi olarak hazırlanmıştır ve her bir madde, 1-Hiçbir zaman 2-Nadiren 3-Ara sıra 4-Sık sık ve 5-Her zaman arası değerler almakta ve ifadelerinden kendilerine en uygun olanının seçilmesi istenmiştir.

Tablo 3.8: Siber güvenlik farkındalığı sağlama ölçeği

II. KISIM					
Çalışanların Siber Güvenlik Farkındalığı Sağlama Ölçeği	HER ZAMAN	ÇOĞUNLUKLA	SIK SIK	ARA SIRA	HİÇBİR ZAMAN
	5	4	3	2	1
1.Kullandığım elektronik cihazların yazılımlarını güncellerim.					
2.Kullandığım elektronik cihazlarda anti-virüs yazılımı programı bulundururum.					
3.İnternet ortamında kullandığım kullanıcı şifrelerinin aynı olmamasına dikkat ederim.					
4.İnternetten yaptığım bankacılık işlemlerini kişisel bilgisayarımdan yaparım.					
5.Herhangi bir bilgi güvenliği ihlali olduğunda IT (bilgi işlem) veya bilgi güvenliği birimine bildiririm.					
6. Kimlik ya da bankacılık bilgilerimin çalınması amacıyla atılan yanıltıcı saldırılara karşı e-posta servisimizi test ederim.					
7.Siber güvenlik farkındalık eğitimlerine katılırım.					
8.Güvenliğinden şüphe duyduğum sitelere üye olurum.					
9.Bilgisayarımda başkalarının flash belleklerini kullanırım.					
10.E-maillerime güvenlik şifresi kullanarak giriş yaparım.					
11.Siber saldırıya maruz kaldım.					
12.Sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddederim.					
13. (E-posta, sosyal ağ vb.) Sanal şifrelerimi düzenli olarak değiştiririm.					
14. Elektronik cihazlarıma uygulamaları yüklerken üreticinin orijinal sitesi olmasına dikkat ederim.					
15. E-posta, forum siteleri vb. sanal şifrelerimi paylaşırım.					
16.Kabul etmek istemediğim e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye özen gösteririm.					
17.Bana ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösteririm.					
18.Bilgisayarımda şifreli ekran koruyucusu kullanmaya özen gösteririm.					
19. İnternetten link geldiğinde sorgulamadan tıklarım.					
20. Mobil cihazıma erişim sağlamak amacıyla pin kodu ya da parola kullanırım.					
21.Kişisel verilerin işlenmesi ile ilgili yasaları okurum.					
22. Uygulamalarda şahsi bilgilerin açık onayım bulunmadan ülke dışına gönderilmesine izin veririm.					
23.Çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım.					
24.Kullandığım elektronik cihazlarda arkadaşlarımın da bilgilerini tutuyorum.					
25. Kişisel verilerin korunması hakkındaki eğitimlere katılırım.					

3.4.VERİLERİN ANALİZİ

Veriler SPSS 26.0 istatistiksel paket programı ile değerlendirilmiştir. Tanımlayıcı değerler sayı (S) ve yüzdeler (%) şeklinde ifade edilmiştir.

Veriler ankette yer alan sorulara verilen yanıtlara göre frekans ve yüzde değerleri ile betimlenmiştir.

4. BULGULAR

Siber güvenlik farkındalığının, cinsiyet, yaş, gelir ve eğitim durumuna göre farklılaşıp farklılaşmadığı madde madde ki-kare ile incelenmiştir.

4.1.SİBER GÜVENLİK FARKINDALIĞININ CİNSİYETE GÖRE FARKILAŞIP FARKLILAŞMADIĞI Kİ KARE TESTİ İLE İNCELENMESİ

Tablo 4.1: Katılımcıların cinsiyetleri ile interneti kullanma nedenleri arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	**Erkek**
		χ^2=20,942**	**p=0,000***
İnterneti Kullanma Nedeniniz	**Genellikle iş için kullanırım.**	**93**	**159**
		36,9%	**63,1%**
	Genellikle sosyal medya için kullanırım.	**235**	**194**
		54,8%	**45,2%**
	Genellikle eğitim ve araştırma için kullanırım.	**85**	**104**
		45,0%	**55,0%**

Tablo 4.1 Katılımcıların interneti kullanma nedeni ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların ağırlıklı olarak interneti kullanım nedenin sosyal medya olduğu, kadın ve erkek katılımcı karşılaştırıldığında kadınların interneti sosyal medya için kullanım oranı **%54,8** iken erkeklerin **%45,2** olması nedeniyle kadınların internetin kullanım amacının erkeklerden daha çok sosyal medya olduğu, iş için kullanan karşılaştırıldığında erkeklerin oranın kadınlardan daha fazla olduğu görülmüştür.

Tablo 4.2: Katılımcıların cinsiyetleri ile kullandıkları elektronik cihazların yazılımlarını güncelleme durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	Erkek
		χ^2=27,936**	p=0,000*
Kullandığım elektronik cihazların yazılımlarını güncellerim.	Hiçbir zaman	8	9
		47,1%	52,9%
	Nadiren	146	110
		57,0%	43,0%
	Ara sıra	32	29
		52,5%	47,5%
	Sık sık	138	140
		49,6%	50,4%
	Her zaman	89	169
		34,5%	65,5%

Tablo 4.2 Katılımcıların kullandıkları elektronik cihazların yazılımlarını güncelleme durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların elektronik cihazların yazımları güncelleme konusunda erkeklerin kadınlara göre daha çok güncelleme yaptıkları ve daha hassas oldukları, her zaman güncelleme yapan kadın ve erkek katılımcı karşılaştırıldığında kadınlarının oranının **%34,5** erkeklerin ise **%65,5** olduğu görülmüştür.

Tablo 4.3: Katılımcıların cinsiyetleri ile siber güvenlik farkındalık eğitimlerine katılma durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	Erkek
		χ^2=17,974**	p=0,001*
Siber güvenlik farkındalık eğitimlerine katılırım.	Hiçbir zaman	201	169
		54,3%	45,7%
	Nadiren	139	161
		46,3%	53,7%
	Ara sıra	23	32
		41,8%	58,2%
	Sık sık	30	52
		36,6%	63,4%
	Her zaman	20	43
		31,7%	68,3%

Tablo 4.3 Katılımcıların siber güvenlik farkındalık eğitimlerine katılma durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Katılımcıların siber güvenlik farkındalık eğitimlere katılım konusunda cinsiyetleri arasındaki ilişki incelendiğinde erkeklerin kadınlara kıyasla siber güvenlik eğitimlere katılımının daha sık olduğu görülmüştür. Kadınların **%46,3'ü** siber eğitimlere ara sıra katılım gösterirken, erkeklerin **%53,7'si** ara sıra katılım gösterdiğini bildirmiştir.

Tablo 4.4: Katılımcıların cinsiyetleri ile güvenliğinden şüphe duydukları sitelere üye olma durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	Erkek
		χ^2=17,495**	p=0,002*
Güvenliğinden şüphe duyduğum sitelere üye olurum.	Hiçbir zaman	370	376
		49,6%	50,4%
	Nadiren	26	61
		29,9%	70,1%
	Ara sıra	4	5
		44,4%	55,6%
	Sık sık	3	10
		23,1%	76,9%
	Her zaman	10	5
		66,7%	33,3%

Tablo 4.4 Katılımcıların güvenliğinden şüphe duydukları sitelere üye olma durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların ağırlıklı olarak güvenliğinden şüphe duydukları sitelere üye olmadıkları, tüm katılımcıların tercihleri değerlendirildiğinde güvenliğinden şüphe duyulan sitelere üyeliğe az olduğu görülmektedir. Güvenliğinden şüphe duyulan sitelere üye olunmaması ilişkin kadın ve erkeklerin oranların yakın olduğu gözlenmiştir.

Tablo 4.5: Katılımcıların cinsiyetleri ile bilgisayarlarında başkalarının flash belleklerini kullanma durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	Erkek
		χ2=17,226**	p=0,002*
Bilgisayarımda başkalarının flash belleklerini kullanırım.	Hiçbir zaman	160	132
		54,8%	45,2%
	Nadiren	212	251
		45,8%	54,2%
	Ara sıra	13	26
		33,3%	66,7%
	Sık sık	25	33
		43,1%	56,9%
	Her zaman	3	15
		16,7%	83,3%

Tablo 4.5 Katılımcıların bilgisayarlarında başkalarının flash belleklerini kullanma durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların bilgisayarında başkalarına ait flash belleklerini kullanımının az olduğu gözlemlenmiştir. Ayrıca kadınların bilgisayarlarında başkalarına ait flash belleklerini hiçbir zaman kullanılmayan katılımcıların **%54,8** kadın iken **%45,2** erkeklerden oluştuğu görülmektedir. Bu oranlara göre kadınların erkeklere göre başkalarına ait flash belleklerin kullanmama konusunda daha hassas oldukları görülmüştür.

Tablo 4.6: Katılımcıların cinsiyetleri ile siber saldırıya maruz kalma durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	Erkek
		χ^2=14,687**	p=0,005*
Siber saldırıya maruz kaldım.	Hiçbir zaman	319	304
		51,2%	48,8%
	Nadiren	86	135
		38,9%	61,1%
	Ara sıra	7	12
		36,8%	63,2%
	Sık sık	0	4
		0,0%	100,0%
	Her zaman	1	2
		33,3%	66,7%

Tablo 4.6 Katılımcıların siber saldırıya maruz kalma durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların çoğunluğunun siber saldırıya maruz kalmadığı gözlemlenmiştir. Katılımcıların **%28,4'ü** siber saldırıya maruz kalmıştır. Siber saldırıya maruz kalan katılımcıların arasında erkek katılımcı sayısının **153** olduğu, kadın katılımcının sayısı **94** olduğu görülmüştür. Bu sonuçlara göre erkek katılımcılara kadınlara oranlara daha çok siber saldırıya maruz kaldığı gözlemlenmiştir.

Tablo 4.7: Katılımcıların cinsiyetleri ile uygulamalarda şahsi bilgilerinin açık onayları bulunmadan ülke dışına gönderilmesine izin verme durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	Erkek
		χ^2=22,827**	p=0,000*
Uygulamalarda şahsi bilgilerin açık onayım bulunmadan ülke dışına gönderilmesine izin veririm.	Hiçbir zaman	342	318
		51,8%	48,2%
	Nadiren	52	103
		33,5%	66,5%
	Ara sıra	9	19
		32,1%	67,9%
	Sık sık	7	7
		50,0%	50,0%
	Her zaman	3	10
		23,1%	76,9%

Tablo 4.7 Katılımcıların uygulamalarda şahsi bilgilerinin açık onayları bulunmadan ülke dışına gönderilmesine izin verme durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların büyük çoğunluğunun uygulamalarda şahsi bilgilerin açık onayım bulunmadan ülke dışına gönderilmesine izin vermediği gözlemlenmiştir. Bu sonuçlara göre erkek katılımcılara kadınlara oranlara daha az dikkat ettikleri görülmüştür.

Tablo 4.8: Katılımcıların cinsiyetleri ile çevrelerindeki insanlar ile beraber çektirdikleri fotoğraflarını sosyal paylaşım sitelerinde yayınlama durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	Erkek
		χ^2=9,927**	p=0,042*
Çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım.	Hiçbir zaman	70	99
		41,4%	58,6%
	Nadiren	210	242
		46,5%	53,5%
	Ara sıra	41	24
		63,1%	36,9%
	Sık sık	65	69
		48,5%	51,5%
	Her zaman	27	23
		54,0%	46,0%

Tablo 4.8 Katılımcıların çevrelerindeki insanlar ile beraber çektirdikleri fotoğraflarını sosyal paylaşım sitelerinde yayınlama durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların **%20'** sinin çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım sorusuna hiçbir zaman yanıtına verdiği görülmüştür. Katılımcı çalışanların **%80**'nin ara sırada olsa sosyal medyada çevresindeki insanlar ile beraber çektirdiği fotoğrafların sosyal paylaşım sitelerinde paylaştıkları anlaşılmaktadır. Bu sonuçlara göre erkek katılımcıların kadınlara oranla daha az paylaşım yaptıkları görülmektedir.

