T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ ANA BİLİM DALI

YÜKSEK LİSANS TEZİ

KAMUDA ÇALIŞAN PERSONELLERİN BİREYSEL SİBER GÜVENLİK FARKINDALIKLARI

Serhat BAYSIZ

Ağustos-2025
BATMAN

T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ ANA BİLİM DALI

YÜKSEK LİSANS TEZİ

KAMUDA ÇALIŞAN PERSONELLERİN BİREYSEL SİBER GÜVENLİK FARKINDALIKLARI

Serhat BAYSIZ

Danışman
Dr. Öğr. Üyesi Hafzullah İŞ

Diğer Jüri Üyeleri

Doç. Dr. Abdulkerim ÖZTEKİN **Dr. Öğr. Üyesi İrfan KILIÇ**

Ağustos-2025
BATMAN

TEZ KABUL VE ONAYI

Serhat BAYSIZ tarafından hazırlanan “Kamuda Çalışan Personellerin Bireysel Siber Güvenlik Farkındalıkları” adlı tez çalışması 28/08/2025 tarihinde aşağıdaki jüri tarafından oy birliği ile Batman Üniversitesi Batman Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgi Teknolojileri Anabilim Dalı’nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Başkan Dr. Öğr. Üyesi İrfan KILIÇ	……..
Danışman Doç.Dr. Abdulkerim ÖZTEKİN	……..
Üye Dr. Öğr. Üyesi Hafzullah İŞ	……..

Yukarıdaki sonucu onaylarım.

Dr. Öğr. Üyesi Ömer Murat ÖTER
Lisansüstü Eğitim Enstitüsü Müdürü

ETİK BEYAN

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını beyan eder, aksinin ortaya çıkması durumunda her türlü yasal sorumluluğu kabullendiğimi bildiririm.

ETHICAL DECLARATION

I declare that all the information in this thesis has been obtained within the framework of ethical behavior and academic rules, and that the source of any statements and information that do not belong to me in this study prepared in accordance with the thesis writing rules has been fully cited, and I declare that I accept all kinds of legal responsibility in case of any contrary situation.

İmza
Serhat BAYSIZ
Tarih: 28/08/2025

ÖZET

YÜKSEK LİSANS TEZİ

KAMUDA ÇALIŞAN PERSONELLERİN BİREYSEL SİBER GÜVENLİK FARKINDALIKLARI

Serhat BAYSIZ

Batman Üniversitesi Lisansüstü Eğitim Enstitüsü

Bilgi Teknolojileri Ana Bilim Dalı

Danışman: Dr. Öğr. Üyesi Hafzullah İŞ

2025, 96 Sayfa

Bu tez çalışması, kamuda çalışan personellerin bireysel siber güvenlik farkındalık düzeylerini belirlemeyi ve bu farkındalığı etkileyen faktörleri incelemeyi amaçlamaktadır. Araştırmanın temel çıkış noktasını, artan siber tehditlere karşı kamu çalışanlarının bilgi güvenliği konusundaki tutum ve davranışlarının hem çalıştıkları kamu kuruluşu hem de ülke bazında oluşabilecek tehditlere karşı siber güvenlik açısından kritik öneme sahip olması belirlemiştir. Araştırmada nicel yöntemler benimsenmiştir. Veri toplama süreci dört hafta sürmüş ve çevrim içi anket yöntemi(Google Forms) kullanılmıştır. Veri toplama aracı olarak iki bölümden oluşan bir anket formu kullanılmıştır. İlk bölüm, katılımcıların demografik bilgilerini (yaş, cinsiyet, eğitim durumu, görev yaptığı kamu sektörü ve çalışma süresi) toplamaya yönelik 5 sorudan oluşmuştur. İkinci bölüm ise katılımcıların bireysel siber güvenlik farkındalık düzeylerini ölçmeye yönelik beşli Likert tipinde hazırlanmış 25 sorudan sorudan oluşmaktadır. Elde edilen veriler Microsoft Excel ve IBM SPSS Statistics programı ile analiz edilmiştir. Daha detaylı analizler kapsamında ANOVA, Kruskal-Wallis, Mann-Whitney U, Chi-Square testi, Temel Bileşen Analizi (PCA) ve korelasyon analizleri uygulanmıştır. Araştırmaya, toplam 303 kamu personeli katılmıştır.

Araştırma kullanılan puanlama sistemine göre Genel siber güvenlik farkındalık oranı %72,0 olarak belirlenmiştir. Katılımcıların 197'si erkek olup bu grubun ortalama farkındalık düzeyi %73,7'dir. 106'sı kadın katılımcıdan oluşan grubun ortalama farkındalık düzeyi ise %68,8 olarak tespit edilmiştir. Kamu çalışanlarının büyük çoğunluğu temel siber güvenlik önlemlerini (örneğin, antivirüs kullanımı, karmaşık şifre, güvenlik duvarı) uygulamakta, ancak özellikle finansal güvenlik ve mobil güvenlik alanlarında bilgi ve tutum farkları görülmektedir. Güvenlik davranışlarının çoğu, eğitim düzeyi veya dijital okuryazarlık ile ilişkili olarak, birlikte geliştiği görülmüştür. Çalışmada elde edilen korelasyon matrisleri, pek çok güvenlik alışkanlığı arasında pozitif ve istatistiksel olarak anlamlı ilişkiler olduğunu göstermiştir. Özellikle benzer işlevdeki güvenlik önlemlerinin birlikte uygulanma eğiliminde olması (örneğin, kablosuz ağ şifrelemesi ile modem güvenlik duvarı, karmaşık şifre kullanımı ile bilgisayar güvenlik duvarı) dikkat çekici olduğu gözlemlenmiştir. Temel Bileşen Analizi (PCA) sonucunda, güvenlik alışkanlıklarının birkaç temel boyut etrafında toplandığı saptanmıştır. Araştırmada, ilk beş soru veri setinin yarısından fazlasını (≈%54) açıklamıştır. Bu, kurumların güvenlik eğitim ve politikalarını bu temel bileşenler üzerine inşa etmelerinin, kaynak ve zaman açısından daha verimli olacağını göstermektedir. Sonuç olarak, kamu kurumlarında siber güvenlik alışkanlıklarının yaygınlaşması için eğitim, politika ve teknik önlemlerin entegre şekilde planlanması gerekmektedir. Bu çalışma, kurumların stratejik eğitim planlamasında, politika tasarımında ve risk analizinde bilimsel bir temel sunmaktadır.

Anahtar Kelimeler: Anket Çalışması, Kamu Personeli, İstatiksel Yöntemler, Siber Güvenlik, Siber Güvenlik Farkındalığı

ABSTRACT

MASTER THESIS

INDIVIDUAL CYBER SECURITY AWARENESS OF PUBLIC STAFF

Serhat BAYSIZ

Batman University Graduate Education Institute

Department of Informatıon Technologıes

Advisor: Asst. Prof. Dr. Hafzullah İŞ

2025, 96 Pages

This thesis aims to determine the individual cybersecurity awareness levels of public sector employees and to examine the factors influencing this awareness. The research's main starting point is the critical importance of public sector employees' attitudes and behaviors regarding information security in the face of increasing cyber threats, both within their respective public institutions and within the country. Quantitative methods were employed in the study. The data collection process lasted four weeks and employed an online survey method (Google Forms). A two-part survey form was used as the data collection tool. The first part consisted of five questions to collect participants' demographic information (age, gender, education level, public sector, and length of service). The second section consists of 25 five-point Likert-type questions designed to measure participants' individual cybersecurity awareness levels. The data obtained were analyzed using Microsoft Excel and IBM SPSS Statistics. For more detailed analyses, ANOVA, Kruskal-Wallis, Mann-Whitney U, Chi-Square tests, Principal Component Analysis (PCA), and correlation analyses were applied. A total of 303 public sector employees participated in the study.

According to the scoring system used in the study, the overall cybersecurity awareness rate was determined to be 72,0%. Of the participants, 197 were male, and the average awareness level of this group was 73,7%. The average awareness level of the group, consisting of 106 female participants, was determined to be 68,8%. The vast majority of public sector employees implement basic cybersecurity measures (e.g., antivirus use, complex passwords, firewalls), but differences in knowledge and attitudes are observed, particularly in the areas of financial security and mobile security. Many security behaviors have been observed to develop in conjunction with education level or digital literacy. The correlation matrices obtained in the study revealed positive and statistically significant relationships among many security habits. It was particularly noteworthy that security measures with similar functions tended to be implemented together (e.g., wireless network encryption and a modem firewall, or complex passwords and a computer firewall). Principal Component Analysis (PCA) revealed that security habits clustered around a few key dimensions. The first five questions explained more than half of the dataset (≈54%). This suggests that it would be more resource- and time-efficient for institutions to build their security training and policies on these key components. Consequently, integrated planning of training, policy, and technical measures is necessary to promote cybersecurity habits in public institutions. This study provides a scientific basis for institutions' strategic training planning, policy design, and risk analysis.

Keywords: Survey study, Public personnel, Statistical methods, Cybersecurity, Cybersecurity awareness,

ÖN SÖZ

Yüksek Lisans Tez çalışmam süresince bilgi ve deneyimlerinden sürekli yararlandığım, tezin başlangıcından sonuna kadar yardımlarını esirgemeyen danışman hocam Dr. Öğretim Üyesi Hafzullah İŞ'e sonsuz teşekkürlerimi sunarım.

Ayrıca desteklerini esirgemeyen aileme ve tez çalışmam süresince motivasyon anlamında yanımda olan Ahmet Alper COŞKUN ve Yiğit ŞENER'e ve yüksek lisans eğitimi süresince desteklerini esirgemeyen Bilgi Teknolojileri Anabilim Dalının değerli tüm öğretim üyelerine teşekkür ederim.

Serhat BAYSIZ
BATMAN-2025

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

2FA	İki Faktörlü Kimlik Doğrulama (Two-Factor Authentication)
ABD	Amerika Birleşik Devletleri
ANOVA	Varyans Analizi (Analysis of Variance)
AP	Erişim Noktası (Access Point)
BT	Bilgi Teknolojileri
CIA	Gizlillik, Bütünlük, Ulaşılabilirlik (Confidentiality, Integrity, Availabilty)
CISO	Bilgi Güvenliği Yöneticisi (Chief Information Security Officer)
CSF	Siber Güvenlik Çatısı (Cybersecurity Framework)
DHS	Amerika Birleşik Devletleri İç Güvenlik Bakanlığı (Department of Homeland Security)
DIR	Bilgi Kaynakları Departmanı
EFT	Elektronik Fon Transferi
FORTUNE 500	Amerika merkezli en büyük 500 şirketin yer aldığı sıralama listesi
NICCS	Ulusal Siber Güvenlik Yetkinlikleri Sistemi (National Initiative for Cybersecurity Careers and Studies)
PCA	Temel Bileşen Analizi (Principal Component Analysis)
PC	Kişisel Bilgisayar (Personal Computer)
PEW ARAŞTIRMA MERKEZİ	PEW Research Center; sosyal konularda veri analizleri yapan bağımsız araştırma kurumu
ROI	Yatırım Getirisi (Return on Investment)
SGF	Siber Güvenlik Farkındalığı
SMS	Kısa Mesaj Servisi (Short Message Service)
SPSS	İstatistiksel Paket Programı (Statistical Package for the Social Sciences)
SS	Standart Sapma
WPA	Wi-Fi Korumalı Erişim (Wi-Fi Protected Access)

ŞEKİL DİZİNİ

TABLO LİSTESİ

1. GİRİŞ

Dijital bir toplum olarak, kişisel, profesyonel ve akademik hayatlarımızı kapsayan bağlantılı bir dünyada yaşıyoruz. Ayrıca, dijital vatandaşlar, devlet kurumlarıyla olan etkileşimlerinde belirli beklentilere sahiptir. Bu etkileşimler, devlet kurumlarının vatandaşlarının ihtiyaçlarını karşılayacak yeni teknolojileri benimsemelerini gerektirir. Ancak, teknoloji benimsemesi siber saldırılar ve fidye yazılımları şeklinde ek riskleri de beraberinde getirir. Devlet kurumları artık kamuya ve siyasete dair zorlukların ötesinde sorunlarla karşı karşıyadır. Topladıkları büyük miktardaki vatandaş verileri, onları siber suçlular için cazip bir hedef hâline getirmektedir. Kurum içindeki siber güvenlik sorunlarını hafifletmek için teknolojik çözümler mevcut olsa da, ilk savunma hattı ve önleme yöntemi siber güvenlik eğitimi almış bir iş gücüdür. Son yıllarda, internete erişimin artması, birden fazla bağlantılı cihazın kullanımının yaygınlaşması ve dijital vatandaşlık olgusunun ortaya çıkması nedeniyle siber güvenlik farkındalığı daha da önemli hâle gelmiştir.

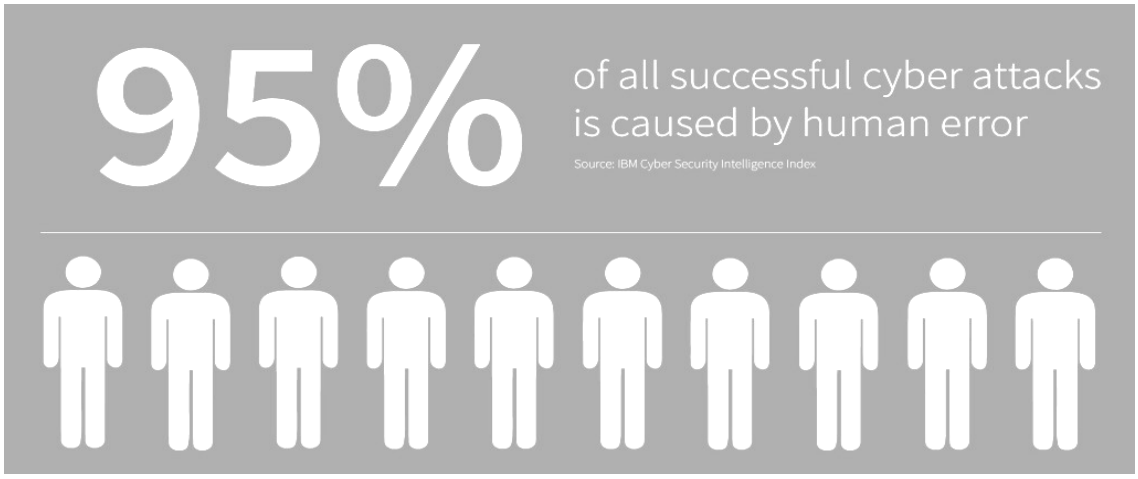
"Değerli ve gizli bilgileri elde etmek amacıyla sosyal mühendislik yöntemleri kullanarak kullanıcıları kandırmaya çalışan kötü niyetli aktörler vardır" (Diaz ve diğ., 2020, s. 44). Siber güvenlik farkındalığı olan bireyler, siber eğitim aracılığıyla kurumsal düzeyde veri ihlallerini hafifletmeye ya da tamamen önlemeye yardımcı olur. Siber ihlaller, bir organizasyon içinde meydana gelebilecek en yıkıcı olaylardan bazıları olabilir; bu nedenle, siber güvenlik eğitimlerinin çalışanların bilgi düzeyleri üzerindeki etkisinin ve siber güvenlik kavramlarının anlaşılmasının önemi büyüktür. Ancak birçok organizasyon, genellikle bir ihlal yaşadıktan sonra –ki bu genellikle kuruluş ve müşterileri açısından felaketle sonuçlanır– siber güvenlik araçlarını ve eğitimlerini benimsemektedir (Chowdhury ve diğ., 2019). Black ve diğ. (2018) ayrıca, "siber güvenlik alanında resmi bir eğitimi veya mesleki deneyimi olmayan kişilerin, siber güvenlik kavramlarını anlamakta zorlandıklarını" ve bu nedenle organizasyonlarını riske attıklarını savunur (s. 1822). Dahası, devlet kurumlarının ihlale uğradığı veya güvenliğinin tehlikeye girdiği pek çok vaka rapor edilmiştir; ancak, siber saldırılara hazırlık ve saldırıları hafifletmeye yönelik daha önce atılan adımlara dair nicel araştırmalar yetersizdir (Macmanus ve diğ., 2013; Kweon ve diğ., 2019). Siber güvenlik

kavramlarına dair bu bilgi ve farkındalık eksikliği, devlet kurumlarının topladığı büyük miktardaki vatandaş verisinin siber saldırılarla tehlikeye girmesine neden olabilir.

1.1. Sorunun Tanımı

İnternet kullanıcıları arasında siber güvenlik kavramlarına yönelik bilgi eksikliği ciddi bir sorun hâline gelmişken, çalışanlarının siber güvenlik farkındalığı olmayan devlet kurumları için bu durum kritik bir problem hâlini almıştır (Diaz ve diğ., 2020; CISA, 2020; Chowdhury ve diğ., 2019). Siber tehditlere yönelik bu farkındalık eksikliği, siber suçluların bu bireyleri istismar etmesini ve çalıştıkları kurumları tehlikeye atmasını kolaylaştırmıştır. Bu tür ihlaller, birey açısından utanç verici durumlara ve finansal yıkıma yol açabileceği için yıkıcı ve hayat değiştirici sonuçlar doğurabilir. Ancak devlet düzeyinde meydana gelen bir veri ihlali veya fidye yazılımı saldırısı, hem çalışan hem de vatandaş verilerinin ifşa olmasına, on binlerce bireyin etkilenmesine ya da milyonlarca dolarlık zarara neden olabilecek hizmet kesintilerine yol açabilir.

Bu zorluk birçok soruyu da beraberinde getirir. Bir kurum, konular ortalama bilgisayar kullanıcıları için çok karmaşık olduğunda siber güvenlik farkındalık eğitimini, nasıl yaygınlaştırabilir? Bu sorunun yanıtından bağımsız olarak, özellikle Şekil 1.1'de verildiği gibi "güvenlik olaylarının %95'inin insan hatasından kaynaklandığı" gerçeği göz önüne alındığında siber güvenlik eğitimi ciddiyetle ele almalıdır.(Diaz ve diğ., 2020, s. 53).



Şekil 1.1. Siber Saldırıların İnsan Hatasından Kaynaklanma Oranı (IBM Siber Güvenlik İstihbarat Endeksi)

Yalnızca bir çalışanın yapacağı hata, tüm bir kuruluşu felç edebilir, hassas verileri ifşa edebilir ya da milyonlarca dolarlık zarar ve verimlilik kaybına neden olabilir.