Tablo 4.9: Katılımcıların cinsiyetleri ile kullandıkları elektronik cihazlarda arkadaşlarının da bilgilerini tutma durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	**Erkek**
		χ^2=10,839**	**p=0,028***
Kullandığım elektronik cihazlarda arkadaşlarımın da bilgilerini tutuyorum.	**Hiçbir zaman**	**286**	**271**
		51,3%	**48,7%**
	Nadiren	**90**	**127**
		41,5%	**58,5%**
	Ara sıra	**14**	**25**
		35,9%	**64,1%**
	Sık sık	**17**	**29**
		37,0%	**63,0%**
	Her zaman	**6**	**5**
		54,5%	**45,5%**

Tablo 4.9 Katılımcıların kullandıkları elektronik cihazlarda arkadaşlarının da bilgilerini tutma durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların çoğunluğunun kullandığı elektronik cihazlarda arkadaşlarının ait bilgilerini tutmadığı görülmüştür. İlgili madde incelendiğinde arkadaşlarına ait bilgileri elektronik cihazlarında hiçbir zaman tutmayan kadınların oranın **%51,3'ü** erkeklerin ise **%48,7** olduğu görülmüştür. Bu sonuca göre kadınların bu konuda daha dikkatli olduğu anlaşılmıştır.

Tablo 4.10: Katılımcıların cinsiyetleri ile kişisel verilerin korunması hakkındaki eğitimlere katılma durumları ile arasındaki ilişki

		CİNSİYETİNİZ	
		Kadın	**Erkek**
		χ^2=12,018**	**p=0,017***
Kişisel verilerin korunması hakkındaki eğitimlere katılırım.	**Hiçbir zaman**	**135**	**115**
		54,0%	**46,0%**
	Nadiren	**168**	**179**
		48,4%	**51,6%**
	Ara sıra	**25**	**42**
		37,3%	**62,7%**
	Sık sık	**50**	**60**
		45,5%	**54,5%**
	Her zaman	**35**	**61**
		36,5%	**63,5%**

Tablo 4.10 Katılımcıların kişisel verilerin korunması hakkındaki eğitimlere katılma durumları ile cinsiyetleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların **%28'i** kişisel verilerin korunması hakkındaki eğitimlere katılmadığı görülmüştür. Oranlara bakıldığında erkek katılımcıların kadın katılımcılara göre bu tür eğitimlere daha ilgili olduğu anlaşılmıştır.

4.2.SİBER GÜVENLİK FARKINDALIĞININ YAŞA GÖRE FARKILAŞIP FARKLILAŞMADIĞI Kİ KARE TESTİ İLE İNCELENMESİ

Tablo 4.11: Katılımcıların yaşları ile interneti kullanma nedenleri arasındaki ilişki

χ^2=18,992**		YAŞINIZ				
p=0,015*		18-25	26-33	34-40	41-50	50 yaş ve üstü
İnterneti Kullanma Nedeniniz	Genellikle iş için kullanırım.	11	67	90	58	26
		4,4%	26,6%	35,7%	23,0%	10,3%
	Genellikle sosyal medya için kullanırım.	56	119	149	81	24
		13,1%	27,7%	34,7%	18,9%	5,6%
	Genellikle eğitim ve araştırma için kullanırım.	22	49	64	37	17
		11,6%	25,9%	33,9%	19,6%	9,0%

Tablo 4.11 Katılımcıların yaşları ile interneti kullanma nedenleri arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında ağırlıklı olarak interneti kullanım nedenin sosyal medya olduğu, sosyal medyayı için kullanan yaş grubunun **%34,7** oranla en çok 34-40 yaş grubunun olduğu, en az kullanan yaş grubunun da 50 yaş ve üstü olduğu görülmektedir.

Tablo 4.12: Katılımcıların yaşları ile kullandıkları elektronik cihazların yazılımlarını güncelleme durumları ile arasındaki ilişki

χ^2=27,492**		YAŞINIZ				
p=0,036*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Kullandığım elektronik cihazların yazılımlarını güncellerim.	Hiçbir zaman	1	6	5	2	3
		5,9%	35,3%	29,4%	11,8%	17,6%
	Nadiren	31	53	88	61	23
		12,1%	20,7%	34,4%	23,8%	9,0%
	Ara sıra	10	14	17	12	8
		16,4%	23,0%	27,9%	19,7%	13,1%
	Sık sık	21	81	96	57	23
		7,6%	29,1%	34,5%	20,5%	8,3%
	Her zaman	26	81	97	44	10
		10,1%	31,4%	37,6%	17,1%	3,9%

Tablo 4.12 Katılımcıların yaşları ile kullandıkları elektronik cihazların yazılımlarını güncelleme durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında olarak kullandığı elektronik cihazların yazılımları güncelleme konusunda ağırlıklı olarak ya sık sık ya da her zaman güncelleme yaptıkları görülmüştür. **%37,6** oranla en çok **34-40** yaş grubunun olduğu her zaman güncelleme yaptıkları anlaşılmıştır.

Tablo 4.13: Katılımcıların yaşları ile kullandıkları elektronik cihazlarda anti-virüs yazılımı bulundurma durumları ile arasındaki ilişki

χ^2=42,381**		YAŞINIZ				
p=0,000*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Kullandığım elektronik cihazlarda anti-virüs yazılımı programı bulundururum.	Hiçbir zaman	15	29	17	8	7
		19,7%	38,2%	22,4%	10,5%	9,2%
	Nadiren	32	55	81	47	11
		14,2%	24,3%	35,8%	20,8%	4,9%
	Ara sıra	8	15	28	16	5
		11,1%	20,8%	38,9%	22,2%	6,9%
	Sık sık	12	90	95	58	24
		4,3%	32,3%	34,1%	20,8%	8,6%
	Her zaman	22	46	82	47	20
		10,1%	21,2%	37,8%	21,7%	9,2%

Tablo 4.13 Katılımcıların yaşları ile kullandıkları elektronik cihazlarda anti-virüs yazılımı bulundurma durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$).Araştırmaya katılan çalışanların tüm yaş gruplarında olarak kullandığı elektronik cihazlarda anti-virüs programı bulundurma konusunda ağırlıklı olarak ya sık sık ya da her zaman yaptıkları görülmüştür. **%37,8** oranla en çok 34-40 yaş grubunun olduğu her zaman bulundurdukları anlaşılmıştır.

Tablo 4.14: Katılımcıların yaşları ile internetten yaptıkları bankacılık işlemlerini kişisel bilgisayarlarından da yapma durumları ile arasındaki ilişki

χ^2=35,538**		YAŞINIZ				
p=0,003*		18-25	26-33	34-40	41-50	50 yaş ve üstü
İnternetten yaptığım bankacılık işlemlerini kişisel bilgisayarımdan yaparım.	Hiçbir zaman	19	38	41	25	6
		14,7%	29,5%	31,8%	19,4%	4,7%
	Nadiren	14	43	58	26	16
		8,9%	27,4%	36,9%	16,6%	10,2%
	Ara sıra	11	12	15	8	2
		22,9%	25,0%	31,3%	16,7%	4,2%
	Sık sık	9	63	79	50	8
		4,3%	30,1%	37,8%	23,9%	3,8%
	Her zaman	36	79	110	67	35
		11,0%	24,2%	33,6%	20,5%	10,7%

Tablo 4.14 Katılımcıların yaşları ile internetten yaptıkları bankacılık işlemlerini kişisel bilgisayarlarından da yapma durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında olarak internetten yaptığı bankacılık işlemlerini kişisel bilgisayarımdan yapma konusunda ağırlıklı olarak kişisel bilgisayarında yaptıkları görülmüştür. **%11,0** oranla 18-25 yaş grubu ile **%10,7** oranla 50 yaş ve üstü yaş grubunun her zaman yapmadığı görülmüştür.

Tablo 4.15: Katılımcıların yaşları ile sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddetme durumları ile arasındaki ilişki

χ^2=29,110**		YAŞINIZ				
p=0,023*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddederim.	Hiçbir zaman	3	3	5	3	2
		18,8%	18,8%	31,3%	18,8%	12,5%
	Nadiren	11	21	36	10	8
		12,8%	24,4%	41,9%	11,6%	9,3%
	Ara sıra	9	8	17	7	5
		19,6%	17,4%	37,0%	15,2%	10,9%
	Sık sık	25	52	59	27	8
		14,6%	30,4%	34,5%	15,8%	4,7%
	Her zaman	41	151	186	129	44
		7,4%	27,4%	33,8%	23,4%	8,0%

Tablo 4.15 Katılımcıların yaşları ile sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddetme durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddettikleri görülmüştür.

Tablo 4.16: Katılımcıların yaşları ile (E-posta, sosyal ağ vb.) Sanal şifrelerini düzenli olarak değiştirme durumları ile arasındaki ilişki

χ^2=28,085**		YAŞINIZ				
p=0,031*		18-25	26-33	34-40	41-50	50 yaş ve üstü
(E-posta, sosyal ağ vb.) Sanal şifrelerimi düzenli olarak değiştiririm.	Hiçbir zaman	21	29	45	17	7
		17,6%	24,4%	37,8%	14,3%	5,9%
	Nadiren	33	106	110	61	21
		10,0%	32,0%	33,2%	18,4%	6,3%
	Ara sıra	11	33	37	20	12
		9,7%	29,2%	32,7%	17,7%	10,6%
	Sık sık	13	40	54	43	13
		8,0%	24,5%	33,1%	26,4%	8,0%
	Her zaman	11	27	57	35	14
		7,6%	18,8%	39,6%	24,3%	9,7%

Tablo 4.16 Katılımcıların yaşları ile (E-posta, sosyal ağ vb.) Sanal şifrelerini düzenli olarak değiştirme durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında ağırlıklı olarak sanal şifrelerimi düzenli olarak değiştirme konusunda nadiren değiştikleri görülmüştür.

Tablo 4.17: Katılımcıların yaşları ile kabul etmek istemedikleri e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösterme durumları ile arasındaki ilişki

χ^2=44,405**		YAŞINIZ				
p=0,000*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Kabul etmek istemediğim e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösteririm.	Hiçbir zaman	22	18	22	18	7
		25,3%	20,7%	25,3%	20,7%	8,0%
	Nadiren	23	54	59	26	10
		13,4%	31,4%	34,3%	15,1%	5,8%
	Ara sıra	6	25	42	18	7
		6,1%	25,5%	42,9%	18,4%	7,1%
	Sık sık	18	60	80	44	11
		8,5%	28,2%	37,6%	20,7%	5,2%
	Her zaman	20	78	100	70	32
		6,7%	26,0%	33,3%	23,3%	10,7%

Tablo 4.17 Katılımcıların yaşları ile kabul etmek istemedikleri e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösterme durumları arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında ağırlıklı olarak kabul etmek istemediği e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösterdikleri anlaşılmaktadır. Çünkü her zaman seçeneğini 18-25 yaş aralığı 20 kişi, 26-33 yaş aralığı 78 kişi, 34-40 yaş aralığı 100 kişi, 41-50 yaş aralığı 70 kişi, 50 yaş ve üstü 32 kişi seçmiştir. Her zamanı seçeneğini en çok işaretleyen yaş grubu **%33,3 oranla** 34-40 yaş aralığı olduğu görülmüştür.

Tablo 4.18 : Katılımcıların yaşları ile katılımcılara ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösterme durumları ile arasındaki ilişki

χ^2=27,554**		YAŞINIZ				
p=0,036*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Bana ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösteririm.	Hiçbir zaman	5	8	11	5	1
		16,7%	26,7%	36,7%	16,7%	3,3%
	Nadiren	9	26	33	26	5
		9,1%	26,3%	33,3%	26,3%	5,1%
	Ara sıra	16	26	28	8	2
		20,0%	32,5%	35,0%	10,0%	2,5%
	Sık sık	22	78	98	54	18
		8,1%	28,9%	36,3%	20,0%	6,7%
	Her zaman	37	97	133	83	41
		9,5%	24,8%	34,0%	21,2%	10,5%

Tablo 4.18 Katılımcıların yaşları ile katılımcılara ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösterme durumları arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında bana ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösteririm konusunda 270 kişi sık sık seçeneğini, 391 kişi her zaman seçeneğini işaretlemiştir. Bu sonuçlara göre tüm katılımcıların ağırlıklı olarak onlara ait olmayan cihazlarda şifre isteyen işlemleri yapmadıkları anlaşılmıştır. Ayrıca 18-25 yaş aralığı **%9,5** oranla ve 50 yaş üstü çalışanların **%10,5** oranla diğer yaş gruplarına göre daha az özen gösterdikleri anlaşılmıştır.

Tablo 4.19: Katılımcıların yaşları ile uygulamalarda şahsi bilgilerinin açık onayları bulunmadan ülke dışına gönderilmesine izin verme durumları ile arasındaki ilişki

χ^2=26,864**		YAŞINIZ				
p=0,043*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Uygulamalarda şahsi bilgilerin açık onayım bulunmadan ülke dışına gönderilmesine izin veririm.	Hiçbir zaman	61	171	221	147	60
		9,2%	25,9%	33,5%	22,3%	9,1%
	Nadiren	18	45	60	25	7
		11,6%	29,0%	38,7%	16,1%	4,5%
	Ara sıra	7	9	11	1	0
		25,0%	32,1%	39,3%	3,6%	0,0%
	Sık sık	1	6	5	2	0
		7,1%	42,9%	35,7%	14,3%	0,0%
	Her zaman	2	4	6	1	0
		15,4%	30,8%	46,2%	7,7%	0,0%

Tablo 4.19 Katılımcıların yaşları ile uygulamalarda şahsi bilgilerinin açık onayları bulunmadan ülke dışına gönderilmesine izin verme durumları arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların tüm yaş gruplarında uygulamalarda şahsi bilgilerin açık onayım bulunmadan ülke dışına gönderilmesine izin veririm konusunda çoğunlukla hiçbir zaman seçeneği işaretlenmiştir. Özellikle tüm yaş gruplarında bu konuda özen gösterdikleri görülmüştür. Tüm katılımların sayısı olan 870 kişiden 660 kişi hiçbir zaman seçeneği işaretlemiştir.

Tablo 4.20: Katılımcıların yaşları ile çevrelerindeki insanlar ile beraber çektirdikleri fotoğraflarını sosyal paylaşım sitelerinde yayınlama durumları ile arasındaki ilişki

χ^2=61,932**		YAŞINIZ				
p=0,000*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım.	Hiçbir zaman	14	26	71	45	13
		8,3%	15,4%	42,0%	26,6%	7,7%
	Nadiren	36	117	154	102	43
		8,0%	25,9%	34,1%	22,6%	9,5%
	Ara sıra	11	23	17	9	5
		16,9%	35,4%	26,2%	13,8%	7,7%
	Sık sık	19	58	43	11	3
		14,2%	43,3%	32,1%	8,2%	2,2%
	Her zaman	9	11	18	9	3
		18,0%	22,0%	36,0%	18,0%	6,0%

Tablo 4.20 Katılımcıların yaşları ile çevrelerindeki insanlar ile beraber çektirdikleri fotoğraflarını sosyal paylaşım sitelerinde yayınlama durumları arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım konusunda nadiren seçeneği işaretlendiği görülmüştür. Bu sonuçlara göre tüm yaş gruplarında sosyal medyada çevresinde insanları paylaşmama konusunda hassas oldukları görülmüştür.

Tablo 4.21: Katılımcıların yaşları ile kullandıkları elektronik cihazlarda arkadaşlarının da bilgilerini tutma durumları ile arasındaki ilişki

χ^2=52,847**		YAŞINIZ				
p=0,000*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Kullandığım elektronik cihazlarda arkadaşlarımın da bilgilerini tutuyorum.	Hiçbir zaman	39	135	197	139	47
		7,0%	24,2%	35,4%	25,0%	8,4%
	Nadiren	35	64	75	31	12
		16,1%	29,5%	34,6%	14,3%	5,5%
	Ara sıra	6	16	11	3	3
		15,4%	41,0%	28,2%	7,7%	7,7%
	Sık sık	8	18	12	3	5
		17,4%	39,1%	26,1%	6,5%	10,9%
	Her zaman	1	2	8	0	0
		9,1%	18,2%	72,7%	0,0%	0,0%

Tablo 4.21 Katılımcıların yaşları ile kullandıkları elektronik cihazlarda arkadaşlarının da bilgilerini tutma durumları arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların **%64** hiçbir zaman, **%25** nadiren, **%4** ara sıra, **%5** sık sık, **%1** her zaman seçeneğini işaretlemiştir. Bu sonuçlara göre yaş grupların kişisel verilere önem verdiği anlaşılmaktadır.

Tablo 4.22: Katılımcıların yaşları ile kişisel verilerin korunması hakkındaki eğitimlere katılma durumları ile arasındaki ilişki

χ^2=21,435**		YAŞINIZ				
p=0,162*		18-25	26-33	34-40	41-50	50 yaş ve üstü
Kişisel verilerin korunması hakkındaki eğitimlere katılırım.	Hiçbir zaman	40	63	84	48	15
		16,0%	25,2%	33,6%	19,2%	6,0%
	Nadiren	29	97	116	78	27
		8,4%	28,0%	33,4%	22,5%	7,8%
	Ara sıra	8	18	26	11	4
		11,9%	26,9%	38,8%	16,4%	6,0%
	Sık sık	8	29	42	22	9
		7,3%	26,4%	38,2%	20,0%	8,2%
	Her zaman	4	28	35	17	12
		4,2%	29,2%	36,5%	17,7%	12,5%

Tablo 4.22 Katılımcıların yaşları ile kişisel verilerin korunması hakkındaki eğitimlere katılma durumları arasında istatistiksel olarak anlamlı bir ilişki olmadığı görülmektedir. (p>0,05). Araştırmaya katılan çalışanların kişisel verilerin korunması hakkındaki eğitimlere katılma konusunda hiçbir zaman ve nadiren seçeneğin işaretlediği görülmüştür. Her zaman kişisel verilerin konusunda eğitimlere katılan yaş grubunda **%36,5** oranla 34-40 yaş aralığı en çok katılandır.

4.3.SİBER GÜVENLİK FARKINDALIĞININ GELİRE GÖRE FARKILAŞIP FARKLILAŞMADIĞI Kİ KARE TESTİ İLE İNCELENMESİ

Tablo 4.23: Katılımcıların gelir durumu ile internetten yaptıkları bankacılık işlemlerini kişisel bilgisayarlarından da yapma durumları ile arasındaki ilişki

x^2=39,710**		**GELİR DURUMU**			
P=0,000*		**0-4.000 TL**	**4.000-8.000 TL**	**8.001-12.000 TL**	**12.000 TL ve üstü**
İnternetten yaptığım bankacılık işlemlerini kişisel bilgisayarımdan yaparım.	**Hiçbir zaman**	19	51	51	8
		14,7%	39,5%	39,5%	6,2%
	Nadiren	15	66	59	17
		9,6%	42,0%	37,6%	10,8%
	Ara sıra	11	10	23	4
		22,9%	20,8%	47,9%	8,3%
	Sık sık	19	68	87	35
		9,1%	32,5%	41,6%	16,7%
	Her zaman	36	102	115	74
		11,0%	31,2%	35,2%	22,6%

Tablo 4.23 Katılımcıların gelir durumu ile internetten yaptıkları bankacılık işlemlerini kişisel bilgisayarlarından da yapma durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların "İnternetten yaptığım bankacılık işlemlerini kişisel bilgisayarımdan yaparım." sorusuna 870 katılımcıdan 327 katılımcı her zaman, 209 katılımcı da sık sık olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu internetten yaptığı bankacılık işlemlerini kişisel bilgisayarından yapmaya dikkat ettiği

anlaşılmıştır. 8.001-12.000 TL gelir durumuna sahip katılımcıların **%35,2** oranla diğer gelir durumuna sahip katılımcılara göre daha çok bu konuda hassas oldukları görülmüştür.

Tablo 4.24: Katılımcıların gelir durumu ile siber güvenlik farkındalık eğitimlerine katılma durumları ile arasındaki ilişki

x^2=35,497**		**GELİR DURUMU**			
P=0,000*		**0-4.000 TL**	**4.000 -8.000 TL**	**8.001-12.000 TL**	**12.000 TL Ve üstü**
Siber güvenlik farkındalık eğitimlerine katılırım.	**Hiçbir zaman**	56	132	138	44
		15,1%	35,7%	37,3%	11,9%
	Nadiren	26	104	118	52
		8,7%	34,7%	39,3%	17,3%
	Ara sıra	7	21	19	8
		12,7%	38,2%	34,5%	14,5%
	Sık sık	8	27	36	11
		9,8%	32,9%	43,9%	13,4%
	Her zaman	3	13	24	23
		4,8%	20,6%	38,1%	36,5%

Tablo 4.24 Katılımcıların gelir durumu ile siber güvenlik farkındalık eğitimlerine katılma durumları ile arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır($p<0,05$). Araştırmaya katılan çalışanların "Siber güvenlik farkındalık eğitimlerine katılırım." sorusuna 870 katılımcıdan 370 katılımcı hiçbir zaman, 300 katılımcı da nadiren olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu Siber güvenlik farkındalık eğitimlerine katılmadıkları anlaşılmıştır. İnternetten yaptığı bankacılık işlemlerini kişisel bilgisayarından yapmaya dikkat

ettiği anlaşılmıştır. Bu konuda Hiçbir zaman seçeneğini yanıtlayan katılımcıların %37,3'i 8.001-12.000 TL gelir durumuna sahip katılımcı olduğu görülmüştür.

Tablo 4.25: Katılımcıların gelir durumu ile (E-posta, sosyal ağ vb.) Sanal şifrelerini düzenli olarak değiştirme durumları ile arasındaki ilişki

x^2=24,982**		**GELİR DURUMU**			
P=0,015*		**0-4.000 TL**	**4.000 -8.000 TL**	**8.001-12.000 TL**	**12.000 TL Ve üstü**
(E-posta, sosyal ağ vb.) Sanal şifrelerimi düzenli olarak değiştiririm.	**Hiçbir zaman**	26	34	46	13
		21,8%	28,6%	38,7%	10,9%
	Nadiren	37	113	133	48
		11,2%	34,1%	40,2%	14,5%
	Ara sıra	6	47	40	20
		5,3%	41,6%	35,4%	17,7%
	Sık sık	18	54	65	26
		11,0%	33,1%	39,9%	16,0%
	Her zaman	13	49	51	31
		9,0%	34,0%	35,4%	21,5%

Tablo 4.25 Katılımcıların gelir durumu ile (E-posta, sosyal ağ vb.) Sanal şifrelerini düzenli olarak değiştirme durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların "Sanal şifrelerimi düzenli olarak değiştiririm." sorusuna 870 katılımcıdan 331 katılımcı nadiren olarak cevaplamıştır. Bu sonuçlara göre katılımcıların çoğunluğunun sanal şifrelerinin düzenli olarak değiştirme konusunda çok hassas olmadıkları anlaşılmıştır. Şifrelerinin her zaman değiştiren en çok **%35,4**

oranla 8.001-12.000 TL gelir durumuna sahip katılımcıların olduğu, her zaman değiştirenlerde **%9,0** oranla en az değiştiren 0-4.000 TL gelir durumuna sahip olanlar oldukları görülmüştür.

Tablo 4.26: Katılımcıların gelir durumu ile elektronik cihazlarına uygulamaları yüklerken üreticinin orijinal sitesi olmasına dikkat etme durumları ile arasındaki ilişki

x^2=21,767**		**GELİR DURUMU**			
P=0,040*		**0-4.000 TL**	**4.000 -8.000 TL**	**8.001-12.000 TL**	**12.000 TL Ve üstü**
Elektronik cihazlarıma uygulamaları yüklerken üreticinin orijinal sitesi olmasına dikkat ederim.	**Hiçbir zaman**	4	6	11	4
		16,0%	24,0%	44,0%	16,0%
	Nadiren	14	27	30	10
		17,3%	33,3%	37,0%	12,3%
	Ara sıra	12	31	26	3
		16,7%	43,1%	36,1%	4,2%
	Sık sık	30	84	79	38
		13,0%	36,4%	34,2%	16,5%
	Her zaman	40	149	189	83
		8,7%	32,3%	41,0%	18,0%

Tablo 4.26 Katılımcıların gelir durumu ile elektronik cihazlarına uygulamaları yüklerken üreticinin orijinal sitesi olmasına dikkat etme durumları ile arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır($p<0,05$). Araştırmaya katılan çalışanların "Elektronik cihazlarıma uygulamaları yüklerken üreticinin orijinal sitesi olmasına dikkat ederim." sorusuna 870 katılımcıdan 461 katılımcı her zaman, 231 katılımcı da sık sık olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu Elektronik cihazlarına uygulamaları yüklerken üreticinin orijinal

sitesi olmasına dikkat ettikleri görülmüştür. 8.001-12.000 TL gelir grubuna sahip katılımların **%41,0** oranla her zaman Elektronik cihazlarına uygulamaları üreticinin sitesinden yükledikleri görülmüştür.