Dolayısıyla, bir çalışanın siber suç taktiklerini tanıyacak temel siber güvenlik bilgisine sahip olmaması, kurumlar açısından ciddi sonuçlara yol açabilir. Bu bağlamda, organizasyonlar "çalışanları güçlendirerek, 21. yüzyılın artan güvenlik beklentilerine uygun bir iş gücü dönüşümü gerçekleştirmelidir" (Axelrod, 2019, s. 2). Herhangi bir organizasyon için hazırlanacak bir eğitim programı; işle ilgili görevlerle ilgililiği, son kullanıcı risklerini ve risk azaltma fırsatlarını dikkate almalı; en önemlisi, sorunun bir parçası değil, çözümün bir parçası olmalıdır (Miller, 2017). Bu nedenle, siber güvenlik farkındalığı olan bir iş gücü, kurumun siber tehditlere karşı savunmasında paha biçilmez bir katkı sağlar.

1.2. Çalışmanın Gerekliliği

Siber güvenlik tehditleri yoğunluk, düzenlilik ve şiddet açısından artış göstermekte ve Türkiye'nin ulusal güvenliği için ciddi bir tehdit oluşturmaktadır. İnternet artık kullanıcılarının eskiden düşündüğü kadar güvenli bir ortam değildir; siber suç, küresel çapta bir endişe kaynağı olmaya devam etmektedir. Dijital vatandaşlar, kişisel ve profesyonel hayatlarını kapsayan tamamen bağlantılı bir dünyada yaşamaktadır. İnternet kullanıcıları arasında siber güvenlik farkındalığının eksikliği, özellikle de kurum çalışanları, siber güvenlikle ilgili olayların çoğundan sorumlu olduğunda siber suçluların bu bireyleri sömürmesini ve çalıştıkları kurumları tehlikeye atmasını kolaylaştırmıştır; (Diaz ve diğ., 2020). Ancak bu kuruluşlar genellikle güvenlik temelli teknolojileri uygulamakta ve tüm çalışanların siber güvenlik eğitimi almasını sağlamakta zorluk yaşamaktadır.

Bruijn ve Janssen (2017) ayrıca, "siber güvenlik konularında iletişim kurmanın organizasyonlar için zor bir çaba" olduğunu ve çalışan davranışlarının yeterli düzeyde bir farkındalık yansıtmadığını ileri sürmektedir. "Neredeyse herkes siber güvenliği duymuştur," ancak "insanlar genellikle siber güvenlik konusunda endişe duymamaktadır"

Buna bağlı olarak, siber güvenlik bilgisi eksikliği, bugün siber suç olarak bilinen olgulardaki artışla ilişkilendirilebilir; zira potansiyel suçlular, internet kullanıcılarının güvenlik ve internet güvenliği uygulamalarındaki eksikliklerinden faydalanabilecek yöntemler geliştirmektedir. Uygun eğitimin eksikliği ve buna bağlı bilgi yetersizliği,

“siber uzayın sonsuz hizmet ve fırsatlar sunduğunu” ancak bu dünyaya yabancı olan kullanıcılar için “pek çok riskin de eşlik ettiğini ve bu risklerin çoğunun internet kullanıcıları tarafından fark edilmediğini” göstermektedir (Kortjan ve Solms, 2014, s. 29).

Bu kullanıcıların ve sistemlerin istismar edilmesi, her bireyin bir kuruluş için potansiyel tehdit olabileceğini göstermektedir. “Kullanıcı farkındalığının eksikliğinin yeni açıklar doğurabileceği” gerçeği göz önüne alındığında, “politikaların oluşturulması ve insanların bunları anlaması” gereklidir (Bruijn ve Janssen, 2017, s. 4). Siber saldırılara karşı eğitsel bir azaltım aracı olarak siber güvenlik eğitiminin kullanımı, bu eğitimin bir çalışanın siber güvenlik farkındalığı üzerindeki etkisinin bir güvenlik ihlalini önlemek açısından yeterli olup olmadığını belirlemek için eleştirel bir araştırma gerektirmektedir. İnsanların siber güvenlik konusundaki bilgi eksiklikleri, yalnızca kişisel hayatlarını değil, profesyonel yaşamlarını da etkilemekte ve bu durum çalıştıkları kurumları güvenlik ihlallerine açık hâle getirmektedir. Bu doğrultuda, kuruluşların daha siber güvenlik farkındalığına sahip bir iş gücü geliştirmek amacıyla siber güvenlik farkındalık eğitimi sağlamaları gerekmektedir. Başarıyla uygulanan eğitimler, siber güvenlik farkındalığını etkili bir şekilde artırabilir ve siber güvenlik ihlallerinin azaltılmasına yardımcı olabilir. Bu da, daha fazla kamu kurumunun siber güvenlik farkındalık eğitimini kendi eğitim programlarının bir parçası olarak değerlendirmesini mümkün kılar. Bu nedenle, siber güvenlik eğitimi planlamak için kamu çalışanlarının siber güvenlik konularındaki bilgi düzeyini ve siber tehditleri azaltma becerilerini incelemek araştırılmaya değerdir.

1.3. Çalışmanın Amacı

Dijital toplum, teknolojinin ve internet bağlantısının benimsenmesiyle ortaya çıkan ilerici bir toplumdur. Dijital hükümet ise bu süreci, teknolojiye hâkim dijital vatandaşların devletle ilgili işlemlerini çevrim içi olarak yürütme beklentilerine cevap verebilmek için çeşitli dijital araçlar benimseyerek daha da ileri taşır. İnternet tabanlı teknolojilerin herhangi bir organizasyon tarafından benimsenmesi, beraberinde bu verilerin güvenliğini sağlama sorumluluğunu da getirir; bu durum, hem vatandaşlarının hem de kurumsal verilerinin korunmasından sorumlu olan devlet kurumları için özellikle geçerlidir.

Dijital verilerin güvence altına alınması, siber güvenliğin özünü oluşturur. Bu kavram, Ulusal Siber Güvenlik Kariyerleri ve Çalışmaları Girişimi (NICCS) tarafından şu şekilde tanımlanır: "Bilgi ve iletişim sistemlerinin ve bu sistemler içindeki bilgilerin zarar görme, yetkisiz kullanım veya değiştirme ya da kötüye kullanılmaya karşı korunması ve/veya savunulmasıyla ilgili herhangi bir faaliyet, süreç, yetenek veya durumdur" (NICCS, 2021, Vocabulary).

Dijital verilerin güvenliğini sağlamak, söylemesi kolay ama uygulaması zor bir süreçtir; çünkü teknoloji belli bir noktaya kadar bir organizasyonu koruyabilirken, siber suçlular ve modern siber suç taktikleri artık "insan güvenlik duvarı" olarak bilinen kurumsal çalışanları hedef almaya başlamıştır (Diaz ve diğ., 2020; Chowdhury ve diğ., 2019). Kemper (2019), birçok kuruluş için "çalışanların, kurumsal veri ve ağlar için en büyük siber güvenlik tehdidini oluşturduğunu" belirtmektedir; özellikle de bu çalışanlar siber güvenlik konusunda eğitimli değilse (s. 11).

Siber suçlular, bu taktiklerin farkında olmayan çalışanları istismar etmeye çalışır ve bu potansiyel tehdidi azaltmanın tek yolu farkındalık eğitimiyle mümkündür. Bu çalışmanın araştırmacısının görev yaptığı Güney Teksas'taki bir devlet kurumu, Kasım 2017'de bir kullanıcının kötü amaçlı ek içeren bir e-postayı açması sonucu bir virüs saldırısı yaşamıştır. Bu saldırı kontrol altına alınıp hafifletilmiş olsa da, söz konusu binadaki operasyonların tamamen normale dönmesi birkaç gün sürmüştür. Bu tür durumlar, Teksas eyaletinde işletmelerde, okullarda ve devlet kurumlarında sıkça yaşanmaktadır.

Siber suç tehdidinin artmasını önlemek amacıyla, 2019 yılında Teksas Temsilciler Meclisi, Bilgi Kaynakları Departmanı (DIR) ile birlikte, Temsilciler Meclisi Yasa Tasarısı 3834'ü geçirmiştir. Bu yasa, işlerinin en az %25'ini bilgisayar kullanarak gerçekleştiren tüm eyalet ve yerel kamu çalışanlarının her yıl bir siber güvenlik farkındalık eğitimi almasını zorunlu kılmıştır. İlk pilot eğitim, 2020 yılının ilk yarısında gerçekleştirilmiş ve bu kapsamda kurum genelinde zorunlu eğitimlerin temeli atılmıştır.Bu eğitim planlama aşamasında kurum genelinde çalışanların siber güvenlik farkındalık düzeylerini bilmek önemli bir yere sahiptir.

Bu araştırmanın temel amacı, kamu kurumlarında görev yapan personelin bireysel siber güvenlik farkındalık düzeylerini değerlendirmektir. Araştırma kapsamında yaş, cinsiyet, eğitim durumu, çalıştığı sektör ve çalışma süresi gibi demografik faktörlerin siber güvenlik farkındalığı üzerindeki etkilerini belirlemek hedeflenmektedir. Bunun yanı sıra, kamuda çalışan personelin siber güvenlik

farkındalık düzeyleri arasında anlamlı farklılıklar olup olmadığının ortaya konulması amaçlanmaktadır. Çalışmada, kamu personelinin bireysel farkındalık düzeylerinin belirlenmesi için bir anket uygulaması gerçekleştirilecektir. Anket yoluyla elde edilecek veriler doğrultusunda yapılacak puanlama sistemi ile, çalışanların siber güvenlik konularına ilişkin bilgi, tutum ve davranış düzeyleri analiz edilerek puanlanacak, kamu kurumlarının siber güvenlik farkındalığına yönelik eğitim ve politika geliştirme süreçlerine katkı sağlanması hedeflenmektedir.

1.4. Araştırma Soruları

Bu araştırma, siber güvenlik farkındalığının artırılmasının yalnızca bireysel veya kurumsal seviyede değil, ulusal ve uluslararası güvenlik açısından da kritik bir öneme sahip olduğu temelinden hareketle aşağıdaki sorulara odaklanmıştır:

- Kamu çalışanlarının sahip oldukları farklı siber güvenlik alışkanlıkları (parola güvenliği, e-posta güvenliği, mobil cihaz güvenliği, finansal güvenlik vb.) ne ölçüde birbirleriyle ilişkilidir? Bu alışkanlıklar bir bütün olarak bireylerin genel siber güvenlik farkındalık düzeyini nasıl şekillendirmekte ve ülke güvenliği açısından nasıl bir anlam taşımaktadır?
- Hizmet süresi dikkate alındığında, kamu çalışanlarının dijital tehditlere karşı verdikleri tepkiler ve geliştirdikleri güvenlik farkındalık düzeyi ne durumdadır? Bu farkındalık, kıdemli çalışanların deneyimleriyle birlikte nasıl bir farklılaşma göstermektedir ve ülke genelinde siber güvenlik kapasitesine nasıl katkı sağlamaktadır?
- Yaş grupları açısından kamu çalışanlarının dijital tehditlere karşı aldıkları önlemler, teknoloji kullanım biçimleri ve güvenlik davranışları hangi düzeydedir? Yaş faktörü, bireysel ve kurumsal siber güvenlik farkındalığında nasıl bir rol oynamaktadır?
- Eğitim düzeyine göre kamu çalışanlarının siber güvenlik konusundaki bilgi, bilinç ve uygulama becerileri ne düzeydedir? Eğitim seviyesi, çalışanların dijital tehditlere karşı dirençliliklerini ve güvenlik önlemlerine uyumlarını nasıl etkilemektedir?

1.5. Araştırma Hipotezi

Araştırma kapsamında aşağıdaki hipotezler test edilmiştir:

- H1: Hizmet süresinin, kamu çalışanlarının görevleri boyunca karşılaştıkları dijital tehditlere verdikleri tepkileri, edindikleri deneyimleri ve güvenlik farkındalık düzeylerini şekillendirdiği; dolayısıyla kıdemli çalışanların daha yüksek bir farkındalığa sahip olacağı öngörülmektedir.
- H2: Kamu çalışanlarının yaş gruplarının, dijital tehditlere karşı aldıkları önlemleri, teknolojiyi kullanım biçimlerini ve güvenlik davranışlarını doğrudan etkilediği; dolayısıyla yaş faktörü siber güvenlik farkındalık düzeylerinde önemli farklılıklar ortaya çıkarmaktadır.
- H3: Eğitim düzeyinin, kamu çalışanlarının siber güvenlik konusundaki bilinç, bilgi ve teknik uygulama becerileri üzerinde doğrudan etkili olduğu ve yükseköğrenim seviyesindeki bireylerin farkındalıkları daha gelişmiştir.
- H4: Kamu çalışanlarının sahip oldukları farklı siber güvenlik alışkanlıklarının birbirleriyle ilişkili olduğu ve bu alışkanlıkların genel farkındalık düzeyini etkilediği kabul edilmektedir.

1.6. Çalışmanın Önemi

İnternet, devasa boyutlara sahip dünyamızdaki bilgilere, birçok bağlantılı cihaz üzerinden bireylerin daha kolay erişmesini sağlayan bir yenilik olmuştur. İnternet, toplumların birbirleriyle nasıl etkileşim kurduğundan, işletmelerin nasıl yönetildiğine kadar hayatımızın neredeyse her yönünü değiştirmiştir. Aynı zamanda modern savaş kurallarını da değiştirmiş; ülkeler artık tek bir kurşun sıkmadan ya da bomba atmadan birbirlerine saldırabilecek duruma gelmiş, buna rağmen rakip bir ülkenin altyapısını felç edebilecek güce ulaşmışlardır. Bunun kanıtı olarak, 2021 yılında gerçekleşen ve Rus tehdit aktörleri (hackerlar) tarafından gerçekleştirildiği düşünülen Solarwinds siber saldırısı örnek gösterilebilir; bu saldırı, ABD Savunma Bakanlığı da dahil olmak üzere 12 federal kurumun ve birçok büyük Fortune 500 şirketinin güvenliğinin ihlal edilmesine yol açmıştır (Jibilian ve Canales, 2021).

Her siber saldırı politik ya da askeri amaçlarla gerçekleştirilmemektedir; çoğu zaman bu saldırılar, bir organizasyonun zayıf anını fırsat bilen ve bundan mali kazanç

elde etmeyi hedefleyen tehdit aktörlerinin eseridir. Bu tehdit aktörleri genellikle güvenlik olaylarından sorumlu kötü niyetli kişi ya da gruplardır ve bir organizasyonun güvenlik altyapısını tehlikeye atabilirler. Bu saldırılar bir organizasyonun bilgisayar ağını felç edebilir ya da gizlice, çalışanlarına ya da müşterilerine ait kişisel tanımlayıcı bilgileri onların haberi olmadan çalabilir.

Bu tehditler, birçok organizasyonu, siber güvenlik kavramları konusunda daha bilgili bir iş gücü geliştirmek ve koruma altındaki verilerinin ihlal edilme olasılığını azaltmak amacıyla güçlü siber güvenlik eğitimleri sağlamaya yöneltmektedir. Bir veri ihlali ya da tehdit aktörleri tarafından gerçekleştirilen hassas veya tescilli verilerin çalınması, bir organizasyonun itibarını kalıcı olarak zedeleyebilir ve müşteri nezdindeki güven düzeyini düşürebilir ki bu durum, seçmen verilerini yöneten kamu kurumları için çok daha kritik bir sorundur.

Bu araştırmanın önemi, günümüzün artan dijital tehdit ortamında, kamu çalışanlarının siber güvenlik konusundaki bilgi ve bilinç düzeyinin sadece kurumsal değil, aynı zamanda ulusal güvenliğin güçlendirilmesi açısından da kritik bir rol oynamasında yatmaktadır. Çalışmanın bulguları, siber güvenlik farkındalığı yüksek bir iş gücüne duyulan ihtiyacın altını çizerken, özellikle küresel ölçekte yaşanan siber saldırılar, hibrit savaş örnekleri ve güncel uluslararası krizler (ör. İsrail-Hizbullah gerilimi, Ukrayna-Rusya savaşı) ışığında, kamu kurumlarının dirençli dijital altyapılara sahip olmasının gerekliliğini ortaya koymaktadır. Ayrıca, bu çalışma sayesinde güvenlik uzmanları ve politika yapıcılar, mevcut eğitim programlarının etkililiğini değerlendirme ve daha etkili farkındalık stratejileri geliştirme imkânına kavuşabilirler. Sonuç olarak, elde edilen bulgular hem bireysel hem de ülke çapında sürdürülebilir bir siber güvenlik kültürünün inşasına bilimsel katkı sağlamayı amaçlamaktadır. Araştırma verilerine dayalı daha etkili eğitim uygulamaları, kamu, özel sektör ve eğitim kurumları da dâhil olmak üzere organizasyonlardaki mevcut siber güvenlik farkındalığı düzeyinin iyileştirilmesinde kullanılabilir.

Ayrıca, bir organizasyonun güvenlik duruşunda insan faktörünün, teknik savunmalar kadar önemli olduğunun anlaşılması, iş gücünün güvenlik eğitimi almasının kurumsal düzeyde gerekliliğini ortaya koymaktadır. Diaz ve arkadaşlarının (2020) belirttiği gibi, “insan faktörü ya da hata, güvenlik olaylarının %95’inden sorumludur” (s. 53) ve bu durum Chowdhury ve arkadaşları (2019) tarafından da “başarılı siber saldırıların %95’inden fazlasının insan hatasından kaynaklandığı tahmin edilmektedir” (s. 1290) şeklinde doğrulanmıştır. İnternete erişimin artması, birden fazla bağlantılı

cihazın yaygınlaşması ve dijital vatandaşlık olgusunun gelişmesiyle birlikte siber güvenlik farkındalığı son yıllarda daha da önemli hâle gelmiştir.

Siber güvenlik ihtiyacı, çoğu internet kullanıcısının "anti-virüs ve güvenlik duvarının veri, gizlilik ve güvenliği korumak için tek gereklilik olduğuna" inanmasıyla daha da belirginleşmektedir (Tirumala ve arkadaşları, 2016, s. 228). Bu araştırma, politika yapıcılara güvenlik sorunlarını tanımlamada yardımcı olabileceği gibi, güvenlik politikaları, prosedürleri ve eğitim müfredatlarının geliştirilmesinde de katkı sağlayabilir. Aynı zamanda, siber güvenlik bilgisi ediniminin çalışanlara yönelik farkındalık programları yoluyla artırılmasına dair çözüm arayan organizasyonların algılarını da şekillendirmeye yardımcı olabilir.