Tablo 4.27: Katılımcıların gelir durumu ile kabul etmek istemedikleri e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösterme durumları ile arasındaki ilişki

x^2=32,761**		**GELİR DURUMU**			
P=0,001*		**0-4.000 TL**	**4.000-8.000 TL**	**8.001-12.000 TL**	**12.000 TL Ve üstü**
Kabul etmek istemediğim e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösteririm.	**Hiçbir zaman**	17	30	33	7
		19,5%	34,5%	37,9%	8,0%
	Nadiren	25	69	57	21
		14,5%	40,1%	33,1%	12,2%
	Ara sıra	9	31	49	9
		9,2%	31,6%	50,0%	9,2%
	Sık sık	21	78	80	34
		9,9%	36,6%	37,6%	16,0%
	Her zaman	28	89	116	67
		9,3%	29,7%	38,7%	22,3%

Tablo 4.27 Katılımcıların gelir durumu ile kabul etmek istemedikleri e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösterme durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların "Kabul etmek istemediğim e-postaları "spam /gereksiz/önemsiz" olarak işaretlemeye özen gösteririm." sorusuna 870 katılımcıdan 300 katılımcı her zaman, 213 katılımcı da sık sık olarak

yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu bu konuda dikkatli oldukları görülmüştür.

Tablo 4.28: Katılımcıların gelir durumu ile katılımcılara ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösterme durumları ile arasındaki ilişki

x^2=26,779**		**GELİR DURUMU**			
P=0,008*		**0-4.000 TL**	**4.000 -8.000 TL**	**8.001-12.000 TL**	**12.000 TL Ve üstü**
Bana ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösteririm.	**Hiçbir zaman**	4	10	14	2
		13,3%	33,3%	46,7%	6,7%
	Nadiren	12	38	40	9
		12,1%	38,4%	40,4%	9,1%
	Ara sıra	16	31	31	2
		20,0%	38,8%	38,8%	2,5%
	Sık sık	23	90	104	53
		8,5%	33,3%	38,5%	19,6%
	Her zaman	45	128	146	72
		11,5%	32,7%	37,3%	18,4%

Tablo 4.28 Katılımcıların gelir durumu ile katılımcılara ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösterme durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların "Bana ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösteririm ." sorusuna 870 katılımcıdan 391 katılımcı her zaman, 30 katılımcı ise hiçbir zaman olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu kendilerine ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen

gösterdikleri anlaşılmıştır. **%37,3** oranla her zaman özen gösteren 8.001-12.000 TL gelir durumuna sahip katılımcı grubunun olduğu görülmüştür.

Tablo 4.29: Katılımcıların gelir durumu ile çevrelerindeki insanlar ile beraber çektirdikleri fotoğraflarını sosyal paylaşım sitelerinde yayınlama durumları ile arasındaki ilişki

x^2=29,094**		**GELİR DURUMU**			
P=0,004*		**0-4.000 TL**	**4.000 -8.000 TL**	**8.001-12.000 TL**	**12.000 TL Ve üstü**
Çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım.	**Hiçbir zaman**	18	44	78	29
		10,7%	26,0%	46,2%	17,2%
	Nadiren	44	153	177	78
		9,7%	33,8%	39,2%	17,3%
	Ara sıra	13	23	18	11
		20,0%	35,4%	27,7%	16,9%
	Sık sık	22	57	45	10
		16,4%	42,5%	33,6%	7,5%
	Her zaman	3	20	17	10
		6,0%	40,0%	34,0%	20,0%

Tablo 4.29 Katılımcıların gelir durumu ile çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlama arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır. ($p<0,05$).Araştırmaya katılan çalışanların "Çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım." sorusuna 870 katılımcıdan 169 katılımcı hiç bir zaman, 452 katılımcının nadiren, 50 katılımcının ise her zaman olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu Çevresindeki insanlar

ile beraber çektirdikleri fotoğrafları sosyal paylaşım sitelerinde yayınlama konusuna özen gösterdikleri anlaşılmıştır.

Tablo 4.30: Katılımcıların gelir durumu ile kişisel verilerin korunması hakkındaki eğitimlere katılma durumları ile arasındaki ilişki

x^2=40,615**		**GELİR DURUMU**			
P=0,000*		**0-4.000 TL**	**4.000 -8.000 TL**	**8.001-12.000 TL**	**12.000 TL Ve üstü**
Kişisel verilerin korunması hakkındaki eğitimlere katılırım.	**Hiçbir zaman**	45	98	79	28
		18,0%	39,2%	31,6%	11,2%
	Nadiren	36	117	141	53
		10,4%	33,7%	40,6%	15,3%
	Ara sıra	9	21	23	14
		13,4%	31,3%	34,3%	20,9%
	Sık sık	7	37	49	17
		6,4%	33,6%	44,5%	15,5%
	Her zaman	3	24	43	26
		3,1%	25,0%	44,8%	27,1%

Tablo 4.30 Katılımcıların gelir durumu ile kişisel verilerin korunması hakkındaki eğitimlere katılma arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır. ($p<0,05$). Araştırmaya katılan çalışanların "Kişisel verilerin korunması hakkındaki eğitimlere katılırım." sorusuna 870 katılımcıdan 347 katılımcı nadiren , 250 katılımcının hiçbir zaman olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu Kişisel verilerin korunması hakkındaki eğitimlere az katıldığı anlaşılmıştır.

4.4.SİBER GÜVENLİK FARKINDALIĞININ EĞİTİME GÖRE FARKILAŞIP FARKLILAŞMADIĞI Kİ KARE TESTİ İLE İNCELENMESİ

Tablo 4.31: Katılımcıların eğitim durumu ile kullandıkları elektronik cihazlarda anti-virüs yazılımı bulundurma durumları ile arasındaki ilişki

$\chi^{2=}$63,404**		EĞİTİM DURUMU					
p=0,000*		ORTA OKUL	LİSE	ÖN LİSANS	LİSANS	YÜKSEK LİSANS	DOKTORA
Kullandığım elektronik cihazlarda anti-virüs yazılımı programı bulundururum.	Hiçbir zaman	2	9	15	37	13	0
		2,6%	11,8%	19,7%	48,7%	17,1%	0,0%
	Nadiren	1	25	15	137	41	7
		0,4%	11,1%	6,6%	60,6%	18,1%	3,1%
	Ara sıra	1	5	1	49	15	1
		1,4%	6,9%	1,4%	68,1%	20,8%	1,4%
	Sık sık	1	4	17	176	70	11
		0,4%	1,4%	6,1%	63,1%	25,1%	3,9%
	Her zaman	1	25	16	121	52	2
		0,5%	11,5%	7,4%	55,8%	24,0%	0,9%

Tablo 4.31 Katılımcıların eğitim durumu ile kullandıkları elektronik cihazlarda anti-virüs yazılımı bulundurma durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Katılımcıların kullandıkları elektronik cihazlarda anti -virüs yazılımı bulundurma durumuna "sık sık" yanıtı alınanların %**63,1**' inin eğitim düzeyi lisans iken, en az oranı %**0,4** ile eğitim durumu ortaokul olanların oluşturduğu görülmüştür. Yine "her zaman" yanıtı alınan yüzdelik dilimlere bakıldığında, eğitim durumu lisans olanların anti virüs kullanım oranının en fazla olduğu, bunu yüksek lisans ve ön lisansın takip ettiği görülmüş olmakla

birlikte genellikle eğitim durumu doktora olanların kullanım oranlarında beklenin aksine yüksek lisans olan katılımcılara göre düşük yüzdelikler gözlemlenmiştir.

Tablo 4.32: Katılımcıların eğitim durumu ile internet ortamında kullandıkları kullanıcı şifrelerinin aynı olmamasına dikkat etme durumları ile arasındaki ilişki

x^2=49,931**		**EĞİTİM DURUMU**					
P=0,000*		**ORTA OKUL**	**LİSE**	**ÖN LİSANS**	**LİSANS**	**YÜKSEK LİSANS**	**DOKTORA**
İnternet ortamında kullandığım kullanıcı şifrelerinin aynı olmamasına dikkat ederim.	**Hiçbir zaman**	2	9	8	60	30	3
		1,8%	8,0%	7,1%	53,6%	26,8%	2,7%
	Nadiren	1	16	13	156	54	7
		0,4%	6,5%	5,3%	63,2%	21,9%	2,8%
	Ara sıra	0	5	0	74	16	2
		0,0%	5,2%	0,0%	76,3%	16,5%	2,1%
	Sık sık	2	12	18	135	59	7
		0,9%	5,2%	7,7%	57,9%	25,3%	3,0%
	Her zaman	1	26	25	95	32	2
		0,6%	14,4%	13,8%	52,5%	17,7%	1,1%

Tablo 4.32 Katılımcıların eğitim durumu ile internet ortamında kullandıkları kullanıcı şifrelerinin aynı olmamasına dikkat etme durumları arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır. ($p<0,05$). İnternet ortamında kullanılan şifrelerin aynı kullanımı ile ilgili tabloda yapılan incelemede, eğitim durumu ortaokul ve doktora düzeyinde olanlarda genellikle diğer eğitim düzeylerine göre düşük oranlar görülmüştür. Eğitim durumu lisans olan 135 kişi tarafından internet ortamında kullanılan şifrelerin aynı olmamasına dikkat edildiği

gözlemlenmiş iken 59 kişi ile yüksek lisans, 18 kişi ile ön lisans eğitimindekiler şeklinde sıralanmıştır.

Tablo 4.33: Katılımcıların eğitim durumu ile internetten yaptıkları bankacılık işlemlerini kişisel bilgisayarlarından da yapma durumları ile arasındaki ilişki

x^2=36,096**		EĞİTİM DURUMU					
P=0,015*		ORTA OKUL	LİSE	ÖN LİSANS	LİSANS	YÜKSEK LİSANS	DOKTORA
İnternetten yaptığım bankacılık işlemlerini kişisel bilgisayarımdan yaparım.	Hiçbir zaman	2	19	14	72	20	2
		1,6%	14,7%	10,9%	55,8%	15,5%	1,6%
	Nadiren	2	18	10	86	34	7
		1,3%	11,5%	6,4%	54,8%	21,7%	4,5%
	Ara sıra	0	4	3	30	10	1
		0,0%	8,3%	6,3%	62,5%	20,8%	2,1%
	Sık sık	2	7	13	140	44	3
		1,0%	3,3%	6,2%	67,0%	21,1%	1,4%
	Her zaman	0	20	24	192	83	8
		0,0%	6,1%	7,3%	58,7%	25,4%	2,4%

Tablo 4.33 Katılımcıların eğitim durumu ile internetten yaptıkları bankacılık işlemlerini kişisel bilgisayarlarından da yapma durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Bankacılık işlemlerinin kişisel bilgisayarlardan yapılma durumları tabloda incelendiğinde, **%58,7** oranı ile "her zaman" cevabında bulunanların eğitim durumlarının lisans olduğu, bununla birlikte eğitim durumu ortaokul olanların hiçbirinin bankacılık işlemleri için kendi bilgisayarlarını kullanmadıkları gözlemlenmiştir. Eğitim

durumu ile bankacılık işlemlerindeki şahsi bilgisayar kullanma durumunda genellikle doğru orantılı bir artış olduğu verilerden tespit edilmiştir.

Tablo 4.34: Katılımcıların eğitim durumu ile siber güvenlik farkındalık eğitimlerine katılma durumları ile arasındaki ilişki

x^2=34,041**		**EĞİTİM DURUMU**					
P=0,026*		**ORTA OKUL**	**LİSE**	**ÖN LİSANS**	**LİSANS**	**YÜKSEK LİSANS**	**DOKTORA**
Siber güvenlik farkındalık eğitimlerine katılırım.	**Hiçbir zaman**	4	36	29	228	67	6
		1,1%	9,7%	7,8%	61,6%	18,1%	1,6%
	Nadiren	1	21	20	166	82	10
		0,3%	7,0%	6,7%	55,3%	27,3%	3,3%
	Ara sıra	1	2	9	32	9	2
		1,8%	3,6%	16,4%	58,2%	16,4%	3,6%
	Sık sık	0	2	4	59	15	2
		0,0%	2,4%	4,9%	72,0%	18,3%	2,4%
	Her zaman	0	7	2	35	18	1
		0,0%	11,1%	3,2%	55,6%	28,6%	1,6%

Tablo 4.34 Katılımcıların eğitim durumu ile siber güvenlik farkındalık eğitimlerine katılma durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Eğitim durumu ile siber güvenlik farkındalık eğitimine katılıma ilişkin yer alan tablo incelendiğinde, en düşük yüzde eğitim durumu ortaokul olanlardan görülmüş olup, en yüksek yüzdenin ise eğitim durumu lisans olanlarda olduğu anlaşılmıştır. Söz konusu eğitime "sık sık" katılım sağlayanların **%72'sinin** lisans, **%18,3'ünün** yüksek lisans, **%4,9'unun** ise, ön lisans eğitim durumuna sahip katılımcılar olduğu görülmüştür.