Hipotez odur ki, bir iş gücü siber güvenlik tehditleri hakkında ne kadar bilgi sahibiyse, siber suçluların aldatıcı tekniklerine karşı o denli dirençli olacaktır. Bu görüş, Costa ve arkadaşlarının (2019) şu ifadesiyle de desteklenmektedir: "Kullanıcılarda güvenlik ve sorumluluk kültürünün geliştirilmesi organizasyonlar için hayati önemdedir"; zira kullanıcılar, organizasyonun güvenlik duruşunun işlevsel bir parçasıdır (s. 2033). Bu amaçla, bu araştırma, siber güvenlik eğitimlerinin planlaması ve icrası için kamu çalışanlarının siber güvenlik konularına ilişkin bilgi düzeyleri ve siber tehditleri azaltma yeteneklerinin tespit edilmesinde etkili faktörleri incelemiştir

2. GENEL BİLGİLER VE LİTERATÜR İNCELEMESİ

Bu çalışmanın temel amacı, bir siber güvenlik farkındalık eğitimi programının, kamu çalışanlarının siber güvenlik konularına ilişkin bilgi düzeyleri ve dijital tehditleri azaltma yetenekleri üzerindeki etkisini analiz etmektir. Ayrıca bu programın, ülke güvenliğinin güçlendirilmesine ve kamu kurumlarının uluslararası siber tehditler (örneğin, İsrail-Hizbullah çatışması, Ukrayna-Rusya savaşı gibi) karşı dirençliliğine olası katkıları da ele alınacaktır.
Bu kapsamda, aşağıdaki araştırma soruları incelenecektir:

- Bir siber güvenlik farkındalık eğitimi programının, kamu çalışanlarının siber güvenlik konuları ve uygulamaları hakkındaki bilgileri ve bu bilgilerin ülke genelinde siber savunmaya etkisi nedir?
- Bu tür bir eğitim programı, kamu çalışanlarının hem bireysel hem de kurumsal düzeyde siber tehditleri azaltma yeteneklerini ve ulusal siber güvenlik kapasitesini nasıl etkilemektedir?
- Türkiye'de kamu çalışanlarının siber güvenlik alışkanlıkları, güncel uluslararası krizler ve küresel tehditler ışığında ülke güvenliği için yeterli midir?

Bu bölümde, çalışmaya adapte edilen kuramsal çerçeve doğrultusunda; eğitim, yönetsel müdahale, farkındalık, eylem niyeti ve buna bağlı olarak çalışan davranışlarına ilişkin mevcut siber güvenlik literatürünün bir özeti sunulmaktadır. Literatür taraması, bu çalışmada kullanılan kuramsal çerçevenin geliştirilmesi ve uyarlanmasında kritik bir rol oynamıştır. Mevcut akademik bilgi birikimine yönelik sistematik bir tarama; nitelikli, hakemli ve siber güvenlikle ilişkili literatür aracılığıyla araştırma probleminin varlığını doğrulamakta ve çalışmanın gerekçelendirilmesine ve yapılandırılmasına katkı sağlamaktadır.

2.1. Siber Güvenlik

Siber güvenlik kavramının literatürdeki ilk bahsi yirmi yıl önce ortaya çıktı, bu nedenle nispeten yeni bir kavram olmasına rağmen şimdiden geniş çapta tanınmıştır (Reegård ve diğerleri, 2019). O zamandan beri internet küresel iletişimde önemli bir rol

oynamış ve insanların yaşamlarının ayrılmaz bir parçası haline gelmiştir; öyle ki günümüzde dünya genelinde üç milyardan fazla internet ve siber uzay kullanıcısı bulunmaktadır. Siber uzay, "BT altyapılarından, iletişim ağlarından, bilgisayar sistemlerinden, gömülü işlemcilerden, hayati endüstri denetleyicilerinden, bilgi sanal ortamından ve bu ortam ile insanlar arasındaki bilginin üretimi, işlenmesi, depolanması, değişimi, geri alınması ve kullanılması amacıyla gerçekleşen etkileşimden oluşan birbirine bağlı ağlar" olarak tanımlanabilir. Siber uzay esasen tüm kullanıcı etkileşimlerinin ve faaliyetlerinin gerçekleştiği yerdir. Bu nedenle, kullanıcıların yaşamlarının önemli bir kısmı siber uzayla etkileşim halinde geçer ve siber uzay siber tehditlere maruz kaldığında, onunla bütünleşen kullanıcılar önemli ölçüde etkilenebilir. Siber güvenlik kavramı, kuruluşlar için altyapılarını güvence altına alma ve özel ve müşteri verilerini saldırganlardan koruma yetenekleriyle ilgili olduğundan büyük önem taşır. Bu nedenle siber güvenlik, bir kuruluşun bilgi, ağ ve verilerini hem iç hem de dış tehditlerden korumak için uygulanan pratik önlemleri içerir (Li ve Liu, 2021).

Hassas bilgileri iç ve dış tehditlerden koruma tartışılırken, Gizlilik, Bütünlük ve Erişilebilirlik prensipleri yetkisiz kişilerden bilgiyi saklamanın yolları olduğu için CIA üçlüsü sıkça anılır (Li ve Liu, 2021). Ancak, siber güvenlik terimi uzun süredir bilgi güvenliği ile birbirinin yerine kullanılmıştır. Yine de, iki terim arasında önemli bir örtüşme olmasına rağmen, kavramlar arasında bir fark vardır. Dikkat çekici fark, siber güvenliğin bilgi güvenliğinin geleneksel sınırlarını içermesi ve bu tanımın ötesindeki faktörleri de kapsamasıdır, oysa bilgi güvenliği bunu yapmaz. Örneğin, bilgi güvenliği esas olarak "bilginin ve onu kullanan, depolayan ve ileten sistemler ve donanım dahil olmak üzere kritik unsurlarının korunmasına" odaklanırken, bir olay bilginin CIA'sında bir ihlalle sonuçlanacaktır. Aynı zamanda, siber güvenlik bu unsurlara ve bunun ötesindeki unsurlara odaklanır; bu da insanları, ev aletlerini, ulusal altyapıyı vb. korumayı içerebilir. Siber güvenlikte varlıklardan bahsedilirken, siber uzay aracılığıyla ulaşılabilecek her şey kastedilebilir. Dolayısıyla, siber güvenlikte insan faktöründen bahsedildiğinde, siber saldırıların potansiyel hedefi olan insanlara atıfta bulunulur. Buna karşılık, bilgi güvenliğindeki insan faktörü, güvenlik süreci içindeki rolüne atıfta bulunulacaktır. Bu nedenle, bu iki kavram birbiriyle ilişkili ancak eş anlamlı değildir (Von Solms ve Van Niekerk, 2013).

Bilgisayar ve iletişim teknolojileri, hızlı gelişimleri sürekli olarak daha gelişmiş ve sofistike teknolojiler yarattığı için siber güvenlik alanını değiştirmektedir. Her değişiklik, istismar edilecek yeni olası güvenlik açıkları yaratır ve bu nedenle planlı bir

karşı önlem yanıtı gerektirir. Siber uzay, sürekli değişimin yaşandığı dinamik bir yerdir ve bu durum, tehditler ve teknoloji de onunla birlikte değiştiği için siber güvenlik önlemlerinin oluşturulmasını daha da zorlaştırmaktadır (Li ve Liu, 2021). Bu sofistike teknolojiler, teknolojideki bir değişikliğin kullanıcıların internete bakış açılarını etkilemesi nedeniyle kullanıcılarının davranışlarını değiştirir. Bu nedenle, büyüyen ve sürekli değişen tehdit ortamına uyum sağlamak için tamamen yeni bir tehdit ve koruma modeli oluşturulması gerekmiştir. Siber tehditler teknolojiye bağlı olarak geliştiğinde, kullanıcıların hassas bilgilerini buna göre verimli bir şekilde korumalarını genellikle zorlaştırır. Bunun nedeni genellikle, günümüzdeki mevcut teknoloji ile insanların bunları etkili bir şekilde güvence altına almak için sahip oldukları bilgi arasında bir bilgi boşluğu bulunmasıdır. Bu durum, insanların ileri ve sofistike teknolojileri, nasıl çalıştıkları hakkında minimum anlayış veya bilgi sahibi olmadan kullanmalarına neden olur, bu da daha büyük güvenlik olayı risklerini beraberinde getirir. Kullanıcılar genellikle siber güvenlik konusunda genel bir farkındalığa sahiptir; örneğin, çoğu kişi bilgisayar korsanlarının ne olduğunu ve neden zararlı kabul edildiğini belirsizce açıklayabilir, ancak güvenli davranmakta genellikle büyük zorluk çekerler. İnsan hatalarının ortaya çıkışının sayısız yolu vardır ve bunlar genellikle kullanıcıların kusurlu siber hijyenleriyle ilgilidir. Örneğin, zayıf sistem yapılandırması, zayıf yama yönetimi, zayıf veya varsayılan parola ve kullanıcı adları kullanma, farklı web sitelerinde parolaları yeniden kullanma, virüslü e-posta eklerine tıklama, iş yerinden ayrılırken dizüstü bilgisayarları açık bırakma vb. (Szumski, 2018).

İnternet ve kullanımı, kamu, özel ve eğitim sektörlerinde faaliyet gösteren birçok kuruluşun günlük operasyonlarının kritik bir parçasıdır. Aynı durum, bireylerin sosyal medya, e-posta ve dijital yayın platformları kullanımı ile birlikte interneti yoğun şekilde kullanmaları açısından da geçerlidir. Araştırmalar, internet kullanımının artmakta olduğunu ancak internet üzerindeki güvenli uygulamaların –yani siber güvenliğin– aynı oranda artmadığını göstermektedir (Costa ve diğ., 2019; Chowdhury ve diğ., 2019; Tirumala ve diğ., 2016).

Dijital vatandaşlar olarak, finansal işlemler gerçekleştiriyor, kişisel bilgilerimizi rahatça paylaşıyoruz ve çocuklar çevrim içi oyun oynarken tanımadıkları insanlarla sohbet ediyor. Bu yeni dijital gerçeklik, tehdit aktörlerinin "sosyal mühendislik" olarak bilinen yeni bir taktik geliştirmelerine neden olmuştur. Bu yöntemde suçlular, kamuya açık bilgileri kullanarak kullanıcıları daha hassas bilgileri paylaşmaya veya bir güvenlik ihlaline neden olacak davranışta bulunmaya ikna ederler (MacManus ve diğ., 2013).

Tehdit farkındalığı olmadan internetin ve çevrim içi kaynakların kullanımı, hem kurumlar hem de bireyler için yıkıcı sonuçlara yol açabilir. Farkındalığı olmayan ve eğitilmemiş bir kamu çalışanı iş yerindeyken internete eriştiğinde, büyük miktarda işlem verisini riske atabilir. Kamu çalışanları sıklıkla son teslim tarihlerine uymaları yönünde baskı altındadır ve bu aciliyet hissi, onları güvenlik açısından gevşek bir ruh hâline sokabilir. Güvenlik alışkanlıklarına dair bu durumsal farkındalık eksikliği, "siber güvenlikteki insan güvenlik duvarının sıklıkla ihlal edilmesine ve bunun da kullanıcılar, temsil ettikleri kurumlar ve hizmet verdikleri müşteriler açısından felaket niteliğinde sonuçlara yol açmasına neden olmaktadır" (Chowdhury ve diğ., 2019, s. 1291).

Ayrıca, birçok kişi için "siber güvenlik gereksinimlerini karşılamak, birincil iş görevlerini yerine getirmelerini zorlaştırmakta" ve bu nedenle "kurum içindeki siber güvenliğin önemi algısı daha da bozulmaktadır" (s. 1298). Chowdhury ve arkadaşları (2019), güvenlik politikaları, prosedürleri ve teknik kontrollerin başarısının "nihayetinde güvenlik uygulayıcılarının gerçek davranışlarına bağlı olduğunu" çünkü bu kontrollerin çalışan operasyonlarını karmaşıklaştırıp yük haline getirebildiğini ifade etmektedir (s. 1293).

Costa ve arkadaşları (2019), organizasyon yönetimi tarafından oluşturulan bu güvenlik kontrollerinin, çalışan davranışının "hem iş yerinde hem de evde bilgi, donanım ve sistem güvenliği açısından temel bir rol oynadığını" göstermeye yardımcı olduğunu belirtmektedir (s. 2036). Kortjan ve Solms (2014) ise yöneticilerin güvenlik girişimlerini destekleyerek bir organizasyonun siber güvenlik hedeflerine katkı sağlayabileceğini ve "siber güvenlik farkındalığının teşvik edilmesinin genel olarak siber güvenliğe büyük katkı sağlayacağını" ifade etmektedir (s. 29).

Uygun bir siber güvenlik programının izlenmesi ve yeterli eğitim ile tatbikatlarla desteklenmesi, çalışanların "hizmet kesintisi, kurumsal süreçlerin aksaması ya da daha kötüsü, vatandaşların ihtiyaçlarının karşılanmaması gibi endişelere kapılmadan, vatandaş deneyimini sürekli olarak iyileştirmeye odaklanmalarını" sağlar (Axelrod, 2019, s. 1). Özellikle veri güvenliğinin kamunun çıkarına hizmet etmek ve güveni sürdürmek açısından kilit öneme sahip olduğu bir ortamda, bu unsurların tümü uygun eğitim ve güvenlik alışkanlıkları ile sağlanabilir.

Ancak eğitimin başarılı olabilmesi için, uygun içerik ve yöntemlerin dikkate alınması gerekir. Güvenlik farkındalığı içerik geliştiricileri, Adorjan ve Ricciardelli'nin (2019) önerdiği gibi, katılımcının "günlük yaşam deneyimleriyle ilişki kurabileceği ve bu mesajları uygulayabileceği" içerikler geliştirmeli ve "hem çok düşük olasılıklı hem

de katılımcının mesleki ve sosyal deneyimleriyle çelişen tehlikelere aşırı odaklanmaktan" kaçınmalıdır (s. 432).

Daengsi ve arkadaşları (2021), "bu tür tehditlerin oluşturduğu risklerin, çalışanların siber güvenlik farkındalığına sahip olmaları durumunda azaltılabileceğini" savunmaktadır (s. 102). Bu görüşe, Costa ve diğ. (2019), Heartfield ve Loukas (2018) ile Kortjan ve Solms da katılarak, farkındalık eğitiminin, çalışanların şüpheli faaliyetleri tespit edip güvenlik ekiplerine bildirme yetkinliği kazanmasında kilit rol oynadığını belirtmektedir. Diaz ve arkadaşları (2020) ile Daengsi ve arkadaşları (2021), eğitimin simülasyonlarla desteklenmesi gerektiğini ve bunun daha fazla katılım ve öğrenmeyi teşvik ederken, eğitimdeki eksikliklerin belirlenmesine de yardımcı olabileceğini vurgulamaktadır. Peker ve arkadaşları (2016), "Ortak internet/teknoloji kullanıcılarının dikkatsiz siber alışkanlıklarının şok edici sonuçlarını gösteren yeterince etkileşimli bir güvenlik farkındalığı modülünün, geniş çapta farkındalığı etkili bir şekilde artıracağını" belirtmektedir (s. 4).

Çalışanlarına siber güvenlik eğitimi konusunda yatırım yapan kurumlar, onları "potansiyel bir sorunun parçası olmak yerine, çözümün bir parçası hâline getirir" (Costa ve diğ., 2019, s. 2036).

Bazı organizasyonlar, çalışanlarına –siber güvenlik farkındalık eğitimi de dâhil olmak üzere– eğitim sağlamaya hâlâ temkinli yaklaşabilmektedir. Ancak araştırmacılar, siber güvenlik farkındalık eğitimine yapılan yatırımların organizasyonlar için birçok fayda sağladığı ve çalışanların güçlendirilmesinin, kurumun genel güvenlik duruşunu ve siber saldırılara karşı dayanıklılığını artırma gibi ek avantajlar sunduğu konusunda hemfikirdir (Costa ve diğ., 2019; Diaz ve diğ., 2020; Peker ve diğ., 2016; Daengsi ve diğ., 2021). Bir organizasyonun, bir siber güvenlik farkındalık programının uygulanmasının sağladığı ek faydaları anlayabilmesi için, Tirumala ve arkadaşları (2016) "siber güvenlik farkındalığının öneminin çeşitli istatistiklerin sunulması ve ardından mevcut farkındalık uygulamaları ile ortaya konulduğunu" ve bunun kurumun mevcut başlangıç seviyesini belirlediğini ifade etmektedir (s. 1).

Ayrıca, Oancea ve arkadaşları (2019), "siber saldırıların çoğunun kullanıcıların zafiyetlerini hedef aldığını, yalnızca bir kısmının teknik açıkları kullandığını" ve bu zafiyetlerin giderilmesinin yolunun, çalışanların güvenlik temelli durumsal farkındalıklarının artırılmasından geçtiğini belirtmektedir (s. 46). Eğitimin geçerliliği ve etkinliği bu çalışmada olduğu gibi bir anket yoluyla değerlendirilebilir; Tirumala ve

arkadaşları (2016) “bir anketin, eğitim sonrası bir organizasyonun siber güvenlik farkındalığını kapsamlı biçimde anlamaya yardımcı olduğunu” savunur (s. 1).

Yazdanpanahi (2021), “çalışanlar iyi eğitildiğinde ve bilgilendirildiğinde, siber tehditlere karşı değerli ve ilk savunma hattı olabileceklerini” ancak bunun için “yıl boyunca düzenli eğitim oturumları ve oltalama karşıtı kampanyalar yürütülmesi gerektiğini” vurgular (s. 3). Teksas Eyaleti'nde, 2019’da çıkarılan House Bill 3834 ve 2021’de çıkarılan House Bill 1118 ile siber saldırıların ülke genelinde ve özellikle Teksas’ta artması nedeniyle, eyalet ve yerel kamu çalışanları için siber güvenlik eğitimleri zorunlu hâle getirilmiştir (Yazdanpanahi, 2021).