Tablo 4.35: Katılımcıların eğitim durumu ile bilgisayarlarında başkalarının flash belleklerini kullanma durumları ile arasındaki ilişki

x^2=53,701**		EĞİTİM DURUMU					
P=0,000*		ORTA OKUL	LİSE	ÖN LİSANS	LİSANS	YÜKSEK LİSANS	DOKTORA
Bilgisayarımda başkalarının flash belleklerini kullanırım.	Hiçbir zaman	3	43	30	162	50	4
		1,0%	14,7%	10,3%	55,5%	17,1%	1,4%
	Nadiren	3	24	30	279	114	13
		0,6%	5,2%	6,5%	60,3%	24,6%	2,8%
	Ara sıra	0	1	2	23	10	3
		0,0%	2,6%	5,1%	59,0%	25,6%	7,7%
	Sık sık	0	0	2	43	13	0
		0,0%	0,0%	3,4%	74,1%	22,4%	0,0%
	Her zaman	0	0	0	13	4	1
		0,0%	0,0%	0,0%	72,2%	22,2%	5,6%

Tablo 4.35 Katılımcıların eğitim durumu ile bilgisayarlarında başkalarının flash belleklerini kullanma durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Eğitim durumlarına göre bilgisayarlarında başkalarına ait flash bellek kullanma durumlarına ilişkin tablo incelendiğinde, "her zaman" yanıtını veren orta okul, lise, ön lisans durumunda kişi bulunmazken **%72,2** ile en yüksek yüzdeyi lisans durumundakilerin oluşturduğu görülmüştür. Aynı şekilde "hiçbir zaman" yanıtında da 162 kişi ile en yüksek sayıyı eğitim durumu lisans olanların oluşturduğu anlaşılmıştır. Bu durumunda başkalarına ait flash bellekleri bilgisayarlarında kullananlar eğitim durumları açısından büyük bir yüzdesi kapsamış olsa da bu duruma dikkat edenlerin sayısının da 162 ile oldukça yüksek olduğu görülmüştür.

Tablo 4.36: Katılımcıların eğitim durumu ile siber saldırıya maruz kalma durumları ile arasındaki ilişki

x^2=44,630**		EĞİTİM DURUMU					
P=0,001*		ORTA OKUL	LİSE	ÖN LİSANS	LİSANS	YÜKSEK LİSANS	DOKTORA
Siber saldırıya maruz kaldım.	Hiçbir zaman	6	57	50	367	133	10
		1,0%	9,1%	8,0%	58,9%	21,3%	1,6%
	Nadiren	0	11	12	140	51	7
		0,0%	5,0%	5,4%	63,3%	23,1%	3,2%
	Ara sıra	0	0	2	9	4	4
		0,0%	0,0%	10,5%	47,4%	21,1%	21,1%
	Sık sık	0	0	0	3	1	0
		0,0%	0,0%	0,0%	75,0%	25,0%	0,0%
	Her zaman	0	0	0	1	2	0
		0,0%	0,0%	0,0%	33,3%	66,7%	0,0%

Tablo 4.36 Katılımcıların eğitim durumu ile siber saldırıya maruz kalma durumları ile arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır. ($p<0,05$). Siber saldırıya maruz kalma durumuna ilişkin tablo üzerinden yapılan incelemede, eğitim durumu lisans ve yüksek lisans olanların yüksek oranlarda maruz kaldığı görülmüş iken ortaokul, lise, ön lisans ve doktorada "sık sık" ve "her zaman" yanıtı alınan kişi olmadığı gözlemlenmiştir.

Tablo 4.37: Katılımcıların eğitim durumu ile sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddetme durumları ile arasındaki ilişki

x^2=41,940**		EĞİTİM DURUMU					
P=0,003*		ORTA OKUL	LİSE	ÖN LİSANS	LİSANS	YÜKSEK LİSANS	DOKTORA
Sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddederim.	Hiçbir zaman	1	3	2	8	2	0
		6,3%	18,8%	12,5%	50,0%	12,5%	0,0%
	Nadiren	0	17	4	47	16	2
		0,0%	19,8%	4,7%	54,7%	18,6%	2,3%
	Ara sıra	0	2	5	26	10	3
		0,0%	4,3%	10,9%	56,5%	21,7%	6,5%
	Sık sık	0	10	16	108	32	5
		0,0%	5,8%	9,4%	63,2%	18,7%	2,9%
	Her zaman	5	36	37	331	131	11
		0,9%	6,5%	6,7%	60,1%	23,8%	2,0%

Tablo 4.37 Katılımcıların eğitim durumu ile sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddetme durumları ile arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmektedir. ($p<0,05$). Araştırmaya katılan çalışanların "Sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddederim." sorusuna 870 katılımcıdan 551 katılımcı her zaman, 16 katılımcı ise hiçbir zaman olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddetme konusunda özen gösterdikleri anlaşılmıştır.

Tablo 4.38: Katılımcıların eğitim durumu ile bilgisayarlarında şifreli ekran koruyucusu kullanmaya özen gösterme durumları ile arasındaki ilişki

x^2=31,816**		EĞİTİM DURUMU					
P=0,045*		ORTA OKUL	LİSE	ÖNLİSANS	LİSANS	YÜKSEK LİSANS	DOKTORA
Bilgisayarımda şifreli ekran koruyucusu kullanmaya özen gösteririm.	Hiçbir zaman	2	12	8	74	22	9
		1,6%	9,4%	6,3%	58,3%	17,3%	7,1%
	Nadiren	1	11	5	57	19	2
		1,1%	11,6%	5,3%	60,0%	20,0%	2,1%
	Ara sıra	0	7	6	47	12	4
		0,0%	9,2%	7,9%	61,8%	15,8%	5,3%
	Sık sık	1	7	10	88	41	2
		0,7%	4,7%	6,7%	59,1%	27,5%	1,3%
	Her zaman	2	31	35	254	97	4
		0,5%	7,3%	8,3%	60,0%	22,9%	0,9%

Tablo 4.38 Katılımcıların eğitim durumu ile bilgisayarlarında şifreli ekran koruyucusu kullanmaya özen gösterme ile arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır. ($p<0,05$). Bilgisayarlarında şifreli ekran koruyucu kullanımına özen gösterme ile eğitim durumları arasındaki bağlantıları gösteren tablo incelendiğinde, genellikle eğitim durumu lise ve ön lisans olanların dikkat etme oranları birbirine yakın seyrederken en yüksek özen gösterenlerin eğitim durumu lisans olanlar olduğu gözlenmiştir. Eğitim durumu ortaokul ve doktora olanların birbirlerine yakın oranlarda olduğu görülse de doktora durumundakilerin daha özenli olduğu görülmüştür. "Her zaman" olarak yanıt alınan 254 lisans durumundakilerin olduğu ve diğerlerine göre **%60** ile büyük bir yüzdesi oluşturduğu anlaşılmıştır.

Tablo 4.39: Katılımcıların eğitim durumu ile E-posta, forum siteleri vb. sanal şifrelerini paylaşma durumları ile arasındaki ilişki

x^2=41,209**		EĞİTİM DURUMU					
P=0,004*		ORTA OKUL	LİSE	ÖN LİSANS	LİSANS	YÜKSEK LİSANS	DOKTORA
E-posta, forum siteleri vb. sanal şifrelerimi paylaşırım.	Hiçbir zaman	5	57	57	470	164	17
		0,6%	7,4%	7,4%	61,0%	21,3%	2,2%
	Nadiren	1	5	3	35	17	1
		1,6%	8,1%	4,8%	56,5%	27,4%	1,6%
	Ara sıra	0	2	0	6	5	3
		0,0%	12,5%	0,0%	37,5%	31,3%	18,8%
	Sık sık	0	2	4	7	2	0
		0,0%	13,3%	26,7%	46,7%	13,3%	0,0%
	Her zaman	0	2	0	2	3	0
		0,0%	28,6%	0,0%	28,6%	42,9%	0,0%

Tablo 4.39 Katılımcıların yaşları ile E-posta, forum siteleri vb. sanal şifrelerini paylaşma durumları ile arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır. ($p<0,05$). Araştırmaya katılan tüm öğretim gruplarında "E-posta, forum siteleri vb. sanal şifrelerimi paylaşırım." sorusuna 870 katılımcıdan 770 katılımcı hiçbir zaman, 7 katılımcı ise her zaman olarak yanıtlamıştır.

5. TARTIŞMA VE SONUÇ

Bu çalışmada çalışanların siber güvenliği sağlama farkındalıklarının farklı değişkenler açısından belirlenmesine çalışılmıştır. Siber güvenlik alanda çalışanların, kurumun ve kurumda görev yapan diğer çalışanların dijital ortamlardaki verilerinin güvenliğini sağlamada ve siber ortamlardaki tehdit ve tehlikelerin önlenmesinde, önemli görevler üstlendiği düşünüldüğünde çalışanların farkındalıklarının ortaya konulmasının gelecekteki çalışmalara yön vereceği öngörülmektedir.

5.1.SİBER GÜVENLİK FARKINDALIĞININ CİNSİYET GÖRE İNCELENMESİ

Araştırmaya katılan çalışanların ağırlıklı olarak interneti kullanım nedenin sosyal medya olduğu, kadın ve erkek katılımcı karşılaştırıldığında kadınların interneti sosyal medya için kullanım oranı **%54,8** iken erkeklerin **%45,2** olması nedeniyle kadınların internetin kullanım amacının sosyal medya olarak gösterilmesinin erkeklerden daha yüksek oranda olduğu anlaşılmaktadır. İnternet kullanımın iş için yapılması durumu karşılaştırıldığında erkeklerin oranın kadınlardan daha fazla olduğu görülmüştür.

Elektronik cihazların yazımları güncelleme konusunda erkeklerin kadınlara göre daha çok güncelleme yaptıkları ve daha hassas oldukları, her zaman güncelleme yapan kadın ve erkek katılımcı karşılaştırıldığında kadınlarının oranının **%34,5** 'te kalırken**,** erkeklerde bu oranın **%65,5** olduğu görülmüştür. Erkek katılımcılar, elektronik cihazlarında kullandıkları yazılımların güncel olup olmadığını daha sık takip etmekte ve gerektiğinde güncelleme yapmaktadırlar.

Katılımcıların siber güvenlik farkındalık eğitimlere katılım konusunda cinsiyetleri arasındaki ilişki incelendiğinde erkeklerin kadınlara kıyasla siber güvenlik eğitimlere katılımının daha sık olduğu görülmüştür. Kadınların **%46,3** siber eğitimlere ara sıra katılım gösterirken, erkeklerin **%53,7**' si ara sıra katılım gösterdiği görülmüştür. Buna göre erkek katılımcıların siber güvenlik farkındalık eğitimlerine daha fazla meraklı olduğu sonucuna varılabilir. Bunun yanında, katılımcıların ağırlıklı olarak siber güvenlik eğitimlerine katılmadıkları göz önünde bulundurulmalıdır.

Çalışanların ağırlıklı olarak güvenliğinden şüphe duydukları sitelere üye olmadıkları, tüm katılımcıların tercihleri değerlendirildiğinde güvenliğinden şüphe duyulan sitelere üyeliğe az olduğu görülmektedir. Güvenliğinden şüphe duyulan sitelere üye olunmaması ilişkin kadın ve erkeklerin oranların yakın olduğu gözlenmiştir. Bu sonuca göre kadın ve erkeklerin eşit oranda şüpheli sitelerden uzak durdukları anlaşılmıştır.