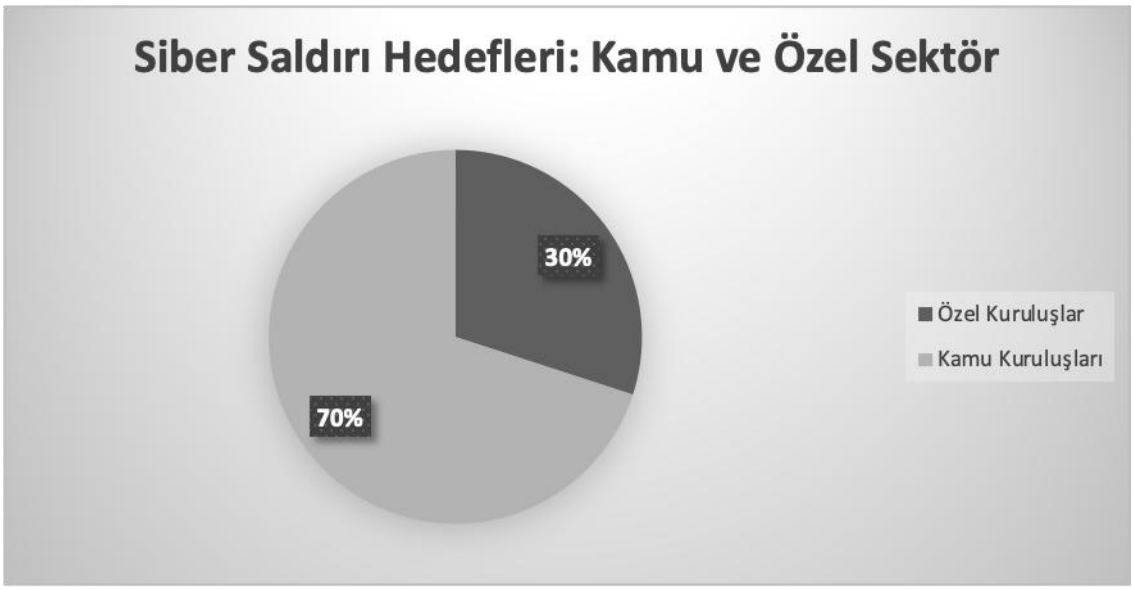
Siber farkındalık eksikliği, işletmelere ait verilerin, kurumsal ağların ve hem grup hem bireylere ait kişisel kimlik bilgilerinin güvenliğini riske atmaktadır (Daengsi ve diğ., 2021; Kortjan ve Solms, 2014; Olmstead ve Smith, 2017). Birçok organizasyon, siber farkındalık eğitimi ve bilgiyi nasıl etkili bir şekilde yayacağını bilememektedir; ayrıca, çoğu birey, interneti kullanırken siber güvenlik kavramlarının farkında olması gerektiğini bile bilmemektedir (Peker ve diğ., 2016; Olmstead ve Smith, 2017). Geleneksel kurumsal eğitim programları, çoğu zaman çalışanların önemli ölçüde zamanını ve verimliliğini almakta; bu nedenle çalışanlar tarafından angarya olarak görülüp yeterince ciddiyetle karşılanmamaktadır. Oysa, özellikle günümüzde artan dijital tehditler ve uluslararası kriz ortamı (örneğin İsrail-Hizbullah çatışması, Ukrayna-Rusya savaşı gibi) siber güvenlik farkındalığının yalnızca bireysel değil, kurumsal ve ulusal düzeyde de yaygınlaştırılmasını zorunlu kılmaktadır.

Bu nedenle sunulan literatür taraması, hem mevcut siber güvenlik eğitimlerinin etkinliğine dair önemli çalışmaları özetlemek hem de toplumda siber güvenlik farkındalığını ve ülke genelinde dirençli dijital kültürün oluşumunu desteklemek amacıyla hazırlanmıştır. Bu kapsamda, siber güvenlik eğitim programlarının hangi koşullarda etkili olduğu, katılımcıların motivasyonu ve eğitime katılım süreçleri gibi konulara odaklanılmıştır.

2.1.1. Kamusal alanda siber güvenlik

Günümüz iş ortamında, bilgi herhangi bir kuruluşun başarısı için değerli bir kaynaktır ve hayatta kalması için hayati hale gelmiştir. Kuruluşlar, dış veya iç kaynaklardan kaynaklanan siber saldırılara maruz kaldığında bu değerli kaynağı korumak giderek zorlaşmakta, böylece kuruluşun ve bilgilerinin güvenliği tehlikeye

girmektedir (Tu ve diğerleri, 2018). Bu nedenle, iyi bir siber güvenlik sürdürmek, kamu ve özel kuruluşlar için iş hedeflerini korumak açısından çok önemlidir. Ancak, kamusal alanda siber saldırılar meydana geldiğinde, yansımaları daha ciddi olma eğilimindedir. Bunun nedeni, kamusal alanın özel sektöre kıyasla daha geniş ve yaygın bir kullanıcı tabanını kapsamasıdır (Aman ve Al Shukaili, 2021). Şekil 2.1'de verildiği gibi siber saldırı hedeflerinin %70'i kamuya yönelik gerçekleşmektedir(Aman ve Al Shukaili, 2021).



Şekil 2.1. Kamu ve özel sektörde saldırı oranları(Aman & Al Shukaili (2021)

Kamusal alan, ekonomik ve sosyal yaşamda ve gelişimde kritik işlevleri yerine getirir; örneğin, silahlı kuvvetler, polis, acil servis ve yasama ve yargı mercilerinden oluşur. Kamusal alan ayrıca, vatandaşlarına kritik altyapı olarak kabul edilen hizmet ve ürünler sağlayan kamu kuruluşlarından oluşur. Bunlar arasında bankalar, hastaneler, eğitim kurumları, enerji, telekomünikasyon, ulaşım kuruluşları, endüstriler, üreticiler vb. yer alır (Loukis ve Spinellis, 2001). Bu kritik işlevler ve altyapılar siber saldırılara karşı savunmasız hale geldiğinde, hizmetlerindeki herhangi bir aksaklık toplum üzerinde önemli bir etkiyle sonuçlanan sonuçlara yol açabilir (Aman ve Al Shukaili, 2021).

Kamusal alandaki kritik altyapıların, diğer altyapı sistemlerine sayısız bağımlılığı olan sistemler içerdiğini belirtmek önemlidir. Bir sistemde bir siber saldırı meydana gelirse, aynı anda diğer sistemleri de bozabilir (Dawson ve diğerleri, 2021). Siber saldırıların toplumsal sonuçları söz konusu olduğunda kamu ve özel kuruluşlar

arasında önemli bir tezat vardır. Bir kamu kuruluşu, kritik sistemlerini bozan bir siber saldırıyla karşılaşması durumunda, aksaklık özel kuruluşlara kıyasla toplum üzerinde daha büyük ölçekli bir etkiye neden olacaktır. Bunun nedeni, böylesine yaygın bir aksaklığın daha büyük ekonomik ve sosyal etkilere sahip olması ve hatta vatandaşların güvenliğini tehdit edebilmesidir (Loukis ve Spinellis, 2001).

Kamusal alanın yüksek sıklıkta hedeflenen siber saldırılar yaşadığı belirtilmiştir. Araştırmalar, güvenlik ihlallerinin yaklaşık yüzde yetmişinin kamu veya devlet kuruluşlarına yönelik olduğunu göstermektedir (Aman ve Al Shukaili, 2021). Ayrıca, başka bir tez, hükümet, emniyet teşkilatı ve sağlık gibi kamusal alanın çeşitli bölgelerindeki kamu kuruluşlarının siber saldırılar tarafından giderek daha fazla hedeflendiği gerçeğini ortaya koymuştur. Tezin bulguları, kamu kuruluşlarını hedef alan bu siber saldırıların dış faktörlerden (dış bilgisayar korsanları gibi) ve iç faktörlerden (mevcut veya eski çalışanlar gibi) kaynaklanabileceğini düşündürmektedir (Bendovschi, 2015). Siber saldırıları önlemek için yalnızca teknik önlemlere güvenmenin kamusal alandaki kuruluşlar için yeterli olmayabileceği giderek daha belirgin hale gelmektedir. Bu nedenle, insan davranışlarını hesaba katan güçlü sosyo-teknik siber güvenlik önlemlerinin uygulanması çok önemlidir (Gandhi ve diğerleri, 2011).

Schürmann ve arkadaşları (2020), kamu çalışanlarının—özellikle seçim süreçlerinde görev alanların—siber güvenlik farkındalığı eğitimi alması gerektiğini vurgulamışlardır. Bunun temel nedeni, yönetilen büyük ölçüde seçmen verisi ve tarihî olarak oltalama (spear-phishing) saldırılarının hedefi olmalarıdır. Bununla birlikte Schürmann ve arkadaşları, "siber güvenlik farkındalığı eğitiminin etkisiz ve sıkıcı" olarak kötü bir üne sahip olduğunu belirtir (s. 196). Dolayısıyla, hem geliştirme sürecinde hem de değerlendirmede bazı değişikliklerin yapılması gerektiğini savunmuşlardır. Bu iyileştirmeler, kavramların kısa vadeli akılda kalıcılığını artırabilir, kurumları güvenlik ihlallerine karşı koruyabilir ve çalışanların siber saldırılarla başa çıkma yetisini artırabilir. Eğitim sayesinde kullanıcıların "mantıksal düşünme, saldırıyı tanıma, tepki verme ve savunma davranışını kazanmaları" hedeflenmelidir (s. 196). Şu hâle gelinmektedir: eğitim, önce bir güvenlik analizi yapıldıktan sonra "metodolojik olarak ilgili ve tutarlı" olmalıdır; böylece çalışan davranışları değiştirilebilir ve eğitim içeriği anlam kazanır.

Schürmann ve arkadaşları(2020), eğitim etkinliğini değerlendirmek için Kirkpatrick Modeli'ni kullanarak katılımcıların ön yüzeylerini ve eğitimin ardından öğrendiklerini

ölçmüşlerdir (s. 203). Bu çalışma, kısa vadede siber güvenlik kavramlarını akılda tutmada e-öğrenmenin rolünü inceleyen ilk çalışmalardan biridir.

Güvenlik farkındalığını üç düzeyde tanımlamışlardır: algı, anlama ve öngörü. Buna göre, siber güvenlik farkındalığına sahip çalışanlar:

1. Tehditlerin varlığını algılar,
2. Tehlikelerin boyutunu anlayıp değerlendirir,
3. Gelecekteki riskli durumları tahmin edebilir (s. 197).

Bu kazanımlar çalışanın kurum için en zayıf bileşen olmaktan çıkarak güvenlik duruşunu güçlendirmesine olanak tanır. "İnsan faktörü" ya da başka bir ifadeyle "insan güvenlik duvarı"nın sürekli ihlal edildiği, birçok siber güvenlik uzmanı tarafından bilinen bir gerçektir (Diaz ve diğ., 2020; Chowdhury ve diğ., 2019).

Ayrıca, Catota ve arkadaşları (2019) farkındalık ve eğitimle öğrenenlerin "belirli saldırı türlerine karşı savunma önlemleri almada aktif rol kazanabileceğini" vurgulamıştır (s. 16).

2.2. Siber Güvenlikte İnsan Faktörleri

Hadlington'a (2017) göre, siber saldırılarda artış olduğunu gösteren raporların sayısı giderek artmaktadır ve bu durum, yol açabilecekleri yıkıcı sonuçlar nedeniyle endişe vericidir. Örneğin, başarılı siber saldırıların ekonomik maliyeti küçük, orta ve büyük kuruluşlar için önemli olabilir. Yetişkinlerin yaklaşık yüzde altmış beşinin bir tür siber saldırıya maruz kaldığı tahmin edilmektedir. Bu nedenle, siber güvenlikteki insan faktörü, birçok kuruluşun siber saldırılara karşı kendilerini korurken göz önünde bulundurması gereken kritik bir faktör olarak dikkatini çekmiştir (Hadlington, 2017). Onlarca yıldır, insan hatalarının siber güvenlik ihlallerinin temel nedenlerinden biri olduğu ve günümüzde de devam eden bir sorun olduğu belirtilmiştir. İnsan hatası endüstrilerde ve mesleklerde her zaman var olmuştur, ancak bu hataların nedenleri büyük ölçüde göz ardı edilmiş veya kaçınılmaz bir şey olarak görmezden gelinmiştir (Pollock, 2017).

İnsan faktörlerine ve hatalarına olan bu ilgisizlik, tekrar tekrar teknolojik korumalar tarafından gölgede bırakılmıştır. Örneğin, bu durum araştırmalarda görülebilir; burada siber güvenliğin ana odak noktası, insan faktörleri yerine teknolojiyle ilgili endişeler olmuştur. Ana odak, teknolojinin siber güvenlik sorunlarını çözmek için nasıl kullanılabileceği üzerindeydi. Bu nedenle, kuruluşlar çabalarını ve

sermayelerini teknolojik koruyucu önlemleri uygulamaya odaklamış, genellikle insan faktörünü göz önünde bulundurmaktan vazgeçmişlerdir. Siber güvenlikte teknik tarafı sosyal tarafa öncelik vermek daha iyi koruma sağlamaz, aksine siber güvenlik karşı önlemlerinin oluşturulmasını ve iyileştirilmesini engeller (Coffey ve diğerleri, 2017).

Bu nedenle, siber güvenliğin hem hükümetler hem de özel sektörler için üstlenilmesi gereken karmaşık bir sosyo-teknik zorluk olduğunu anlamak esastır (Khader ve diğerleri, 2021). İnsan faktörlerinin, insanların doğasındaki içsel zayıflıkları nedeniyle kuruluşların güvenliği için teknolojik tehditlerin oluşturduğundan çok daha büyük bir tehdit oluşturduğu kabul edilmiştir (Wang ve diğerleri, 2018). Siber güvenlik olaylarında, başarılı siber saldırıların kök nedenleri genellikle bir insan hatası bileşenine kadar izlenebilir. Örneğin, bir çalışma, bildirilen siber güvenlik olaylarının yüzde otuz yedisinde insan müdahalesi olduğunu ve bu eylemlerin bir şekilde başarılı siber saldırılara katkıda bulunduğunu göstermiştir.

Günümüzde, güvenlik ihlallerinin bilgi sistemlerindeki beklenmedik güvenlik açıkları tarafından oluşturulanlara kıyasla, kasıtlı veya kasıtsız olarak insan faktörlerinin bir rol oynaması daha yaygındır (Coffey ve diğerleri, 2017). Saldırganlar da bunu fark etmiş ve çabalarını ve dikkatlerini teknik zayıflıklar yerine insan doğasının zayıflıklarını istismar etmeye kaydırmışlardır. Bu durum, bu tür saldırıların siber saldırılar gerçekleştirmek için insan faktörünü istismar etmeye odaklanması nedeniyle, çeşitli sosyal mühendislik biçimleriyle ilgili tehditlere daha fazla odaklanılmasına neden olmuştur (Wang ve diğerleri, 2018).

2.2.1 Sosyal mühendislik tehditleri

Sosyal mühendislik, insan zayıflıklarını istismar etme doğası nedeniyle günümüzün daha zorlu siber güvenlik tehditlerinden biri olarak ortaya çıkmıştır (Aldawood ve Skinner, 2018). İnsanların zayıflıklarına odaklanması nedeniyle, saldırganların "en kolay nüfuz etme ilkesini" kullandığı söylenebilir. Bu, bir sistemin kendi başına güvenli olup olmadığına bakılmaksızın, kullanıcılarından daha güvenli olamayacağı anlamına gelir (Nohlberg, 2008).

Bu sosyal mühendislik uygulaması, siber güvenlik uygulamaları ve tehditleri konusunda insan bilgisizliğini ve kötü niyetli hedeflerine ulaşmak için başkalarına güvenme insan doğasını manipüle etmeyi içerir. Kimileri "sosyal mühendisliğin, kötü niyetli bir hedefe ulaşmak için insan zayıflıklarını manipüle etme sanatı" olduğunu

söyleyebilir (Aldawood ve Skinner, 2018). Şekil 2.2'de sosyal mühendislik saldırılarının aşamaları döngüsü görülmektedir.

Şekil 2.2. Sosyal Mühendislik Saldırı Aşamaları(STM-Savunma ve Güvenlik Siber Tehdit Durum Raporu)

Sosyal mühendislik saldırganlarının hedeflerini manipüle etmek için sıklıkla kullandıkları teknik, bilgiye erişim elde etmek için kendilerini bir içerdeki kişi veya bir yetkili olarak göstermektir (Nohlberg, 2008).

Sosyal mühendislik yöntemlerini kullanan saldırganlar, yalnızca evlerindeki bireyleri değil, aynı zamanda bu ortamlarda çalışan insanları hedefleyerek tüm kurumları ve şirketleri manipüle etmeye çalışırlar (Al-Otaibi ve Alsuwat, 2020).

Sosyal mühendislik saldırılarının zorluğu, insan zayıflıklarının kolayca güvence altına alınamamasıdır çünkü insanlar farklı davranırlar. Bu nedenle, tüm bu değişken zayıflıkları otomatik olarak güvence altına almak inanılmaz derecede zordur. Ayrıca, sosyal siteler sosyal mühendislik saldırılarının sık hedefidir çünkü insanlar, iletişim meşru görünecek şekilde paketlenmişse, iletişime razı olmaya daha yatkındırlar. Böylece, saldırganlar hedeflerine ulaşmak için aradıkları bilgiyi elde etmek için manipülasyon ve ikna becerilerini uygulama şansına sahip olurlar. Sosyal mühendislik, meşru kullanıcıları güvenlik kurallarını ihlal etmeye ikna ederek, gizli bilgi veya değerli

varlıklardan vazgeçmelerini sağlamak için onları manipüle etmeye dayanır (Aldawood ve Skinner, 2018).

2.2.2. Kimlik avı tehditleri

Saldırganların insanları bilgi vermeye ikna etmek için kullandığı sayısız yöntem vardır. Kimlik avı saldırıları, saldırganlar tarafından insanları gizli bilgi ve hassas verilerden vazgeçmeleri için aldatmak amacıyla kullanılan yaygın bir sosyal mühendislik yaklaşımıdır. Kimlik avı saldırıları, çoğunlukla teknik açıkları değil insanın bilişsel önyargılarını istismar etmesinden dolayı, en kalıcı siber güvenlik sorunlarından biri olmaya devam etmektedir." (İş, 2024) Saldırganlar bunu, kötü amaçlı sitelere bağlantılar içeren sahte e-postalar gönderme, telefon görüşmeleri yoluyla gizli bilgileri avlama vb. çeşitli yöntemlerle yaparlar.

Şekil 2.3. Kimlik Avı (quishing) Saldırısı(OPSWAT Blog (Quishing – QR kod kimlik avı açıklaması)

Şekil 2.3'de bulunan bu kimlik avı tehditleri, insanların siber güvenlik farkındalığı eksikliğini istismar ederek neden olabilecekleri zararlar nedeniyle kuruluşlar ve bireyler için oldukça zararlı olabilir. Örneğin, saldırganlar kuruluşlarda çalışan insanları kötü amaçlı dosya ve yazılımları indirmeye veya e-postalarına

gönderilen bağlantılara tıklamaya ikna etmeyi başarabilirler. Böylece, bu e-postaları görünüşte meşru gibi paketleyerek saldırgana kuruluşun gizli verilerine erişim sağlarlar. Kimlik avı saldırıları, teknik açıkları değil, insanın bilişsel önyargılarını istismar ederek en yaygın siber güvenlik tehditlerinden biri olmaya devam etmektedir" (İş, 2024).

Saldırganlar bu kimlik avı saldırılarını tasarlama konusunda da giderek daha sofistike hale gelmekte, o kadar ki meşru olmayanları tanımlamak giderek zorlaşmaktadır, bu da büyük bir endişe kaynağıdır. Kimlik avının bir kuruluşun sistemlerine ve ağlarına insan faktörünü istismar ederek getirebileceği zararlı sonuçlar nedeniyle, bu sosyal mühendislik saldırıları günümüzde insanların karşı karşıya olduğu en tehlikeli siber güvenlik tehditlerinden biri haline gelmiştir (Al-Otaibi ve Alsuwat, 2020). Bu tür saldırıların insan personeli üzerindeki etkileri nedeniyle (Aldawood ve Skinner, 2018), insanların siber güvenlik farkındalıklarını artırmaları ve teknolojiyle bütünleşirken gelişmiş siber hijyen oluşturmaları gerekmektedir.

2.2.3. Siber hijyen

Siber hijyen kavramı, siber güvenlik alanında insan kaynaklı ihlalleri azaltmakla yakından bağlantılıdır. Sosyal mühendislik siber saldırıları ve kimlik avı dolandırıcılıkları gibi insan faktörü etrafında dönen tehditlerin sayısı nedeniyle bu önemlidir (Neigel ve diğerleri, 2020). Siber güvenlikte, insanların zayıf siber hijyenleri olduğu yaygın olarak rapor edilen bir tema olmuştur, çünkü sergiledikleri davranışlar veya hijyen, hatalara neden olmaya ve sürekli güvenlik olaylarına yol açmaya eğilimlidir. Örneğin, insanlar başkalarıyla hızlıca parola paylaşır veya çeşitli sosyal siteler üzerinden özel bilgilerini verirler.

Siber suçların ortalama maliyeti üzerine yapılan araştırmalar, zayıf siber güvenliğin topluma önemli ölçüde pahalıya mal olduğunu göstermiştir; örneğin, siber güvenlik olayları nedeniyle ülkelerin ödemek zorunda kaldığı ortalama zarar maliyeti birkaç milyondur. Daha fazla istatistik, rapor edilen kuruluşların yüzde doksan sekizinin kötü amaçlı yazılımla ilgili saldırılar yaşadığını ve bu saldırıların yüzde yetmişinin sosyal mühendislik ve kimlik avı saldırıları olduğunu göstermektedir. Saldırganlar istismar edebilecekleri zayıflıklar ararlar ve bunlar genellikle insan faktöründe bulunur. Zayıflıkların insanlarda bulunmasının temel nedeni, zayıf siber hijyen sergilemeleridir (Cain ve diğerleri, 2018).

Siber hijyen, "Teknolojiyi tehditlere veya bilgisayar korsanlığı girişimlerine karşı düzenli olarak izleme, parolaları değiştirme ve geri dönüştürülmüş parolalardan kaçınma, virüs koruma yazılımlarını güncelleme, çevrimiçi bilgileri güvenli bir şekilde depolama ve uygun güvenlik taramaları çalıştırma" olarak tanımlanabilir (Neigel ve diğerleri, 2020). Dolayısıyla, siber hijyen esasen siber uzayda verileri ve bilgileri saldırganlardan korumak için uyulması gereken normlar ve yönergelerden oluşur (Singh ve diğerleri, 2020). Sonuç olarak, insanlar arasında iyi siber hijyeni ve güvenli davranışları teşvik etmek, kendilerini tehditlere karşı korumak için zorunludur (Cain ve diğerleri, 2018).

2.3 Siber Güvenlik Farkındalığını Artırma

Literatürde eğitim, öğretim ve farkındalık artırma rolleri arasında bir ayrım yapılmaktadır. Eğitim, güvenlik uzmanlarının siber güvenliğin tasarımı ve uygulanması için kullanılacak beceri ve yetkinliklerini tek bir bilgi sütununda birleştirdikleri alandır. Öğretim ise insanların iş faaliyetlerini gerçekleştirmelerini sağlayan güvenlik beceri ve yetkinliklerini kazandıkları alandır (Alkhazi ve diğerleri, 2022). Buna karşılık**,** siber güvenlik farkındalığı (CSF), insanların bilgi güvenliği uygulamalarını kullanarak kişisel ve kurumsal bilgileri istenmeyen düşmanlardan nasıl korumaları gerektiği konusunda farkındalık yaratmaktır. Farkındalık kavramı genellikle bir durum hakkında bilgi sahibi olmak ve insanların daha bilinçli kararlar vermesini sağlayan olası güvenlik sorunları ve tehditlerin farkında olmak olarak kabul edilir (Korovessis ve diğerleri, 2017). Esasen, birçok kişi CSF'yi kuruluşlardaki bilgi sistemleri ve ağların ilk savunma hattı olarak görmektedir. Bunun nedeni, kullanıcılar arasında iyi bir CSF'nin zarar vermek isteyenlere karşı daha sağlam bir koruma sağlamasıdır (Tasevski, 2016). CSF ayrıca "kişinin siber uzaya yönelik olası tehditleri tanımlama, zararlı olup olmadıklarını değerlendirme, kişisel bilgi ve mülkiyet güvenliğini korumak için sorunları zamanında önleme veya çözme yeteneğine sahip olması" olarak tanımlanabilir (Wang ve diğerleri, 2018).

CSF tanımlarında sayısız varyasyon vardır; ancak literatürde, kuruluşların farkındalık artırma konusunda sürekli olarak çalışmaları gerektiği konusunda bir fikir birliği vardır. "Kuruluşun tüm çalışanlarının, işlevleriyle ilgili olarak uygun farkındalık, eğitim ve öğretim ile kurumsal politikalar ve prosedürler hakkında düzenli güncellemeler alması" önerilmektedir. Bu nedenle, bu farkındalık artırma

programlarının kuruluşun genel güvenlik stratejisine dahil edilmesi tavsiye edilmektedir (Alkhazi ve diğerleri, 2022).

2.3.1 Siber güvenlik farkındalık eğitimi

Sayısız çalışma, siber güvenlik farkındalığını (SGF) artırmanın en etkili yöntemlerinden birinin kuruluşlarda eğitim programları uygulamak olduğunu öne sürmüştür (Alkhazi ve diğerleri, 2022). İnsanların siber güvenlik uygulamalarına ilişkin bilgilerini geliştirmek için kullanılan eğitim girişimleri, farkındalığı artırmak için gerekli görülmektedir. Çünkü eğitim yoluyla SGF'yi yaymak, insanları tehditleri hafifletme ve zararı en aza indirme konusunda daha yetenekli hale getirebilir (Shillair ve diğerleri, 2022). Siber uzayla entegre olurken karşılaşılan riskleri ve tehditleri daha iyi anlamak, insanları daha güvenli davranış kalıplarını veya siber hijyeni uygulamaya ve daha iyi ve daha bilinçli kararlar almaya teşvik edebilir (Szumski, 2018).

Literatürde, kuruluşların farkındalık eğitim programlarını nasıl geliştirmesi gerektiğine dair çok sayıda rehber sunulmaktadır. Yazar Alkhazi ve diğerleri (2022)'ne göre, bunlar esasen üç temel aşamaya ayrılabilir: geliştirme, uygulama ve değerlendirme. Ayrıca, SGF eğitimindeki faaliyetler birçok şekilde olabilir. Genel olarak, bir siber güvenlik eğitim programının etkili olabilmesi için bu faaliyetlerde iki önemli faktörün göz önünde bulundurulması gerekir. İlk faktör, siber uzay sürekli geliştiği için tüm eğitim bilgilerinin güncel ve alakalı olması gerektiğidir. Sistemleri koruma şansı varsa, örneğin dünyada kullanılan yeni teknolojiler veya en son sıfırıncı gün tehditleri gibi güncel gelişmeleri bilmek önemlidir. Bu nedenle, SGF programlarındaki eğitim materyalleri sürekli olarak güncellenebilir (Alkhazi ve diğerleri, 2022).

Eğitim yoluyla farkındalığı artırmak için son derece önemli olan ikinci faktör, eğitim programının nasıl tasarlandığıdır. Yani, programa hangi eğitim faaliyetlerinin dahil edildiği, kullanıcıları nasıl öğretecek şekilde tasarlandığı, programın teslimat yöntemleri vb. Güvenlik farkındalık eğitimi, kullanıcıların sadece öğrenmek ve farkındalıklarını geliştirmek istemelerini sağlamakla kalmayıp, aynı zamanda işi kendileri de sürdürmek için yeterince motive olmalarını sağlayacak şekilde geliştirilmelidir (Alkhazi ve diğerleri, 2022). Başka bir yazar olan Kävrestad ve diğerleri (2022), siber güvenlik eğitimini iki geniş kategoriye ayırır: fiziksel ve dijital güvenlik eğitimi. Fiziksel güvenlik eğitimi yüz yüze eğitimi ifade ederken, dijital eğitim

ağırlıklı olarak siber güvenlik eğitimini dijital olarak yürütmenin çeşitli yollarını ifade eder. Örneğin, kullanıcıların isteğe bağlı olarak eğitim materyallerine erişebildiği e-öğrenme platformları, oyun tabanlı ve bağlamsal eğitim gibi popüler dijital eğitim yöntemleridir. Eski eğitim yöntemi, materyali daha ilgi çekici bir şekilde öğretmek için geliştirilen sınavlar, hikâye tabanlı, rekabet tabanlı ve tek oyunculu oyunlar gibi farklı oyunları içerir. İkincisi ise, kullanıcıların bir siber güvenlik riski oluşturabilecek belirli durumlarla karşılaştıklarında eğitim materyalleri sağlandığı simülasyon tabanlı eğitimi içerir (Kävrestad ve diğerleri, 2022). SGF eğitiminin amacı, insanlara siber güvenlik hakkında düşünmenin sonuçlarını söylemek değil, insanlara siber güvenlik hakkında kendi başlarına düşünme fırsatları sunmaktır (Stahl, 2006).

Kamu kurumları için siber güvenlik farkındalığı kritik öneme sahiptir, çünkü bu kurumlar sorumlulukları altındaki büyük miktarda seçmen verisini korumakla yükümlüdür (Schürmann ve diğ., 2020; Macmanus ve diğ., 2013; de Bruijn ve Janssen, 2017). Ayrıca, kamu çalışanları tarihsel olarak siber suçluların oltalama (phishing) saldırılarında öncelikli hedefleri arasında yer alır; özellikle zaman baskısı ve teslim tarihleri gibi etkenler, onları daha dikkatsiz ve savunmasız hâle getirebilmektedir (Schürmann ve diğ., 2020; Chowdhury ve diğ., 2019; McCormac ve diğ., 2017; Kemper, 2019).

Siber güvenlik kavramlarına yönelik farkındalık eksikliği, kamu kurumlarının topladığı büyük miktardaki seçmen verisinin ihlal edilmesi riskine yol açabilir. Kamu çalışanlarının siber tehditlerle başa çıkabilmek ve bu tehditleri azaltabilmek için özel beceri ve yetkinliklere sahip olmaları gerekmektedir (Yazdanpanahi, 2021; Anwar ve diğ., 2017). Siber güvenlik farkındalığını etkileyen birkaç faktör olduğu düşünülmektedir. Bu bölümde en yaygın dört unsur ele alınacaktır:

1. Siber güvenlik eğitimi,
2. Farkındalığın ölçülmesi,
3. Demografik faktörler,
4. Tehdit algısı ve tehditlerin azaltılması.

2.3.2 Farkındalık eğitimine yönelik eleştiriler

Siber güvenlik eğitimi, siber güvenlik farkındalığını artırmak için en önemli önlemlerden biri olarak kabul edilmesine rağmen, sayısız araştırma mevcut eğitim programlarının yalnızca üçte birinin güvenlik ihlallerini azaltmada etkili olduğunu eleştirmektedir (Alkhazi ve diğerleri, 2022). Siber güvenlik farkındalık eğitimi sağlandığında bile, çoğu zaman görevlerini yerine getiremezler (Caldwell, 2016) ve Stahl'a (2006) göre, güvenlik farkındalık eğitim programlarının yüzde yetmiş beşinden fazlası uygulamadan kısa bir süre sonra başarısız olur (Stahl, 2006). Çok sayıda farkındalık eğitimi mevcuttur; ancak, kullanıcıları eğitmek ile davranışlarını değiştirmek arasında bir fark vardır. Kuruluşların, kullanıcılarını daha güvenlik bilincine sahip davranmaları için eğitimlerine sermaye yatırması, ancak örneğin eğitimin hem işyerini hem de kullanıcının siber güvenliğe yaklaşımını olumlu yönde etkileyip etkilemediğini sağlamak için eğitimi takip etmemesi alışılmadık bir durum değildir. Bu durum, kuruluşların sonunda etkisiz olan eğitime çok para harcadığı bir tuzak haline gelebilir. Kuruluşlar, davranışları değiştirmek ve kullanıcıların siber güvenlik farkındalığını artırmak için yalnızca eğitime güvenemezler; kullanıcılarının davranışlarını koşullandırmaları ve onları çözümün bir parçası olmaya dahil etmeleri ve güçlendirmeleri gerekir (Caldwell, 2016).

Siber güvenlik farkındalık eğitim programlarının etkinliğine yönelik eleştiriler, insanların risk algısını olumlu yönde gerçekten değiştirmenin zorluğu, etkili eğitim üretmek için hangi teslimat yöntemlerinin kullanılacağı konusunda anlaşmaya varma ve siber güvenlik farkındalığı (SGF) eğitimi sayesinde farkındalıkta somut iyileşmeler olup olmadığını görmek için zayıf bir şekilde oluşturulmuş değerlendirme kriterlerine sahip olma ile ilgilidir. SGF programlarının başarısının, ilgili kişileri dahil etme ve motive etme yeteneğine bağlı olduğu sıkça belirtilir. Eğitim programının etkinliği yetersiz olarak tanımlandığında, sorun genellikle kullanıcı katılımı ve motivasyon eksikliği ile ilgilidir. Bu kullanıcı katılımı ve motivasyon eksikliği, insanların farkındalık eğitimi girişimlerini sıkıcı bulmalarıyla ilgili olabilir, bu da olumsuz algılarının katılımlarını etkilemesine izin verir.

Kullanıcıları siber güvenlik hakkında öğrenmekten zevk almaya motive etmek ve dahil etmek, kullanıcıları dahil etmek ve motive etmek için çaba gösterilip

gösterilmemesine bakılmaksızın bir sorun olarak kalabilir. Bunun nedeni, insanların inatçı olmaları ve eğitimle ilgili olarak genellikle farklı ihtiyaçlara, görüşlere ve algılara sahip olmalarıdır, bu da eğitimden etkilenme olasılıklarını güçlü bir şekilde etkiler. Böylece, SGF'yi artırma yönünü zorlaştırır. Güvenlik farkındalık eğitimini daha ilgi çekici ve etkili hale getirme zorluğunun üstesinden gelmek için sürekli çabalar devam etmektedir.

Bir yaklaşım, daha iyi sonuçlar üretmesi ve güvenlik farkındalık programlarının genel etkinliğini artırması beklenen oyun tabanlı ve simülasyon tabanlı eğitim yöntemlerini kullanmaktır. Son zamanlarda, araştırmalar siber güvenlik eğitimi için 'Kişiselleştirilmiş Öğrenme Teorisi' sunmaya yoğunlaşmıştır. Bu tür bir eğitim, belirli bireysel tercihlere göre uyarlanmıştır, bu nedenle eğitim, her kişinin öğrenme hedeflerine, öğrenci profiline vb. dayanarak öğrenmeleri için ilgi çekici yollar oluşturur. Ancak, bu tür bir eğitim henüz siber güvenlik eğitimi veya farkındalık artırma programlarına uygulanmamıştır. Ancak, bu öğrenme yöntemi gelecekte bu amaçlar için mevcut olabilir (Chowdhury ve diğerleri, 2019).

2.3.3 Siber güvenlik farkındalığını artıran eğitim dışındaki faktörler

Akademide, insan faktörünün "güvenlikteki en zayıf halka" olduğu (Bélanger ve diğerleri, 2022) ve bu zayıflığı gidermenin nihai yolunun güvenlik farkındalık eğitiminin uygulanması olduğu (Alkhazi ve diğerleri, 2022) defalarca ortaya konmuştur; ancak, eğitimin ötesindeki diğer faktörler de farkındalığı artırmak için aynı derecede önemli olabilir. Motivasyon, insanların siber güvenlik en iyi uygulamalarını benimsemeleri ve kurumsal güvenliğe fayda sağlayan siber güvenlik davranışlarında bulunmaları için teşvik edilmelerinde büyük rol oynar. Bu, özellikle insanların siber güvenlik konusunda genellikle olumsuz algılara sahip olması ve bu olumsuz kullanıcı algılarının üç alt faktöre ayrılabilmesi nedeniyle önemlidir. İlk alt faktör, güvenliğin korkutucu olması, ikincisi güvenliğin anlaşılmasının karmaşık olması ve üçüncüsü güvenliğin sıkıcı olmasıdır. Kullanıcıların siber güvenliğe yönelik hisleri, kuruluşların siber güvenlik uygulamalarını ve teknolojilerini uygulayamamasının ve etkin bir şekilde kullanamamasının kısmen sorumlusu olmuştur, bu da kullanıcı algısını başarılı farkındalık artırma için hayati hale getirmektedir. Bu nedenle, kuruluşların siber güvenlik uygulamalarını takip etmeleri, yeni teknolojileri kabul etmeleri ve daha siber güvenlik bilincine sahip davranışları kolaylaştırmaları için kullanıcıları daha iyi motive

etmek ve dahil etmek amacıyla, kullanıcıların hissedebileceği bu olumsuz algıları ele almak esastır (Haney ve Lutters, 2017).