Çalışanların bilgisayarında başkalarına ait flash belleklerini kullanımının az olduğu gözlemlenmiştir. Ayrıca kadınların bilgisayarlarında başkalarına ait flash belleklerini hiçbir zaman kullanılmayan katılımcıların **%54,8**'ü kadın iken **%45,2**'i erkeklerden oluştuğu görülmektedir. Bu oranlara göre kadınların erkeklere göre başkalarına ait flash belleklerin kullanmama konusunda daha hassas oldukları görülmüştür. Kadın katılımcıların kendi bilgisayarlarını koruma konusunda dikkatli oldukları anlaşılmıştır.

Araştırmaya katılan çalışan katılımcılarının büyük çoğunluğunun siber saldırıya maruz kalmadığı gözlemlenmiştir. Katılımcıların yalnızca **%28,4**'ü siber saldırıya maruz kalmıştır. Siber saldırıya maruz kalan katılımcıların arasında erkek katılımcı sayısının **153** olduğu, kadın katılımcının sayısı **94** olduğu görülmüştür. Bu sonuçlara göre erkek katılımcılara kadınlara oranlara daha çok siber saldırıya maruz kaldığı gözlemlenmiştir. Erkek katılımcıların başkalarına ait flash bellekleri kullanma gibi alışkanlıklarının kadınlara göre daha fazla olması, bu katılımcıların siber saldırılara daha fazla maruz kalmasına sebep olabilmektedir.

Araştırmaya katılan çalışanların büyük çoğunluğunun uygulamalarda şahsi bilgilerini açık onayları bulunmadan ülke dışına gönderilmesine izin vermediği gözlemlenmiştir. Bu sonuçlara göre erkek katılımcılara kadınlara oranlara daha az dikkat ettikleri görülmüştür. Katılımcıların çoğunluğunun şahsi bilgilerinin kötü amaçlı da kullanabileceği farkında olduğu bu nedenle gerekli hassasiyeti gösterdiği anlaşılmıştır.

Çalışanların **%20**'sinin "çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım" sorusuna hiçbir zaman yanıtına verdiği görülmüştür. Katılımcı çalışanların **%80'** sinin ara sıra da olsa sosyal medyada çevresindeki insanlar ile beraber çektirdiği fotoğrafların sosyal paylaşım sitelerinde paylaştıkları anlaşılmaktadır. Bu sonuçlara göre katılımcıların çevresindeki insanların kişisel verisi olan fotoğrafların başkaları tarafından

erişime açtıkları konusunda bilgili olmadıkların anlaşılmıştır. Kadın ve erkek katılımcıların karşılaştırıldığında; erkeklerin kadınlara oranla daha az paylaşım yaptıkları görülmektedir.

Çalışanların çoğunluğunun kullandığı elektronik cihazlarda arkadaşlarının ait bilgilerini tutmadığı görülmüştür. Çalışanların arkadaşlarına ait bilgileri kendi bilgisayarlarında tuttuklarında herhangi bir siber saldırı durumunda arkadaşlarının da verilerin çalınabileceğini farkında oldukları anlaşılmaktadır. İlgili soruya verilen cevaplar incelendiğinde arkadaşlarına ait bilgileri elektronik cihazlarında hiçbir zaman tutmayan kadınların oranın **%51,3,** erkeklerin ise **%48,7**'i olduğu görülmüştür. Bu sonuca göre kadınların bu konuda daha dikkatli olduğu anlaşılmıştır.

Araştırmaya katılan çalışanların **%28**'i kişisel verilerin korunması hakkındaki eğitimlere katılmadığı görülmüştür. Oranlara bakıldığında erkek katılımcıların kadın katılımcılara göre bu tür eğitimlere daha ilgili olduğu anlaşılmıştır.

5.2.SİBER GÜVENLİK FARKINDALIĞININ YAŞA GÖRE İNCELENMESİ

Çalışanların tüm yaş gruplarında ağırlıklı olarak interneti kullanım nedenin sosyal medya olduğu, daha sonra iş için kullandıkları en az ise eğitim için kullandıkları görülmüştür. Sosyal medyayı için kullanan yaş grubunun **%34,7** oranla en çok 34-40 yaş grubunun olduğu, en az kullanan yaş grubunun da 50 yaş ve üstü olduğu görülmektedir.

Çalışanların tüm yaş gruplarında olarak kullandığı elektronik cihazların yazılımları güncelleme konusunda ağırlıklı olarak ya sık sık ya da her zaman güncelleme yaptıkları görülmüştür. Yaş grupları incelendiğinde 26-33 ile 34-40 yaş arasındaki çalışanların yazılım güncelleme konusunda benzer oranda oldukları görülmüştür. **%37,6** oranla en çok 34-40 yaş grubunun olduğu her zaman güncelleme yaptıkları anlaşılmıştır. Hiçbir zaman güncelleme yapmayanların tüm yaş gruplarında çok az oldukları görülmüştür.

Çalışanların tüm yaş gruplarında olarak kullandığı elektronik cihazlarda anti-virüs programı bulundurma konusunda ağırlıklı olarak ya sık sık ya da her zaman şıklarını işaretledikleri görülmüştür. **%37,8'**lik oranla en çok 34-40 yaş grubunun elektronik cihazlarında anti-virüs programı bulundurduğu anlaşılmıştır. Hiçbir zaman haricindeki diğer seçenekleri toplandığında

18-25 yaş aralığı 74 kişiyle **%83** oranı, 26-33 yaş aralığı 206 kişiyle **%88** oranı, 34-40 yaş aralığı 286 kişiyle **%94** oranı, 41-50 yaş aralığı 168 kişiyle **%95** oranı, 50 yaş ve üstü 60 kişisiyle **%90** oranıyla anti virüs programı bulundukları görülmüştür. Bu sonuçlara göre 18-25 yaş aralığı bu konuya daha az dikkat ettikleri anlaşılmıştır.

Araştırmaya katılan çalışanların tüm yaş gruplarında olarak internetten yaptığı bankacılık işlemlerini kişisel bilgisayarlarından yapma konusunda ağırlıklı olarak kişisel bilgisayarını tercih ettikleri anlaşılmıştır. Bankacılık işlemleriyle kişilerin mali varlılarını başkalarının eline geçme konusunda tedirgin olmaları nedeniyle bu konuda tüm yaş grupların dikkatli oldukları anlaşılmıştır. **%11,0** oranla 18-25 yaş grubu ile **%10,7** oranla 50 yaş ve üstü yaş grubunun bankacılık işlemlerini her zaman kişisel bilgisayarlarından yapmadıkları görülmüştür.

Çalışanların tüm yaş gruplarında sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri çoğunlukla reddettikleri görülmüştür. Bununla birlikte, bu istekleri hiçbir zaman reddetmediğini belirten katılımcı sayısının çok az olduğu gözlemlenmiştir.

Araştırmaya katılan çalışanların tüm yaş gruplarında ağırlıklı olarak sanal şifrelerimi düzenli olarak değiştirme konusunda şifrelerini nadiren değiştikleri anlaşılmıştır. Bu sonuca göre, kişilerin sanal şifrelerini değiştirmesi için bir nedenleri olması gerektiği sonucuna varılabilir. Çünkü katılımcıların yaş aralıklarından bağımsız olarak aynı şifreleri kullanma konusunda ısrar ettikleri görülmüştür.

Çalışanların tüm yaş gruplarında ağırlıklı olarak kabul etmek istemediği e-postaları “spam /gereksiz/önemsiz” olarak işaretlemeye özen gösterdikleri anlaşılmaktadır. Çünkü her zaman seçeneğini 18-25 yaş aralığı 20 kişi, 26-33 yaş aralığı 78 kişi, 34-40 yaş aralığı 100 kişi, 41-50 yaş aralığı 70 kişi, 50 yaş ve üstü 32 kişi seçmiştir. Her zamanı seçeneğini en çok işaretleyen yaş grubu **%33,3’**lük oranla 34-40 yaş aralığı olduğu görülmüştür.

Çalışanların tüm yaş gruplarında “bana ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösteririm konusunda” 270 kişi sık sık seçeneğini, 391 kişi her zaman seçeneğini işaretlemiştir. Bu sonuçlara göre tüm katılımcıların ağırlıklı olarak kendilerine ait olmayan cihazlarda şifre isteyen işlemleri yapmadıkları anlaşılmıştır. Ayrıca 18-25 yaş aralığı

%9,5 oranla ve 50 yaş üstü çalışanların **%10,5** oranla diğer yaş gruplarına göre daha az özen gösterdikleri anlaşılmıştır.

Araştırmaya katılan çalışanların tüm yaş gruplarında uygulamalarda şahsi bilgilerin açık onayım bulunmadan ülke dışına gönderilmesine izin veririm konusunda çoğunlukla hiçbir zaman seçeneği işaretlenmiştir. Özellikle tüm yaş gruplarında bu konuda özen gösterdikleri görülmüştür. Tüm katılımların sayısı olan 870 kişiden 660 kişi hiçbir zaman seçeneği işaretlemiştir. Katılımcıların çoğunluğunun şahsi bilgilerinin kötü amaçlı da kullanabileceği farkında olduğu bu nedenle gerekli hassasiyeti gösterdiği anlaşılmıştır.

Araştırmaya katılan çalışanların çevremdeki insanlar ile beraber çektirdiğim fotoğraflarımı sosyal paylaşım sitelerinde yayınlarım konusunda nadiren seçeneği işaretlendiği görülmüştür. Bu sonuçlara göre tüm yaş gruplarında sosyal medyada çevresinde insanları paylaşmama konusunda hassas oldukları görülmüştür. Araştırmaya katılan çalışanların **%64**'ü hiçbir zaman, **%25**'i nadiren, **%4**'ü ara sıra, **%5**'i sık sık, **%1**'i de her zaman seçeneğini işaretlemiştir. Bu sonuçlara göre yaş grupların kendilerinin ve çevresindeki insanların kişisel verilere önem verdiği anlaşılmaktadır.

Araştırmaya katılan çalışanların kişisel verilerin korunması hakkındaki eğitimlere katılma konusunda hiçbir zaman ve nadiren seçeneğin işaretlediği görülmüştür. Her zaman kişisel verilerin konusunda eğitimlere katılan yaş grubunda **%36,5** oranla 34-40 yaş aralığı en çok katılandır. Eğitimlere hiçbir zaman katılmama oranı 18-25 yaş aralığında **%45** oranıyla en fazla olduğu bu nedenle 18-25 yaş aralığının bu türdeki eğitimlere daha az meraklı olduğu ya da daha az fırsat bulduğu anlaşılmıştır.

5.3.SİBER GÜVENLİK FARKINDALIĞININ GELİRE GÖRE İNCELENMESİ

Çalışanların "İnternetten yaptığım bankacılık işlemlerini kişisel bilgisayarımdan yaparım." sorusuna 870 katılımcıdan 327 katılımcı her zaman, 209 katılımcı da sık sık olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu internetten yaptığı bankacılık işlemlerini kişisel bilgisayarından yapmaya dikkat ettiği anlaşılmıştır. 8.001-12.000 TL gelir durumuna sahip katılımcıların **%35,2** oranla diğer gelir durumuna sahip katılımcılara göre daha çok bu konuda hassas oldukları görülmüştür.

Araştırmaya katılan çalışanların “Siber güvenlik farkındalık eğitimlerine katılırım.” sorusuna 870 katılımcıdan 370 katılımcı hiçbir zaman, 300 katılımcı da nadiren olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu Siber güvenlik farkındalık eğitimlerine katılmadıkları anlaşılmıştır. Gelir durumu 0-4.000 TL arasında olan katılımcıların eğitimlere her zaman katılanlar arasında en düşük orana (**%3)** sahiptir. 12.000 TL ve üstü gelire sahip olan katılımcılar **%17’**lik oranla en yüksek orana sahiptir. Buna göre gelir durumu yükseldikçe eğitimlere katılım oranı artmaktadır.

Araştırmaya katılan çalışanların “Sanal şifrelerimi düzenli olarak değiştiririm.” sorusuna 870 katılımcıdan 331 katılımcı nadiren olarak cevaplamıştır. Bu sonuçlara göre katılımcıların çoğunluğunun sanal şifrelerinin düzenli olarak değiştirme konusunda çok hassas olmadıkları anlaşılmıştır. Şifrelerinin her zaman değiştiren en çok **%35,4** oranla 8.001-12.000 TL gelir durumuna sahip katılımcıların olduğu, her zaman değiştirenlerde **%9,0** oranla en az değiştiren 0-4.000 TL gelir durumuna sahip olanlar oldukları görülmüştür.