Kurumsal siber güvenlik farkındalığını (SGF) savunanların, insanları güvenlik konusundaki olumsuz algılarını aşmaları için motive edebilmesi gerekir. Bunu başarmanın ön koşullarından biri, güvenilir bir bilgi kaynağı olarak görülmektir. Etkilenmesi hedeflenen insanlar arasında güven oluşturmak, başarılı farkındalık artırma için çok önemlidir. Bu genellikle, güvenilirliği sağlamak için kuruluşun itibarına güvenerek, iyi teknik bilgi sergileyerek, güveni teşvik eden ilişkiler kurarak ve güvenilirliği kazanmak için içeriden gelen güveni kullanarak gerçekleştirilir. Ayrıca, motivasyonun insanların siber güvenliğe ilişkin olumsuz algılarını değiştirmeye çalıştığı birkaç yol olmuştur. Siber güvenliğin korkutucu olduğu algısına sahip insanlar için motivasyon yaratma yolları, siber güvenliğin neden önemli olduğunu dürüstçe ve insanları harekete geçmeye teşvik ederek iletmeyi içerir.

Bu, riskler ve güvenlik iyi bir şekilde tesis edilmediğinde neyin tehlikede olduğu konusunda açık sözlü olmak ve insanlara umut aşılamak anlamına gelir, böylece davranışlarını değiştirmenin anlamsız olmadığına inanırlar. Siber güvenliğin karmaşık olduğu algısına sahip insanlar için motivasyon yaratmanın diğer yolları, teknik ve teknik olmayan kullanıcılar arasında ortak bir zemin oluşturmak, kullanıcılara güvenlik davranışlarını nasıl iyileştirebileceklerine dair basit talimatlar sağlamak, pratik ve öncelikli güvenlik önerileri sunmak ve güvenliğin karmaşıklığını ve yükünü hafifletmek için teknolojilerin ve politikaların kullanılabilirliğini teşvik etmektir (Haney ve Lutters, 2017). Dahası, siber güvenliği sıkıcı, alakasız, yatırıma değmez vb. olarak algılayan insanlar için motivasyon yaratmanın yolları vardır. Bu yollar, kullanıcıları iç ve dış motivasyonlarına hitap ederek iyi güvenlik davranışlarına yatırım yapmaya ikna etmeyi içerir. Bu, örneğin "tek beden herkese uyar" yaklaşımını teşvik etmek yerine güvenliği satarken bir bireyin özel ihtiyaçlarına uyum sağlamayı içerir.

Güvenliğin sıkıcı olduğuna inananlar için motivasyonu artırmak amacıyla, örneğin güvenlik uyarlamasının desteklendiği bir kültürü teşvik etmek için bir ödül ve sonuç sistemi oluşturulmuştur. Diğerleri, insanların ilgisizliğini aşmak için siber güvenliğin önemi hakkındaki iletişimlerini coşku ve ilişkilendirilebilir hikayelerle doldurmaya çalışmıştır. Diğerleri ise güven oluşturmak, farkındalık yaratmak ve insanları harekete geçmeye motive etmek için bunu güvenlik dışı risk alanlarıyla ilişkilendirmeye çalışmıştır (Haney ve Lutters, 2017). SGF'yi artıran ve motivasyon yaratma ile yakından iç içe olan bir diğer önemli faktör, bir siber güvenlik kültürü

geliştirmek ve beslemektir. Bir siber güvenlik kültürünün rolü, bir kuruluşun siber güvenlik politikalarının dikte edilmesi ile insanların güvenlik davranışları arasındaki boşluğu kapatmaktır, çünkü bir SGF eğitim programının etkinliği nihayetinde insan faktörüne ilişkin motivasyonlara ve davranışlara bağlıdır. Davranış, insanların sahip olduğu bilgi türüne, algılarına ve içgüdülerinin onlara ne yapmaları gerektiğini söylemesine bağlı olduğu için insanların davranışlarını anlamaya önemli ölçüde dikkat edilmiştir (Stahl, 2006).

Bir siber güvenlik kültürü, literatüre bağlı olarak çeşitli şekillerde tanımlanabilir; örneğin, iki yazar siber güvenlik kültürünü "grubun öğrendiği paylaşılan temel varsayımların bir deseni; dış adaptasyon ve iç entegrasyon sorunlarını çözerken yeterince iyi çalışmış ve bu nedenle, bu sorunlara ilişkin doğru algılama, düşünme ve hissetme yolu olarak yeni üyelere öğretilmesi gereken bir desen" olarak tanımlar (Gcaza ve Von Solms, 2017; Stahl, 2006). Başka bir yazar, kültürleri, kuruluşun ortamının bir parçası olanların kolektif değerleri, normları ve bilgileri içinde sıkça ifade edilen varsayımlar ve inançlar olarak açıklar. Bu kolektiflerin sonucu, bu ortamdaki insanlar arasında aranan bir güvenlik davranışını teşvik eder veya aşılar (Ramluckan ve diğerleri, 2020). Ayrıca, başka bir yazar siber güvenlik kültürünün tanımını, bir grup insanın davranışlarını etkileyen algıları, duyguları ve düşünceleri paylaştığı bir şekilde, dünyanın nasıl olması gerektiğine kıyasla nasıl olduğu hakkında temel varsayımları sunmanın bir yolu olarak sunar. Siber güvenlik kültürü fenomenine ilişkin tanımlardaki farklılıklar, bunun nispeten yeni bir kavram olmasındandır. Araştırmacılar, kültürü bir kuruluşun güvenliğine dahil etmenin önemini ancak bu yüzyılın başından beri fark etmişlerdir. Bu nedenle, henüz geniş çapta kabul görmüş temel kavramlar, belirlenmiş tanımlar veya bir siber güvenlik kültürü için yönergeler bulunmamaktadır. Bir siber güvenlik kültürünün neyi gerektirdiğine dair birleşik bir resim olmadan, tanımlarda ve bu kavramların kuruluşlarda pratik olarak nasıl yorumlandığı ve uygulandığı konusunda her zaman bir farklılık olacaktır (Reegård ve diğerleri, 2019). Ancak literatür, insanlarda olumlu siber güvenlik davranışını etkilemek için olumlu siber güvenlik hijyenini teşvik eden bu ortamları oluşturmak ve geliştirmek için büyük bir ihtiyaç olduğu konusunda hemfikirdir (Hadlington, 2017).

Bir siber güvenlik kültürü oluşturmak ve farkındalığı artırmak için, güçlü, kararlı bir liderin bir kuruluşu denetlemesi gerekir. Bu görev, gerekli kültürel değişimi mümkün kılmak için Bilgi Güvenliği Yöneticisi (CISO) iş tanımının bir parçası olabilir. Çünkü bir liderden güçlü bir taahhüt, enerji ve zaman ile, bir siber güvenlik alt

kültürünü kuruluşun baskın kültürünün işleyişine kademeli olarak yerleştirmek mümkündür (Stahl, 2006). CISO iş tanımı, "bilgi varlıklarının ve BT sistemlerinin korunmasını ve güvenliğini sağlamaktan ve bu korumanın kuruluşun stratejik yönüyle uyumlu olmasından sorumlu stratejik düzeyde bir pozisyon" olarak tanımlanabilir (Hooper ve McKissack, 2016). Bu nedenle, bir CISO kuruluşun kültürünü şekillendirebilir ve biçimlendirebilir, böylece zamanla o ortamdaki insanlar doğru davranır, güvenlik davranışlarına dikkat eder ve hatta birbirlerini eğitirler. Kültür, bir grup insanın belirli bir şekilde davranmaya başladığında daha fazlasının liderliği takip etme eğiliminde olduğu hedefiyle sosyal ilişkilere dayanır.

Güçlü liderlik, insanları bir siber güvenlik kültürünü geliştirmeye ve beslemeye katkıda bulunmaya motive etmek ve yönlendirmek için zorunludur. Dolayısıyla, SGF'yi artırmak için önemli bir alt faktördür. Belirtildiği gibi, bir kültürü değiştirmek, siber güvenlik hakkında nasıl algıladıklarını, düşündüklerini ve hissettiklerini değiştirmeleri beklenen insanlardan ilişkiler kurmak ve güven beslemekle ilgilidir. İkna ve kullanıcı katılımının etkili farkındalık artırma için bu alanlarda gerekli olması nedeniyle, motivasyon ve siber güvenlik kültürü burada yakından iç içedir (Stahl, 2006).

2.4. Siber Güvenlik Eğitimi

Eğitim süreci, siber güvenlik farkındalığına sahip bir zihniyet kazandırmak için kullanılabilir. Eğitim stratejileri, “siber saldırılara karşı ulusal yanıtımızda yeni düşünme yolları, yeni anlayışlar ve yeni stratejiler uygulamak” amacıyla kullanılabilir (Kessler ve Ramsay, 2013, s. 36). Çalışanların siber güvenlik kavramlarını anlaması, ortalama bir internet kullanıcısının siber tehditleri tanımlamasını ve hatta bunları azaltmasını sağlayarak öz-yeterliklerini artırabilir (Olmstead ve Smith, 2017b).

Kessler ve Ramsay (2013) ayrıca, “eğitimin bireylere siber güvenlik disiplini hakkında sistematik bir anlayış kazandırdığını” belirtmektedir (s. 40). Yönetimin siber güvenlik eğitimine destek vermesi, farkındalığı artırabilir ve bu farkındalık; politika, prosedürler ve teknolojik altyapıyla birlikte organizasyonların güvenlik duruşunu güçlendirmelerine olanak tanır.

2.4.1. Siber güvenlik eğitimi için paradigmalar

ABD İç Güvenlik Ajansı (DHS), daha fazla siber güvenlik eğitiminin yaygınlaştırılması konusunda öncü devlet kurumlarından biri olmuştur (Kessler ve Ramsay, 2013). Kessler ve Ramsay (2013), federal hükümetin, 2002 yılında çıkarılan İç Güvenlik Yasası ile birlikte akademik kurumları "İç Güvenlik eğitimi konusunda aktif bir rol almaya" yönlendirdiğini belirtmektedir (s. 37). Hükümet araştırmaları, ABD'nin "siber güvenlik uzmanlığı eksikliği" yaşadığını ve yaklaşan bir "Siber Pearl Harbor" saldırısına karşı hayatta kalma şansını artırmak için çok az çaba gösterildiğini ortaya koymuştur (s. 36).

Vatandaşlar arasındaki siber güvenlik farkındalığının düşük olması ve yaşlanmış ancak kritik öneme sahip altyapının varlığı, ABD İç Güvenlik Bakanlığı'nın siber güvenliği ülkenin öncelikli güvenlik konularından biri hâline getirmesine neden olmuştur. Kessler ve Ramsay (2013), siber güvenlik programlarının geliştirilmesi ve bu programların akademik müfredata entegre edilmesine yönelik paradigmalar önermektedir. Yazarlar ayrıca, öğrencilere zorla siber güvenlik programları dayatmanın işe yaramayacağını ve tehditleri anlayabilmek için tam uzmanlık gerekmeyeceğini savunmaktadır.

Önerilen müfredat; günlük operasyonlar, yapılandırılmış yönetim, politika, prosedürler, roller ve ilgili yasal düzenlemeleri içermektedir. Bu yapı, öğrencilere siber risklerle başa çıkabilmeleri için gereken spesifik beceri ve yetkinlikleri kazandırırken, "eğitim bireylere siber güvenlik disiplini hakkında sistematik bir anlayış sağlar" (Kessler ve Ramsay, 2013, s. 40). Önerilen müfredat ve öğretim yöntemi, öğrencileri yıldırmamak adına teknik detaylardan uzak ve genel yapıdadır. Ayrıca, bu paradigma "scaffolding" (aşamalı öğrenme) gibi tekniklerin kullanımını önerir; böylece öğrenciler, öğrendikleri bilgileri ülke güvenliği ile ilgili diğer alanlara uygulayabilirler.

Bu tür bir paradigma tüketici tabanlı eğitime uyarlandığında, benzer bir öğretim yaklaşımının benimsenmesi –sistematik anlayış sağlayan, aşırı teknik olmayan ve en önemlisi katılımcının günlük yaşamına uygulanabilir olan– oldukça önemlidir (Yazdanpanahi, 2021; Carlton, 2016). Siber güvenlik, çalışanın organizasyon içindeki rolüyle tutarlı ve ilgili olmalıdır.

Bu müfredat, İç Güvenlik Bakanlığı tarafından siber suçluların organizasyonlara yönelik tehditlerini azaltmak amacıyla önerilmektedir. DHS, ülkenin siber güvenliği hakkında endişe duymakta olup, eyalet ve yerel kurumların birincil hedef hâline

geldiğini belirtmektedir (Kessler ve Ramsay, 2013; Macmanus ve diğ., 2013; Schürmann ve diğ., 2020). Kendi ajanslarının güvenliği konusunda güçlü bir sahiplenme duygusunun gerekli olduğunu ve yerel kurumların ulusal hükümet kadar hedef alınma ihtimalinin yüksek olduğunu ifade etmektedirler. Eğitim, yerel kamu kurumlarının siber saldırılardan sağ çıkma şansını artıran ve genel siber risklerini azaltan değerli bir araçtır (Yazdanpanahi, 2021).

Kortjan ve Solms (2014), "siber uzay sonsuz hizmet ve fırsatlar sunsa da, birçok internet kullanıcısının farkında olmadığı pek çok riskle de birlikte geldiğini" belirtmektedir (s. 29). Kessler ve Ramsay (2013), "genel olarak teknik becerileri düşük olan bir öğrenci kitlesine teknik okuryazarlık kazandırmanın zor olduğunu" ve bu durumun, çalışanlara veya bireylere ihtiyaç duyduklarını bilmedikleri teknik içerikleri öğretmeyi daha da güçleştirdiğini savunmaktadır (s. 41).

Siber güvenlik farkındalığı olmayan tek bir çalışanın, bir kuruma milyonlarca hatta milyarlarca dolara mal olabilecek veri ihlallerine yol açabileceği ve bu durumun kurumlar için pahalı bir utanç kaynağı olabileceği ifade edilmektedir (Skertic, 2021; Kostyuk ve Wayne, 2020). Bu tür ihlaller veya fidye saldırıları organizasyonlar için felaket niteliğinde kayıplar anlamına gelirken, siber suçlular için büyük kazançlar anlamına gelebilir.

Kortjan ve Solms (2014), "hedef kitleye kendileriyle ilgili konuların sunulması gerektiğini" önererek, içeriğin daha erişilebilir ve kullanıcı dostu hâle getirilmesinin, teorik olarak daha fazla siber güvenlik farkındalığına sahip bireylerin yetişmesini sağlayabileceğini ve bu sayede siber güvenlik olaylarının yaşanma olasılığının azaltılabileceğini belirtmektedir (s. 33). Bu görüş, Schürmann ve arkadaşları (2020) tarafından da desteklenmiştir; onlar, "siber güvenlik eğitiminin hedef kitle tarafından anlamlı ve ilgili olarak algılanması gerektiğini" savunmaktadır (s. 199).

Kortjan ve Solms (2014), ayrıca "eğitimin güvenli davranış kültürünün geliştirilmesinde kritik bir rol oynadığını" bulgulamıştır (s. 29). Günümüzde insanlar ve çalışanlar, günlük faaliyetlerinin çoğunda internete bağımlıdır. Diaz ve arkadaşları (2020), dijital bir toplumda bile aktif internet kullanıcılarının siber güvenlik farkındalığının eksik olmasının kişisel bilgilerini riske attığını ve "değerli ve gizli bilgilerin elde edilmesi için kullanıcıları kandırmaya yönelik sosyal mühendislik taktiklerinin hızla arttığını" belirtmektedir (s. 53).

Tirumala ve arkadaşları (2016) da bu görüşü destekleyerek, "siber güvenliğin çoğu kişi tarafından yanlış anlaşıldığını, sadece internet üzerindeki bilgisayarların

güvenliğini sağlamakla sınırlı olmadığını" ve insan faktörünün en az makineler kadar önemli olduğunu ifade etmektedir (s. 1). Teknoloji konusunda deneyimsiz internet kullanıcıları, siber suçlarla ilişkili taktiklere şaşırtıcı derecede açıktır ve "şu anda sosyal mühendislik, bireysel bilgi ve özel verileri çalmak için en yaygın kullanılan yöntemlerden biridir" (s. 2).

Eğitsel içeriklerin uygulanması, çalışanların siber güvenlik kavramlarını anlama ve öğrenme yoluyla bu tür tehditlere karşı davranışsal bir değişim yaratabilir (Kostyuk ve Wayne, 2020; Peker ve diğ., 2016). Dünya giderek daha fazla birbirine bağlı hâle gelirken, siber alanın güvenliğinden herkesin sorumlu olduğu unutulmamalıdır (Kessler ve Ramsay, 2013).

2.4.2. Kötü amaçlı yazılım eğitimi yoluyla çalışanların siber güvenlik kapasitelerinin artırılması

He ve arkadaşları (2020), multimedya kullanımı ve basılı siber güvenlik risk raporlarının dâhil edilmesiyle siber güvenlik eğitiminin etkinliğini artırmaya yönelik yöntemleri incelemiştir. Ayrıca, farklı medya kombinasyonlarından oluşan bir eğitim programıyla birlikte ön test-son test anketleri uygulamışlardır. Bu çalışmada, multimedya ile birlikte basılı risk raporlarının kullanımı gözlemlenmiş ve bu uygulamaların eğitim üzerindeki etkisini, katılımcıların "güvenlik açıklarına karşı algıladıkları kırılganlık, tehdidin ciddiyeti, öz-yeterlilik, güvenlik niyeti ve kendi bildirdikleri siber güvenlik davranışlarındaki değişim" açısından değerlendirmek amaçlanmıştır (s. 208).

Araştırma sonucunda, multimedya kullanımının etkisinin sınırlı olduğu; ancak eğitim sağlama ya da "insan yamalama" (people patching) yaklaşımının, katılımcıların siber tehditleri tanıma, önleme veya tamamen kaçınma becerilerini geliştirdiği ortaya çıkmıştır (s. 209). Bu, çalışanların yeni siber tehditler hakkında düzenli olarak bilgilendirilmesi ve bu tehditleri nasıl tanıyacaklarının öğretilmesini de içermektedir; böylece iş yerindeki kesintilerin önüne geçilebilir. Eğitimin etkinliğini artırmanın bir diğer önemli unsuru ise, "siber farkındalığı çalışanların kişisel hayatı, ailesi ve eviyle ilişkilendirmek"tir. Bu yaklaşım, eğitimi daha ilgi çekici hâle getirebilir ve çalışanları hem kişisel hem de profesyonel hayatlarında siber güvenlik davranışlarını değiştirmeye teşvik edebilir (s. 210).

Temel olarak, bir organizasyonun çalışanlarını siber güvenlik farkındalık eğitimiyle buluşturma yönünde gösterdiği her çaba faydalıdır. Ancak eğitimin kalitesi ne kadar yüksek olursa, elde edilen sonuçlar da o kadar etkili olacaktır (Daengsi ve diğ., 2021; Yazdanpanahi, 2021; Peker ve diğ., 2016; Costa ve diğ., 2019).

2.4.3. Siber güvenlik olaylarında eğitimin etkinliği

Heartfield ve Loukas (2018) ile Carlton (2016), siber güvenlik eğitiminin uygulanması veya yürütülmesinde öz-yeterlik kavramının en büyük endişe kaynaklarından biri olduğunu öne sürmektedir. Kweon ve arkadaşları (2019), önerilen bir eğitimin etkinliğini ölçmek amacıyla, siber güvenlik olaylarının sayısı ile bu olayların siber güvenlik eğitimiyle ilişkisini incelemiştir. Araştırmacılar, insan hatasının siber güvenlik olaylarının en önemli nedenlerinden biri olduğunu ve bu durumun ciddi bir endişe kaynağı olduğunu vurgulamaktadır.

Birçok organizasyon fiziksel güvenliğe yatırım yapmaya istekliyken, siber güvenlik eğitimine yapılan yatırımlarda geri dönüş (ROI) sağlayamayacağını düşünerek aynı ilgiyi göstermemektedir (Kweon ve diğ., 2019). Son araştırmalar, fidye yazılımlarına bağlı siber saldırıların artmakta olduğunu ve bu saldırıların genellikle sosyal mühendislik ve oltalama gibi tekniklerle çalışanları hedef aldığını göstermektedir. Bu saldırıların maliyeti oldukça yüksektir (Kweon ve diğ., 2019; Yazdanpanahi, 2021; Kostyuk ve Wayne, 2020).

Kweon ve arkadaşları (2019), bir organizasyondaki siber güvenlik farkındalığı seviyesinin anlaşılmasının, siber risklerin azaltılmasında kritik bir rol oynadığını vurgulamaktadır. Araştırmalarında, gerçekleştirilen eğitim programları sonrasında siber güvenlik olaylarının sayısında meydana gelen değişiklikleri gözlemleyerek ve bu verileri nicel olarak analiz ederek, siber güvenlik eğitiminin gerçek etkisini değerlendirmişlerdir. Ayrıca, etkili bir siber güvenlik kültürünün oluşturulabilmesi için eğitimlerin yalnızca çalışanlarla sınırlı kalmaması, aynı zamanda yönetici ve bölüm başkanlarını da kapsaması gerektiğini belirtmişlerdir. Nitekim yürütülen anket çalışması, güvenlik ihlallerinin %28'inin doğrudan yönetim kadrosunun siber güvenlik farkındalığındaki eksiklikten ve siber güvenliğe yeterince öncelik vermemesinden kaynaklandığını ortaya koymuştur (Kweon et al., 2019, s. 4). Bu bulgu, üst yönetimin siber güvenlik konusunda aktif rol almasının, kurumsal güvenliğin sağlanmasında belirleyici olduğuna işaret etmektedir.

Yazarlar ayrıca, siber güvenlik konusunda pasif bir duruş sergileyen kurumların, çalışanlarının da siber sorumluluklarını ihmal etme eğiliminde olduğunu belirtmektedir. Bununla birlikte, nitelikli teknik personel eksikliği bulunduğunu ve özellikle eğitim verme yeterliliğine sahip personelin sayısının daha da az olduğunu gözlemlemişlerdir. Kweon ve arkadaşlarının (2019) çalışmasının sonucuna göre, siber güvenlik kavramlarına ve eğitimine daha fazla zaman ayrılması, siber riskin azaltılması açısından daha faydalı olacaktır.

Bu, siber güvenlik eğitimine katılan çalışanlar ile siber tehditlerin azalması veya yavaşlaması arasında bir korelasyon olduğunu ortaya koymaktadır. Benzer şekilde, eğer eğitim sonrası tehdit olaylarının sayısı artıyor ya da sabit kalıyorsa, araştırmacılar çalışanların eğitimine ilişkin tehditlerle anlamlı bir ilişki olmadığını ifade edebilir. Ayrıca, yazarlar verilerinin soyut nitelikte olmasına rağmen, organizasyonlar için temel varlıklar arasında yer aldığını ve bu nedenle kritik öneme sahip olduğunu yinelemektedir. Siber güvenlik olaylarından doğan zararlar soyut değil, fiziksel olup parasal maliyetlerle doğrudan ilişkilidir (Kweon ve diğ., 2019).

Yazarlar ayrıca, siber güvenlik eğitiminin çalışanların siber riskleri azaltma becerilerini geliştirdiğini kabul etmektedir. Genel olarak, bir organizasyonun çalışanlarının eğitilmesi, kurumun dış tehditlere karşı korunmasına olumlu katkı sağlar. Siber güvenlik eğitiminin yalnızca ilgili olması değil, aynı zamanda düzenli olarak verilmesi gerektiği de Kortjan ve Solms (2014), de Bruijn ve Janssen (2017), Adorjan ve Ricciardelli (2019) ve Yazdanpanahi (2021) tarafından önerilmektedir.

2.5. Farkındalığın Ölçülmesi

Bir organizasyondaki siber güvenlik farkındalığı düzeyini anlamak, bir siber saldırı karşısında hayatta kalmak ya da kaybetmek arasındaki farkı yaratabilir; bu farkındalık, o organizasyonun iş gücü içinde ölçülür. Bir organizasyonun çalışanları, genellikle güvenlik duruşundaki en zayıf halka olarak görülmekte ve çoğu zaman güvenlik ihlallerinin kaynağı olmaktadır; bu durum pek çok siber güvenlik uzmanı tarafından iyi bilinen bir sorundur (Diaz ve diğ., 2020; Chowdhury ve diğ., 2019).

Araştırmacılar, siber güvenlik farkındalığı düzeylerini düşük, orta ve yüksek olarak kategorize etmiş; ayrıca teknoloji kullanımı ve siber güvenlik bilgisi konularındaki dikkatsizlik ya da özenli davranışları anlamak için veri analitiğini kullanmışlardır (Zwilling ve diğ., 2020; Tirumala ve diğ., 2016).

Eğitim programının etkinliğini değerlendirmek ve bu programın belirli bir toplulukta siber güvenlik farkındalığı kavramlarını artırıp artırmadığını analiz etmek, öğrenme içeriklerinin geliştirilmesine katkı sağlar ve organizasyonların daha güçlü bir siber güvenlik duruşuna ulaşmasına destek olur.

Siber güvenlik bilgisi ve farkındalığı, araştırma sonrası da devam eden farkındalık ve eğitim içeriklerinin düzenli sunulmasıyla sürdürülebilir. Bunlar arasında, çalışanların öğrendiklerinden ne kadar faydalandığını ölçmek için rastgele gönderilen "sahte oltalama" e-postaları gibi periyodik değerlendirmeler yer alabilir. Eğitim programlarının organizasyonlar tarafından yaygınlaştırılması, "son kullanıcı kaynaklı risklerin etkilerini dikkate almalı, bu riskleri azaltma fırsatlarını göz önünde bulundurmalı ve bilgiye dayalı kararlar verebilecek bir iş gücü oluşturmalıdır" (Miller, 2017, s. 13). Böyle bir iş gücü, sorunun değil çözümün parçası olabilir.

2.5.1. Siber güvenlik farkındalığı ile ilişkili faktörler

Daengsi ve arkadaşları (2021), siber güvenlik ihlalleriyle ilişkili tehditlerin, çalışanların siber güvenlik farkındalığına sahip olmaları durumunda azaltılabileceğini savunmaktadır. Kortjan ve Solms (2014) ise bu farkındalığın, çalışanlara siber güvenlik kavramları hakkında ilgili bilgi ve eğitim sağlanarak geliştirilebileceğini ifade etmektedir. Daengsi ve arkadaşları (2021), siber güvenliğe dair "en iyi uygulamalar, kavramlar, politikalar, güvence mekanizmaları, rehberler, koruma önlemleri, eylemler, risk yönetim yöntemleri, eğitimler, araçlar ve kullanıcı varlıklarını ve organizasyon ortamını korumaya yönelik teknolojilerin" yaygınlaştırılmasını önermektedir (s. 102).

Daengsi ve arkadaşları (2021), farklı şirket departmanları arasında siber güvenlik simülasyonları (phishing saldırıları) aracılığıyla farkındalık düzeylerini test etmiş ve "aynı organizasyon içindeki teknoloji temelli departmanlar (örneğin, BT departmanı) ile sosyal temelli departmanlar (örneğin, İnsan Kaynakları departmanı) arasında siber güvenlik farkındalığı düzeyinde anlamlı farklar" olduğunu ortaya koymuştur (s. 102). Ayrıca, çalışanların siber güvenlik farkındalığı geliştirme süreçlerine dahil edilmeleri sonucunda bu farkındalığın arttığı gözlemlenmiştir.

Buna ek olarak, Daengsi ve arkadaşları (2021) ile Diaz ve arkadaşları (2020), siber güvenlik farkındalığının; eğitim geçmişi, iş deneyimi, çalışma alanı, cinsiyet, yaş ve sosyoekonomik durum gibi çeşitli demografik faktörlerden etkilendiğini belirtmektedir. Ayrıca, siber güvenlik farkındalığını, siber tehditlere ve saldırılara

teknik yollarla ve çalışanların çabalarıyla doğru şekilde tepki verebilme yetisi olarak tanımlamaktadırlar.

Yazdanpanahi (2021) ve Costa ve arkadaşları (2019), siber güvenlik farkındalık eğitimi sağlanmasının yatırım geri dönüşünün, çalışanların şirket varlıklarını siber tehditlere karşı koruma becerilerinde yattığını ve böylece onları "potansiyel bir sorunun değil, çözümün bir parçası" hâline getirdiğini savunmaktadır (s. 2036).

2.5.2. Siber güvenlik farkındalığı ve bilgi

Bilgi teknolojilerinin ve internetin gelişimi, "netizen" ya da dijital vatandaş olarak adlandırılan yeni bir tüketici türüyle birlikte, yeni bir tüketilebilir kaynak ortaya çıkarmıştır (Zwilling, 2020, s. 1). Ancak bu yeni dijital tüketiciler, çevrim içi ortamda kendilerini siber suçlardan korumak için yeterli farkındalığa ya da asgari bilgiye çoğu zaman sahip değildir. Bu güvensiz davranış, onların çalıştıkları organizasyonların güvenlik duruşundaki en zayıf halka hâline gelmelerine neden olur.

Zwilling ve arkadaşları (2020) tarafından yapılan bir çalışmada, siber güvenlik farkındalık düzeyleri düşük, orta ve yüksek olarak sınıflandırılmış ve bu sınıflandırma aracılığıyla internet kullanıcılarının teknoloji kullanımı ve siber tehdit bilgisine karşı ne derece dikkatsiz veya dikkatli oldukları ortaya konmuştur. Ayrıca, siber güvenlik farkındalığı, "kullanıcıların bilgi güvenliğinin önemi hakkında sahip oldukları anlayış düzeyi ile bu güvenliği sağlamak için yeterli kontrol uygulama sorumluluğunu ve davranışını gösterme derecesi" olarak tanımlanmıştır (Zwilling, 2020, s. 2). Dolayısıyla bireyler ve organizasyonlar genelinde siber güvenlik farkındalığı eksikliğini azaltmak için ek eğitime ihtiyaç duyulmaktadır. Bu nedenle, bu eğitim programları özellikle devlet kurumları başta olmak üzere bazı organizasyonlarda zorunlu hâle getirilmiştir.

İnternet tabanlı teknolojilere olan bağımlılık hem kamu hem özel tüm modern organizasyonlarda artarken, internet kullanıcılarının siber tehditler konusundaki bilgi düzeyi aynı oranda artmamıştır. Araştırmalar, "kendini uzman olarak tanımlayan bireylerin, siber hijyen bilgisi konusunda, uzman olmadığını söyleyen bireylerden daha düşük bilgiye sahip olduğunu" ortaya koymuştur; bu durum, siber güvenlik alanındaki hızlı değişimin sürekli ve tutarlı eğitim gerektirdiğini göstermektedir (Zwilling, 2020, s. 3).

Davranış değişikliği, siber güvenlik farkındalığının nihai hedeflerinden biridir. Çalışanların risk alma eğilimleri ve öz-yeterlik düzeyleri, organizasyon açısından

taşıdıkları tehdit seviyesinin iyi bir göstergesidir. Bu durum, sürdürülebilir davranış değişikliği sağlamak ve çalışanların siber güvenlik bilgilerini artırmak için ek farkındalık eğitimi gerekliliğini ortaya koymaktadır.

2.5.3. İnternet kullanımı ve siber güvenlik farkındalığının ölçülmesi

Hem kamu hem de özel sektör, hizmetlerinin önemli bir kısmını hızla internete taşımakta, bu sürece "siberleşme" adı verilmektedir. İnternet kullanımındaki bu hızlı artış –özellikle son on yılda gerçekleşen– siber suçlarda da eş zamanlı bir artışa neden olmuştur. Siber suçlar, yani internet ya da siber uzayda işlenen yasa dışı eylemler, kurumları çalışanlarına uygun siber güvenlik farkındalık eğitimi sunmaya zorlamaktadır; zira "çalışanlar, işletmeler için en büyük siber güvenlik tehditlerini oluşturmaktadır" (Kemper, 2019, s. 11). Bu görüş, Peker (2016) tarafından da desteklenmektedir; "güvenli siber davranış kültürü oluşturma ihtiyacı önemli ölçüde artmaktadır" (s. 3). Bu siber farkındalık kültürünü oluşturmanın tek yolu ise, uygun eğitsel kurslar ve iyi yapılandırılmış, yaygınlaştırılmış güvenlik politikalarıdır.

Bir siber farkındalık eğitimi geliştirebilmek için, öncelikle hedeflenen kitlenin mevcut farkındalık düzeyinin ölçülmesi gereklidir. Tirumala, Valluri ve Babu (2016), mevcut bilgi düzeyini ölçmek amacıyla "belirli bir kitlenin siber güvenlik farkındalığını kapsamlı biçimde anlayabilmek için anketlerin" kullanılabileceğini önermektedir (s. 1).

Tirumala ve arkadaşlarının (2016) gerçekleştirdiği anket bazı değerli veriler ortaya koymuştur: Katılımcıların %80'inden fazlası internete evdeki geniş bant bağlantısı üzerinden erişmektedir; toplam katılımcıların yalnızca %38'i aktif internet güvenliği önlemleri uygulamaktadır ve yaklaşık %10'luk bir kesim güvenlik konusunda çok az endişe duymakta ya da hiç endişe duymamaktadır. Bu endişe verici bulgular, siber farkındalık ihtiyacını daha da pekiştirmektedir.

Bu tür metrikler, eğitsel içerik geliştiricilerine rehberlik edebilir. Tirumala ve arkadaşları (2016), "siber güvenlik farkındalığı oluşturma sürecine öncülük edecek bir çerçeve" önermiştir (s. 1). Bu çerçeve; parolalar, siber zorbalık ve yaygın siber suç tekniklerini dikkate alan bir yapıdadır. Belirli bir kitlenin zihinsel tutumunu ve mevcut bilgi düzeyini değerlendirmek, siber risk farkındalığına yönelik öğretim içeriği hazırlamak açısından oldukça önemlidir.

2.5.4. Veri analitiği ile siber güvenlik farkındalığının artırılması

Tirumala ve arkadaşlarının (2016) sunduğu istatistiksel analiz verileri, ders materyallerinin geliştirilmesinde kullanılmak üzere bir siber farkındalık çerçevesinin oluşturulmasına veri sağlasa da, bu analiz bireyin ders içeriğine verdiği değerle ilgili nitel "insan faktörü" verisini dikkate almamaktadır. Eğitim materyali, konusu ne olursa olsun, eğer öğrenen kişi için ilgi çekici değilse veya anlaşılamayacak şekilde tasarlanmışsa, etkisiz kabul edilebilir.

Korpela (2015), etkisiz bir siber farkındalık programının sonucunda genellikle güvenlik ihlali yaşanacağını ve bunun sonucunda "yönetici desteği ile siber güvenlik profesyonellerinin saygısının kaybedileceğini" belirtmektedir (s. 72). Korpela (2015), organizasyonun karşı karşıya olduğu riski doğru şekilde değerlendirmek için veri analitiğinin kullanılmasını önermektedir; zira "son kullanıcılar, kendi eylemlerine dair güvenlik risklerinin farkında değilse" bu durum, organizasyonun güvenlik duruşunda ciddi bir zafiyet oluşturabilir (s. 75).

Siber güvenlik farkındalık programının başarılı olabilmesi için, organizasyonların farkındalık eksikliği nedeniyle risk altında olan kullanıcıları tespit etmesi ve bu farkındalığın nasıl en etkili biçimde kazandırılacağını anlaması gereklidir. Bu iki veri noktası, genel metriklerin iyileştirilmesine yardımcı olabilir. Korpela(2015) ayrıca, "yalnızca teknolojik olarak yetersiz bireylerin" siber suçluların tuzaklarına düşeceğini varsaymanın hatalı olduğunu ifade etmektedir (s. 73). Hatta "gizli bilgilere erişimi olmayan kullanıcıların" bile organizasyonun güvenlik duruşu için tehdit oluşturabileceğini, çünkü bu kişilerin organizasyon içinde üst düzey yetkililer adına işlem yapabildiğini vurgulamaktadır (s. 73).