Çalışanların çoğunluğunun elektronik cihazlarına uygulamaları yüklerken üreticinin orijinal sitesi olmasına dikkat ettikleri görülmüştür. Geliri 8000 TL üstünde olan katılımcılar ile 8000 TL altında olanlar karşılaştırıldığı geliri 8000 TL üstünde olanlar daha hassas oldukları anlaşılmıştır.

Araştırmaya katılan çalışanların “Kabul etmek istemediğim e-postaları “spam /gereksiz/önemsiz” olarak işaretlemeye özen gösteririm.” sorusuna 870 katılımcıdan 300 katılımcı her zaman, 213 katılımcı da sık sık olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu bu konuda dikkatli oldukları görülmüştür.

Araştırmaya katılan çalışanların “Bana ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösteririm.” sorusuna 870 katılımcıdan 391 katılımcı her zaman, 30 katılımcı ise hiçbir zaman olarak yanıtlamıştır. Bu sonuçlara göre, katılımcıların çoğunluğu kendilerine ait olmayan cihazlarda şifre isteyen işlemler yapmamaya özen gösterdikleri anlaşılmıştır. **%37,3** oranla her zaman özen gösteren katılımcıların 8.001-12.000 TL gelir durumuna sahip katılımcı grubu olduğu görülmüştür.

Çalışanların çoğunluğunun çevresindeki insanlar ile beraber çektirdikleri fotoğrafları sosyal paylaşım sitelerinde yayınlama konusuna özen gösterdikleri anlaşılmıştır. Gelir durumuna göre

karşılaştırma yapıldığında paylaşmama konusunda oranların birbirine yakın olduğu görülmüştür.

Araştırmaya katılan çalışanların "Kişisel verilerin korunması hakkındaki eğitimlere katılırım." sorusuna 870 katılımcıdan 347 katılımcı nadiren, 250 katılımcının hiçbir zaman olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu kişisel verilerin korunması hakkındaki eğitimlere katılmadığı anlaşılmıştır. Hiçbir zaman katılmayanların gelir duruma karşılaştırıldığında gelir azaldıkça katılmama oranının arttığı görülmüştür.

5.4.SİBER GÜVENLİK FARKINDALIĞININ EĞİTİME GÖRE İNCELENMESİ

Genel olarak, katılımcı çalışanların eğitim durumu yükseldikçe, elektronik cihazlarında anti-virüs yazılımı programı bulundurma oranları yükselmektedir. Buna göre, eğitim durumu ortaokul mezunu olan katılımcıların yalnızca **%33,3**'ü elektronik cihazlarında anti-virüs yazılımı programı bulundurma seçeneğini her zaman veya sık sık olarak işaretlerken, bu oran eğitim durumu yüksek lisans ve doktora mezuniyeti olan katılımcılarda sırasıyla **%63,9** ve **%61,9** olarak ölçümlenmiştir.

Katılımcıların kullandıkları elektronik cihazlarda anti -virüs yazılımı bulundurma durumuna "sık sık" yanıtı alınanların **%63,1** inin eğitim düzeyi lisans iken, en az oranı **%0,4** ile eğitim durumu ortaokul olanların oluşturduğu görülmüştür. Yine "her zaman" yanıtı alınan yüzdelik dilimlere bakıldığında, eğitim durumu lisans olanların anti virüs kullanım oranının en fazla olduğu, bunu yüksek lisans ve ön lisansın takip ettiği görülmüş olmakla birlikte genellikle eğitim durumu doktora olanların kullanım oranlarında beklenin aksine eğitim durumu yüksek lisans olan katılımcılara göre düşük yüzdelikler gözlemlenmiştir. Bu bölümde yapılan araştırmaya göre, katılımcıların elektronik cihazlarında anti-virüs programı bulundurma istekleri gördükleri eğitim süresine göre paralel şekilde artmaktadır.

İnternet ortamında kullanılan şifrelerin aynı kullanımı ile ilgili tabloda yapılan incelemede, eğitim durumu ortaokul ve doktora düzeyinde olanlarda genellikle diğer eğitim düzeylerine göre düşük oranlar görülmüştür. Eğitim durumu lisans olan 135 kişi tarafından internet ortamında kullanılan şifrelerin aynı olmamasına dikkat edildiği gözlemlenmiş iken 59 kişi ile yüksek lisans, 18 kişi ile ön lisans eğitimindekiler şeklinde sıralanmıştır.

İnternet ortamında kullanılan şifrelerin aynı olmaması durumunun katılımcıların eğitim durumlarında gözlemlenen farklılıklara göre dağılmadığı anlaşılmaktadır. Özetle katılımcıların en düşük eğitim düzeyi olan ortaokul mezuniyetinde internet ortamında kullanılan şifreler sürekli aynı şifreler olmamakla birlikte, eğitim durumu yüksek lisans veya doktora olan katılımcılarda internet ortamında kullanılan şifrelerin genellikle aynı şifre olduğu görülmektedir. Bu sebeple, katılımcıların eğitim hayatında geçirdikleri sürelerin internet ortamında kullandıkları şifreleri farklılaştırma eğilimlerine bir katkısı bulunmadığı söylenebilir.

Bankacılık işlemlerinin kişisel bilgisayarlardan yapılma durumları tabloda incelendiğinde, **%58,7** oranı ile "her zaman" cevabında bulunanların eğitim durumlarının lisans olduğu, bununla birlikte eğitim durumu ortaokul olanların hiçbirinin bankacılık işlemleri için kendi bilgisayarlarını kullanmadıkları gözlemlenmiştir. Eğitim durumu ile bankacılık işlemlerindeki şahsi bilgisayar kullanma durumunda genellikle doğru orantılı bir artış olduğu verilerden tespit edilmiştir. Bunun yanında eğitim durumu doktora mezuniyeti olanların, kişisel bilgisayarlarında internet bankacılığı işlemleri yapma oranlarının (sık sık ve her zaman) eğitim durumları yüksek lisans, lisans ve lise olanlardan daha düşük olduğu görülmektedir. Bunun sebebi, doktora mezunu katılımcıların, diğer katılımcılara oranla, kişisel bilgisayarlarının siber güvenliği konusuna yeterince güvenmemeleri olabilir. Örneğin bu durum doktoralı katılımcılar bu bölümde anlatıldığı üzere aynı şifreleri farklı internet ortamlarında kullanmaları veya elektronik cihazlarında anti-virüs programı bulundurma konusunda daha az çaba sarf etmeleri bu durumun sebeplerini oluşturuyor olabilir.

Eğitim durumu ile siber güvenlik farkındalık eğitimine katılıma ilişkin yer alan tablo incelendiğinde, en düşük yüzde eğitim durumu ortaokul olanlardan görülmüş olup, en yüksek yüzdenin ise eğitim durumu lisans olanlarda olduğu anlaşılmıştır. Söz konusu eğitime "sık sık" katılım sağlayanların **%72**'sinin lisans, **%18,3**'ünün yüksek lisans, **%4,9'**unun ise, ön lisans eğitim durumuna sahip katılımcılar olduğu görülmüştür. Bunun yanında tüm katılımcıların genellikle siber güvenlik eğitimlerine katılmadığı anlaşılmaktadır. Katılımcıların **%77'**isinin hiçbir zaman siber güvenlik eğitimi almadığı anlaşılmaktadır. Katılımcıların her eğitim seviyesinde siber eğitim açığının olduğu görülmektedir.

Eğitim durumlarına göre bilgisayarlarında başkalarına ait flash bellek kullanma durumlarına ilişkin tablo incelendiğinde, "her zaman" yanıtını veren orta okul, lise, ön lisans durumunda kişi bulunmazken **%72,2** ile en yüksek yüzdeyi lisans durumundakilerin oluşturduğu görülmüştür.

Aynı şekilde "hiçbir zaman" yanıtında da 162 kişi ile en yüksek sayıyı eğitim durumu lisans olanların oluşturduğu anlaşılmıştır. Bu durumunda başkalarına ait flash bellekleri bilgisayarlarında kullananlar eğitim durumları açısından büyük bir yüzdesi kapsamış olsa da bu duruma dikkat edenlerin sayısının da 162 ile oldukça yüksek olduğu görülmüştür. Bunun yanında, katılımcıların eğitim oranı arttıkça, başkalarına ait flash belleklerin kullanım oranında artış görülmüştür. Bunun sebebi, eğitim durumunun artmasıyla birlikte, flash bellek gibi elektronik cihazların kullanımında yaşanan artış olarak gösterilebilir.

Siber saldırıya maruz kalma durumuna ilişkin tablo üzerinden yapılan incelemede, genel olarak katılımcıların eğitim durumundan bağımsız olacak şekilde siber saldırıya maruz kalma oranları çok düşüktür. Bunun yanında, ara sıra da olsa siber saldırılara maruz kalma oranı eğitim durumu lisans ve yüksek lisans olan katılımcılarda daha yüksektir. Katılımcılardan eğitim durumu ortaokul, lise, ön lisans ve doktora olanlarda "sık sık" ve "her zaman" yanıtı alınan kişi olmadığı gözlemlenmiştir. Katılımcıların eğitim sürelerinde yaşanan artışla birlikte siber saldıra ara-sıra da olsa maruz kalma durumu, bu katılımcıların internet ortamında daha fazla işlem yapmaları (örneğin internet bankacılığı, birden fazla kullanıcı hesabı ve şifreleri oluşturmaları gerektiren internet siteleri vb.) olabilir.

Araştırmaya katılan çalışanların "Sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddederim." sorusuna 870 katılımcıdan 551 katılımcı her zaman, 16 katılımcı ise hiçbir zaman olarak yanıtlamıştır. Bu sonuçlara göre katılımcıların çoğunluğu sosyal medya hesaplarında tanımadığı kişilerden gelen istekleri reddetme konusunda özen gösterdikleri anlaşılmıştır. Bunun yanında, ara sıra da olsa tanımadığı kişilerden gelen sosyal medya isteklerini kabul etme oranı eğitim durumu ortaokul ve lise olan katılımcılarda daha yüksektir. Bilgisayarlarında şifreli ekran koruyucu kullanımına özen gösterme ile eğitim durumları arasındaki bağlantıları gösteren tablo incelendiğinde, genellikle eğitim durumu lise ve ön lisans olanların dikkat etme oranları birbirine yakın seyrederken en yüksek özen gösterenlerin eğitim durumu lisans olanlar olduğu gözlenmiştir. Eğitim durumu ortaokul ve doktora olanların birbirlerine yakın oranlarda olduğu görülse de doktora durumundakilerin daha özenli olduğu görülmüştür. Genel olarak katılımcıların eğitim süresinde görülen artış ile bilgisayarlarında şifreli ekran koruyucu kullanmaları oranın artığı anlaşılmaktadır.

Araştırmaya katılan tüm öğrenim gruplarında "E-posta, forum siteleri vb. sanal şifrelerimi paylaşırım." sorusuna 870 katılımcıdan 770 katılımcı hiçbir zaman, 7 katılımcı ise her zaman

olarak yanıtlamıştır. Bu kapsamda, katılımcıların büyük çoğunluğu e-posta, forum siteleri vb. sanal şifrelerini paylaşmamaktadır. Ancak eğitim durumu daha yüksek olan katılımcıların bu tür şifreleri paylaşma oranlarının arttığı görülmektedir. Bu durumun sebebi olarak, eğitim durumu daha yüksek olan katılımcıların, iş, okul ve benzeri ortamlarda daha fazla insan ile iletişimde olmaları ve bu kişiler ile birlikte internet ortamında bulunan e-posta, blog vb. internet ortamlarına dahil olmaları olabilir.

5.5.ÖNERİLER-TESPİTLER

Yapılan araştırmada elde edilen bulgular sonucunda aşağıdaki öneriler getirilmiştir:

- Yaşlı insanlar için kullanıcı dostu ve daha az adım içeren uygulamalar geliştirilebilir.
- Kullanıcının yaşına göre dizayn edilmiş uygulamalar (örneğin: bankacılık uygulamasında genç insanlar için sosyal medya, telefon ödemesi, netflix vb. varken, daha yaşlılarda yatırım seçenekleri, dijital destek sağlayan bankacılık uygulaması) geliştirilebilir.
- Gençler için sosyal medya eğitimi verilebilir.
- İnternet kullanımıyla paralel daha gençken insanları internetle tanıştırılabilir.
- Daha genç insanlar eğitime açık internetten ücretsiz eğitim verilebilir.
- Kadınlara yönelik eğitimler, uygulamalar, sosyal medya eğitimi verilebilir.
- Erkek çalışanları kişisel siber güvenlik farkındalığı kadın çalışanlara göre genellikle daha yüksek çıkmıştır. Buna göre kadın çalışanların internet kullanımı teşvik edilerek kişisel siber güvenliği sağlama farkındalıkları arttırılabilir.
- Kullanıcının cinsiyetine göre dizayn edilmiş uygulamalar (örneğin: sosyal medyada kadınlar daha çok paylaşımcı, burada paylaşıma engel olmayan ancak kişisel verileri daha sıkı koruyan -örnek paylaşmayı onaylıyor musun vb. sorular) geliştirilebilir.
- Eğitim düzeyi düşük olanlara da basitte olsa kişisel veri, paylaşım, siber güvenlik eğitimleri verilebilir.
- Siber güvenlik farkındalığı sağlamak adına kamusal duyurular etkili olabilir. (Cep telefonuna gelen mesajlar)
- Bu araştırmada nicel araştırma yöntemleri kullanıldığı için ileriye dönük araştırmalarda nitel araştırma yöntemleri de kullanılarak çalışanların siber güvenlik bilinç, farkındalık ve davranışları ayrıntılı bir biçimde incelenebilir.

- Bu çalışmada sadece çalışan insanlar incelenmiştir. Çalışmayan öğrenciler, ev hanımları gibi çalışmayan kesimde bulunan kişiler araştırılmalıdır. Bunun yanında çalışanların içinde farklı sektör/meslek grupları için de bu çalışma yapılmalıdır.
- Türkiye geneli daha kapsamlı bir çalışma yapılmalıdır. Araştırmaya katılımı arttırmak için web siteleri oluşturulmalı, kitle iletişim alanlarıyla duyurular yapılmalıdır. Ayrıca, katılımcıların internet ve elektronik cihaz kullanımlarına yönelik alışkanlıkları da çalışmaya dahil edilmelidir.
- İnternet kullanma sıklığı arttıkça ve teknoloji ilerledikçe kişisel siber güvenlik farkındalıkları da artmaktadır. Bundan dolayı interneti az kullananların hangi uygulamaları veya web sitelerini kullandıkları tespit edilip, o sitelerde kişisel siber güvenliği sağlama ile ilgili kamu spotlarının paylaşılması gerekmektedir.
- Cengiz Gündüz Alp (2021) tarafından yapılan "Üniversite Çalışanlarının Dijital Veri ve Kişisel Siber Güvenlik Farkındalıkları (Bilgi İşlem Daire Başkanlıkları Örneği)" isimli çalışma yapılmıştır. Bu çalışmada Türkiye'deki üniversitelerin bilgi işlem daire başkanlıklarında çalışanların dijital veri güvenliği ve siber güvenliği farkındalığı incelenmiş olup kadın ve erkek çalışanların siber güvenlik farkındalıkları karşılaştırıldığında bilgi işlem alanında çalışan kadın çalışanların dijital veri güvenlik farkındalıklarının erkek çalışanlara göre daha yüksek olduğu görülmüştür. Ancak yapmış olduğumuz çalışmada daha geniş sektörlerde çalışanlar incelenmiş olup çalışma sonucunda erkek çalışanların birbirine yakın cevaplar verdiği görülmüştür. Ancak erkek çalışanların kadın çalışanlara oranla siber güvenlik eğitimlerine katılımının, cihaz güncelleme hassasiyetinin, kişisel veri olan fotoğrafların sosyal paylaşım sitelerinde paylaşmamanın daha fazla olduğu görülmüştür.
- Cengiz Gündüz Alp (2021) tarafından bilgi işlem çalışanları arasında yapılan çalışmada dijital veri güvenliği farkındalığı bakımından 60 yaş üstü yaş grubu hariç diğer yaş grupları arasında anlamlı farklar bulunmuştur. 51-60 yaş grubunun dijital veri güvenliği farkındalığı diğer yaş gruplarından daha yüksektir. Bu durum 51-60 yaş grubundaki çalışanların dijital veri güvenliği farkındalığı bakımından daha deneyimli ve bilinçli olmasından kaynaklanmış olabileceği belirtilmiştir. Ancak yapmış olduğumuz çalışmada daha geniş sektörlerde çalışanlar incelenmiş olup çalışma sonucunda tüm yaş gruplarında yapılan karşılaştırma sonucunda 34-40 yaş gruplarının diğer yaş gruplarına göre bu daha hassas oldukları, cihazlarında anti virüs bulundurma, eğitimlere katılma, yazılımları güncelleme, e postları "spam /gereksiz/önemsiz" işaretleme oranlarının daha yüksek olduğu görülmüştür.

- Cengiz Gündüz Alp (2021) tarafından bilgi işlem çalışanları arasında yapılan çalışmada elde edilen sonuçlar dijital veri güvenliği farkındalıklarının farklı öğrenim durumlarına göre gruplarda farklılaştığını gösterdiği, doktora mezunu çalışanların dijital veri güvenliği farkındalıkları diğerlerinden daha yüksek olduğu görülmüştür. Bu durum doktora mezunu çalışanların dijital veri güvenliği konusunda daha fazla bilgi ve deneyime sahip olduğunun bir göstergesi olarak görülebileceği olarak açıklanmıştır. Yapmış olduğumuz çalışmada daha geniş sektörlerde çalışanlar incelenmiş olup çalışma sonucunda Cengiz Gündüz Alp tarafından yapılan çalışma sonucuna paralel sonuçlar elde edilmiştir. Eğitim durumu arttıkça siber güvenlik farkındalığı ve hassasiyetinin arttığı görülmüştür

KAYNAKLAR

Alemdaroğlu, A., 2020, *Çalışanların Bilgi Güvenliği Farkındalığına İlişkin Algıları: Bankacılık Sektöründe Araştırma*, Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü.

Alkan, M., 2012, Siber Güvenlik ve Siber Savaşlar, *Siber Güvenlik Siber Savaşlar TBMM Internet Komisyonu*.

Avcı, Ü., Oruç, O., 2020, Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi, *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21 (1), 284-303.

Aslay, F., 2017, Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi, *International Journal of Multidisciplinary Studies and Innovative Technologies*,1(1), 24-28.

Aytekin, A., 2015, *Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi*, Yüksek Lisans Tezi, Bilişim Sistemleri Anabilim Dalı.

Bahtiyar, A., CAN, B., 2016, Fen Öğretmen Adaylarının Bilimsel Süreç Becerileri ile Bilimsel Araştırmaya Yönelik Tutumlarının İncelenmesi, *Buca Eğitim Fakültesi Dergisi,* 42(1), 47-58

Güçlü, N., Sotirofski, K. (2006). Bilgi yönetimi. *Türk Eğitim Bilimleri Dergisi,* 4(4): 351-373.

Başeskioğlu, M., 2021, *Siber Güvenlik, Bilgisayar Ağları, Kimlik Avı, Kötü Amaçlı Yazılım, Fidye Yazılımı, Sosyal Mühendislik Biçiminde Korsanlıktan Korunmaya Yönelik İncelemeler ve Bir Uygulama,* Yüksek Lisans Tezi, Eğitim Bilimler Enstitüsü.

Bell, D., 2013, *İdeolojinin Sonu: Ellilerdeki Siyasi Fikirlerin Tükenişi Dair Çeviri*, Volkan Hacıoğlu, Bursa, Sentez Yayıncılık.

Canbek, G., Sağıroğlu, Ş., 2006. Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, *Politeknik Dergisi*, 9(3), 165-174.

Çifci, H., 2017, *Her Yönüyle Siber Savaş,* Tubitak, Ankara.

Ganbat, O., (2013). *Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması*. Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü.

Gündüzalp, C., 2021, Üniversite Çalışanlarının Dijital Veri ve Kişisel Siber Güvenlik Farkındalıkları (Bilgi İşlem Daire Başkanlıkları Örneği), *Journal of Computer and Education Research*, 9 (18), 598-303.

Güngör, M., 2015, *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı (Uzmanlık Tezi).

Goodman, S. E, 2008, Critical Information Infrastructure Protection, Terrorism (Ed.), *Responses to Cyber Terrorism NATO Science for Piece and Security,* 34 (9).

Hansen, L., Nissenbaum, H., 2009,Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly*, 53 (1), 1155-1175.

Karakaya, A., 2020, Karabük Üniversitesi Çalışanlarına Yönelik Kişisel Siber Güvenlik Üzerine Araştırma, *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 10 (2),157-172.

Karaca, İ., 2015, *Büyük Veri Analizlerinin Kurumsal Faaliyetlerde Kullanım Alanları*, Lisans Tezi.

Karasar, N., (2011). Bilimsel Araştırma Yöntemleri. Ankara: Nobel Yayınları.

Kaya, M., Aldemir C., 2020, Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları, *Kamu Yönetimi ve Politikaları Dergisi,*1 (7), 6-27.

Ki-Kare Testi, Ki-kare testi - Vikipedi (wikipedia.org), [Ziyaret Tarihi 3 Mayıs 2022].

Kitchin, R., 2014, The Data Revolution: Big Data, Open Data, *Data Infrastructures and Their Consequences*, London.

NATO, 2017. *Başarılı Bir Siber Savunma İçin Harcama Yapmak*. NATO Dergisi. NATO DERGİSİ- Başarılı bir siber savunma için harcama yapmak, [Ziyaret Tarihi 25 Kasım 2021].

Orkan, A.L, 1992, Bilişime Teorik Yaklaşım ve Bazı Temel Kavramlar, *Marmara İletişim Dergisi*, 1, 93-108.

Öğün M.N, Kaya A., 2013, Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler, *Güvenlik Stratejileri Dergisi*, 9 (18), 145-181.

Semerci, A., 2019, Eğitim Fakültesi Öğrencileri İle Diğer Fakültelerdeki Öğrencilerin Siber Güvenlik Farkındalıklarının Karşılaştırılması, *Akdeniz Eğitim Araştırmaları Dergisi*,13(29),138-156.

Sharp, E. D., 2004. Information Security in the Enterprise, Information Security Management Handbook, Fifth Edition, Auerbach Publications.

STM 2016, *2016 Temmuz Eylül Dönemi Siber Tehdit Durum Raporu,* 2016. siber-tehdit durum-raporu-temmuz-eylul-2016.pdf (wordpress.com) [Ziyaret Tarihi:2.01.2021].

Türk Dil Kurumu, Türk Dil Kurumu Sözlükleri (sozluk.gov.tr), [Ziyaret Tarihi 30 Kasım 2021].

UDHB 2012, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. *T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı,* Ankara, 9-47.

VonKnop K., 2008, Institutionslisation of a Web-focused, Multinstional Counter-Terrorism Campaign - Building a Collective Open Source Intelligent System, Terrorism (Ed.), *Responses to Cyber Terrorism NATO Science for Piece and Security,* 34(9),8-23.

Yaşar, H., Çakır, H., Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri, *Düzce Üniversitesi Bilim ve Teknoloji Dergisi,3 (2),488-507.*

Yerlikaya, C., 2019, *Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi*, Yüksek Lisans Tezi, Eğitim Bilimleri Enstitüsü

Yılmaz, S., Sağıroğlu Ş., 2013, "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi" *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara, 323-331.

Yiğit, M., Seferoğlu, S., Öğrencilerin Siber Güvenlik Davranışlarının Beş Faktör Kişilik Özellikleri ve Çeşitli Diğer Değişkenlere Göre İncelenmesi, *Mersin Üniversitesi Eğitim Fakültesi Dergisi,15 (1),186-215.*

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Serdar MASUM
Doğum Yeri	
Doğum Tarihi	
Uyruğu	X T.C. ❒ Diğer:
E-Posta Adresi	
Web Adresi	-

Eğitim Bilgileri	
Lisans	
Üniversite	Sakarya Üniversitesi
Fakülte	Mühendislik Fakültesi
Bölümü	Endüstri Mühendisliği
Mezuniyet Yılı	

Eğitim Bilgileri	
Lisans	
Üniversite	Anadolu Üniversitesi
Fakülte	Açıköğretim Fakültesi
Bölümü	Yönetim Bilişim Sistemleri
Mezuniyet Yılı	-

Yüksek Lisans	
Üniversite	İstanbul Üniversitesi
Enstitü Adı	Fen Bilimleri Enstitüsü
Anabilim Dalı	Enformatik Anabilim Dalı
Programı	Enformatik Programı