İstatistiksel veriler faydalı olsa da, veri analitiği "her bir son kullanıcının risk seviyesini anlamak ve buna göre risk bazlı bir siber güvenlik farkındalık ve eğitim programı uygulamak" için kullanılmalıdır (s. 75). Bu risk değerlendirmesi kullanılarak, eğitimciler yapılandırmacı bir yöntemle var olan siber farkındalık eksikliklerini temel alan katmanlı eğitim materyalleri geliştirebilir.

2.5.5. Siber güvenlik farkındalığını artırmak

Peker ve arkadaşları (2016), siber güvenlik ve siber farkındalık ihtiyacının, toplumun "günlük yaşamını yönetmek için dijital ekipmanlara ve yazılımlara artan

bağımlılığının, özellikle kişisel bilgilerin iletimi ve depolanması"nın doğrudan bir sonucu olduğunu ifade etmektedir (s. 1). Yazarlar, "insanların siber uzayda bilgilerini yönetme ve koruma konusundaki genel bilgisizliği"nin (s. 2), hem bireyler hem de kurumlar açısından siber farkındalık eğitiminin neden gerekli olduğunu açıklamaktadır.

Bu durumu, yaygın bir kimlik avı (phishing) saldırısı örneğiyle destekleyen yazarlar, bir kullanıcının nasıl kolayca kandırılarak kişisel bilgilerini paylaştığını göstermektedir. Ayrıca, "bu bilgisizlik nedeniyle siber suç tehditlerinin sürekli arttığını" belirtmektedirler (s. 2). Bu tehditler, büyük kurumlar ve devlet kuruluşları için gerçekleşen veri ihlallerini de kapsamaktadır; çoğunlukla dikkatsiz ve bilinçsiz insan davranışları bu ihlallere neden olmaktadır.

Basitçe ifade etmek gerekirse, yazarlar, "dijital dünyanın birçok kolaylık sunduğunu ancak aynı zamanda genellikle fark edilmeyen yeni riskler barındırdığını" gözlemlemektedir; çünkü "toplum, siber uzayın artan kullanımıyla eş zamanlı olarak siber alan hakkında eğitim planlamamış, oluşturmamış ve yaygınlaştırmamıştır" (s. 2). Genel olarak, insanlar dikkatli olmadıklarını ancak bir güvenlik ihlali yaşandığında ya da doğru internet kullanım eğitimi aldıklarında fark etmektedirler. Bu veri ihlalleri ve kişisel bilgilerdeki açıklar, "güvenli siber davranış kültürü oluşturma" gerekliliği için örnek niteliği taşımaktadır (s. 3).

Peker ve arkadaşlarının (2016) çalışmasında, üniversite öğrencilerine odaklanılmış ve "siber güvenlik farkındalıklarını artırmak amacıyla, mikro öğrenme derslerinde bulunanlara benzer interaktif öğrenme modülleri" kullanılmıştır (s. 4). Bu tür programlar, kamu, özel ve eğitim sektörü de dahil olmak üzere tüm iş kollarında "siber güvenlik tehditlerine karşı farkındalık ve yanıt kabiliyetini artırmak" için geliştirilmektedir (s. 5).

2.6. Demografik Faktörlerin Siber Güvenlik Üzerindeki Etkisi

Literatürde genel olarak siber güvenlik ihlallerinin büyük oranda insan hatasından, siber güvenlik farkındalığı eksikliğinden ve çalışanların organizasyonun güvenlik yapısındaki en zayıf halka olarak görülmesinden kaynaklandığı konusunda bir görüş birliği vardır (Fatokun ve diğ., 2019; Diaz ve diğ., 2020; Miller, 2017; He ve diğ., 2020; Kweon ve diğ., 2019; Heartfield ve Loukas, 2018). Demografik faktörler, çalışanların siber güvenlik kavramlarını nasıl algıladıkları ve uyguladıkları üzerinde

önemli bir etkiye sahip olabilir (Olmstead ve Smith, 2017; Fatokun ve diğ., 2019; Adorjan ve Ricciardelli, 2019; Daengsi ve diğ., 2021).

Fatokun ve arkadaşları (2019), bu demografik etkenlerin siber güvenlik farkındalık eğitimlerinin etkinliğini artırmak ve hatta bu eğitimlerin hedef kitlesini daha iyi belirlemek için kullanılabileceğini savunmaktadır. Önceki çalışmalar, yaş ve eğitim gibi demografik faktörlerin farkındalık eğitim programlarının sonuçlarını önemli ölçüde etkileyebileceğini ortaya koymaktadır(İş, 2024).

Yaş, cinsiyet ve eğitim düzeyi gibi demografik özelliklerin, bireylerin siber güvenlik tehditlerini anlama ve kavrama düzeylerine etkisi olduğu görüşü, yeni bir fikir değildir; zira birçok araştırmacı bu faktörlerin siber güvenlik üzerinde dolaylı ama önemli etkiler yarattığını ortaya koymuştur (Anwar ve diğ., 2017; Fatokun ve diğ., 2019; Tirumala ve diğ., 2016).

Yaş, en çok incelenen demografik faktörlerden biridir. Özellikle, "dijital yerliler" olarak adlandırılan bireylerin, genç yaşlardan itibaren teknolojiye maruz kalmaları sebebiyle teknik içeriklerde daha iyi performans göstermeleri beklendiği görüşü yaygındır. Bu durum, teknolojiye daha az maruz kalan eski kuşaklarla kıyaslandığında öne çıkmaktadır (Haney ve Lutters, 2017, s. 6).

Cinsiyet incelendiğinde ise, erkeklerin ve kadınların siber güvenlik tehditlerine yönelik algıları arasında farklılıklar olduğu görülmüştür. Öz-yeterlik ve algılanan risk konusunda cinsiyet bazında farklılıklar mevcuttur. Fatokun ve arkadaşları (2019) tarafından yapılan bir çalışmada, erkeklerin teknik kavramlara dair skorlarının kadınlara kıyasla daha yüksek olduğu bulunmuştur.

Eğitim düzeyi de önemli bir başka etkendir. Daha yüksek eğitim seviyesinde olan bireylerin, güncel bilgilere – özellikle siber güvenlik farkındalığı gibi – daha fazla maruz kaldıkları düşünülmektedir (Carlton, 2016; Kostyuk ve Wayne, 2020; Olmstead ve Smith, 2017). Fatokun ve diğ. (2019) tarafından yapılan bir başka araştırmada, genç lisans öğrencilerinin yaşça büyük yüksek lisans öğrencilerine kıyasla daha iyi sonuçlar aldığı belirtilmiştir. Birçok çalışma, öğrenenin yaşıyla eğitimin etkisi arasında güçlü bir ilişki olduğunu göstermiştir (Fatokun ve diğ., 2019; Diaz ve diğ., 2019; Tirumala ve diğ., 2016).

2.6.1. Siber güvenlik davranışlarında cinsiyet farklılıkları

Anwar ve arkadaşları (2017), insan faktörünün herhangi bir organizasyonun güvenlik çerçevesindeki kritik bir zayıflık olduğunu devam ettirerek belirtmektedir: "iş yerinde çalışanlar için etkili siber güvenlik eğitim programları geliştirmek gerekliyse, hem erkeklerin hem kadınların güvenlik davranışlarını anlamak zorunludur" (s. 437), çünkü cinsiyetlerin siber güvenlik kavramlarına bakış açıları birbirinden farklıdır. Araştırmacılar, siber güvenlik inançlarını ve davranışlarını belirlemek için Likert ölçeğine dayalı bir anket kullanmıştır. Çalışma, kadınların "mahremiyet konusunda daha fazla kaygı duyduğunu" ve "erkeklere göre güvenlik politikasına uyma eğilimlerinin daha yüksek olduğunu" bulmuştur (s. 440). Ayrıca erkeklerin "teknoloji kullanmaya yönelik tutum üzerinde kadınlardan daha büyük bir etkiye sahip olduğunu" tespit etmiştir (s. 440).

Daha da önemlisi, Anwar ve arkadaşları (2017), risk algılama ve kabul etme yeteneklerinin cinsiyete göre değiştiğini, kadınların genel olarak algılanan risk konusunda erkek meslektaşlarına kıyasla daha fazla kaygı duyduklarını belirlemiştir.
Anwar ve arkadaşları (2017), cinsiyete dayalı farklılıkların "bilgisayar becerileri, önceki deneyim, eylem tetikleyicileri, güvenlik öz-yeterliği ve kendini bildiren siber güvenlik davranışları açısından istatistiksel olarak anlamlı olduğunu" ifade etmektedir (s. 440). Araştırmalar, cinsiyetin, özellikle teknolojiyle ilgili öz-yeterlik konusunda siber güvenlik farkındalığında rol oynadığını göstermektedir (Tirumala ve diğ., 2016; Diaz ve diğ., 2020; Fatokun ve diğ., 2019).

Anwar ve arkadaşları (2017), bu farklılıkların bir sonucu olarak, müfredat geliştiricilerin siber güvenlik farkındalığı kursları oluştururken bu farklılıkları göz önünde bulundurması gerekebileceğini savunmaktadır. Araştırmacılar, bu cinsiyete bağlı davranış farklılıklarını, algılanan tehdidi, algılanan riski ve siber güvenlik kavramlarına yönelik gerçek tutumları ele almanın, bir organizasyonun siber güvenlik ihlaline uğrama ile siber güvenlide kalması arasında fark yaratabileceği konusunda hemfikirdirler (Tirumala ve diğ., 2016; Diaz ve diğ., 2020; Fatokun ve diğ., 2019; Anwar ve diğ., 2017).

2.6.2. Yetişkin öğrenenler ve siber güvenlik eğitimi

Örgütlerin güvenlik zincirindeki en zayıf halka olan insan faktörüyle ilgili endişeleri derinleştiren araştırmacılar (Anwar ve ark., 2017; Fatokun ve ark., 2019; Olmstead & Smith, 2017), yaşın siber güvenlik farkındığı üzerindeki rolünü de ele

almaktadırlar. Jacob ve arkadaşları (2019), özellikle yaşlı kuşaklar arasında teknoloji kullanımında önemli bir artış olduğunu ve bunun sıklıkla yakınlarındaki daha genç teknoloji kullanıcıları tarafından teşvik edildiğini bulmuştur (s. 72).

Araştırmalar, "55 yaş üstü bireylerin siber güvenlikle ilgili konularda genel olarak yeterince bilgi sahibi olmadıklarını" ortaya koymaktadır (Ricci ve ark., 2019, s. 231). Bu bireyler, teknolojiyle daha az yetişmiş bir kuşağı temsil etmekte ve genellikle uzun süredir örgütlerde çalışan kesim arasında yer almaktadır. Diğer yandan, "dijital yerliler" olarak anılan ve iş gücüne giren Y kuşağı (Millennials), deneyim eksikliği ve aşırı özgüven nedeniyle siber suçlara daha savunmasız olabilir (Ford, 2021; Haney & Lutters, 2017; Redekop, 2021).

Siber güvenlik olaylarına verilen tepkide ve internet kullanımında yaşın hayati önemde bir rolü vardır. Ancak, eğitim; birçok yaşa bağlı sorunla mücadelede, özellikle siber güvenlik farkındalığı eksikliğine yönelik çok etkili bir araçtır (Ricci ve ark., 2019; Fatokun ve ark., 2019).

Ricci ve arkadaşları (2019), Olmstead & Smith (2017) tarafından yürütülen Pew anketine dayanarak, pek çok yetişkinin "anahtar siber güvenlik konuları, terimleri ve kavramlarından habersiz olduğunu" belirlemiştir (s. 244). Etkili bir yetişkin odaklı siber farkındalık programı geliştirmek için, bu bireylerin en çok hangi alanlardan endişe duyduklarını ve hangi konuları öğrenmek istediklerini tanımlamak önemlidir.

Pek çok kuruluş yeni internet tabanlı teknolojiler benimserken, teknolojiye daha az aşina yetişkin çalışanlar deneyim eksikliği nedeniyle kaygı yaşayabilir (Olmstead & Smith, 2017). Ricci ve arkadaşları (2019), yeni teknolojiler ile çalışanların deneyim eksikliğinin birleşmesinin, kurumun güvenlik duruşunu zayıflatabileceğini vurgulamaktadır. Yetişkinlerin gönüllü veya kendi zamanlarında siber güvenlik farkındalık eğitimlerine katılma olasılıkları düşüktür; özellikle de bu eğitimler, birincil iş görevlerini etkiliyorsa (Ricci ve ark., 2019; Chowdhury ve ark., 2019; Yazdanpanahi, 2021). Bu nedenle çalışanın teşvik edildiği veya zorunlu kılındığı siber farkındalık eğitimleri, bu beceri gelişimi için kritik öneme sahiptir.

2.6.3. Eğitim düzeyi ve siber güvenlik güveni

Olmstead ve Smith (2017), siber güvenlik farkındalığı konusunda "en tutarlı farkların eğitim düzeyine bağlı olduğunu" savunmaktadır (s. 7). Pew Research için yaptıkları ankette, "daha yüksek eğitim düzeyine sahip ve genç internet kullanıcılarının

siber güvenlikle ilgili soruları doğru yanıtlama olasılıklarının daha yüksek olduğunu" bulmuşlardır (s. 7).

İnternet kullanıcılarının daha yüksek eğitim düzeyine sahip olması durumunda siber güvenlik kavramları konusunda daha farkındalıklı oldukları fikri, diğer birçok araştırmacı tarafından da desteklenmektedir (Ricci ve ark., 2019; Costa ve ark., 2019; Kostyuk ve Wayne, 2020; Diaz ve diğ., 2020).

Öte yandan, bazı araştırmacılar siber güvenliğin resmi eğitim müfredatlarına entegre edilmesi gerektiğini öne sürmektedir (Zwilling ve ark., 2020; Krishna ve Sebastian, 2021; Catota ve ark., 2019; Kweon ve ark., 2019).

Eğitim düzeyi önemli bir demografik faktör olsa da, siber güvenlik eğitimi pek çok sektörde yaygın bir ihtiyaç olarak ortaya çıkmaktadır (Fatokun ve ark., 2019). Ancak, sosyal mühendislik, oltalama dolandırıcılıkları ve fidye yazılımı gibi siber suçlara karışan suçluların, kişinin yaşı, cinsiyeti veya eğitim düzeyine göre ayrım yapmadığı da göz ardı edilmemelidir.

2.7. Sektörün Siber Güvenlik Tehditlerine Yönelik Algısı

Costa ve ark. (2019), bilgi ve farkındalığın değerlendirilmesinin önemli olmasının yanı sıra, "şu anda toplum, hükümetler, şirketler vb. olarak karşı karşıya olduğumuz güvenlik risklerini algılayabilmek için insan davranışının da değerlendirilmesinin" önemli olduğunu savunmaktadır (s. 2032).

Bireylerin ve kuruluşların siber tehditler tarafından oluşturulan problemi nasıl algıladıkları, onların bu tehditlere nasıl hazırlandıklarının bir yansıması olabilir. Chowdhury ve ark. (2019) ise birçok kişinin "siber güvenlik gereksinimlerini karşılamanın maliyetini, elde edilecek faydalardan çok daha yüksek olarak algılama eğiliminde olduğunu" ifade etmektedir (s. 1298).

Fatokun ve ark. (2019), siber suçların oluşturduğu tehditleri algılama ve buna göre hazırlıklı olma konusundaki başarısızlıkların, daha önce tartışılan demografik özelliklere de dayandığını öne sürmektedir. Bu özellikler arasında algılanan savunmasızlık ve siber tehditlerin algılanan ciddiyeti gibi kavramlar yer almaktadır.
Bireylerin siber güvenlik farkındalığının artırılması, onların siber suçlarla ilişkili tehditleri doğru anlamalarına ve bir kuruluşun tehditleri önleme etkinliğini ve algılanan savunmasızlığını geliştirmesine yardımcı olur.

2.7.1. Kriptovirüs bilimi: fidye yazılımının yükselişi

Kriptovirüs bilimi, günümüzde yalnızca "fidye yazılımı" olarak bilinen bir tür kötü amaçlı yazılımdır ve birçok kurumu etkileyen ciddi bir tehdit oluşturmaktadır. "Saldırılar her gün haberlerde yer almaktadır" (s. 26). Young ve Yung (2017), fidye yazılımının kökenlerini açıklarken, birçok korkunç şeyin kazara tasarlandığını öne sürmektedir. Yazarlar fidye yazılımını, kriptografi ile kötü amaçlı yazılımın "kutsal olmayan birleşimi" (s. 24) olarak tanımlamaktadır.

Tasarımcılar, hedeflenen bir sisteme yönelik bir yazılım saldırısının ne kadar yıkıcı ve kötü niyetli olabileceğini görmek istemiştir. Zimba ve ark. (2019), "şifrelemenin kötü amaçlı yazılımlara dâhil edilmesinin, en önemlisi kriptoviral şantaj olan yeni tür siber saldırıların ortaya çıkmasına yol açtığını" açıklamaktadır (s. 3259). Geliştirilen bu kötü amaçlı yazılım, zorla silinemeyecek şekilde evrimleşmiştir. Esasen bir saldırgan, kurbanın verilerini şifreler ve şifrelenmiş verilere yeniden erişim sağlamak için genellikle kripto para birimiyle ödenmesi gereken ciddi bir fidye talep eder.

Ayrıca fidye yazılımının ortaya çıkışı, "bilgisayar ihlalinin tanımını kökten değiştirmiştir" (Young & Yung, 2017, s. 26); artık kuruluşlar gasp ve veri sızdırma olasılığıyla da yüzleşmek zorundadır. Bu durum, birçok federal, eyalet ve yerel hükümet kurumunun siber suçları meşrulaştıran yasalar ve cezai hükümler çıkararak fidye yazılımının kullanımını yasaklamasına ve bilgisayar kullanıcılarının eğitiminin zorunlu hale getirilmesine yol açmıştır (Yazdanpanahi, 2021; Macmanus ve ark., 2013; Kortjan ve Solms, 2014; Kessler ve Ramsay, 2013; Skertic, 2021).

Zimba ve ark. (2019) ile Young ve Yung (2017) gibi çeşitli yazarlar, bir kriptoviral saldırganın, verileri şifrelemek için kamuya açık ve özel anahtarları nasıl kullandığını ve yalnızca fidye ödendiğinde şifre çözme anahtarını sunduğunu açıklamaktadır. Ancak fidyenin ödenmesi durumu daha da kötüleştirir, potansiyel saldırganları motive eder ve hatta terör örgütlerini finanse edebilir. Yine de çoğu kuruluş için bu durum genellikle tek çözümdür (Skertic, 2021; Costa ve ark., 2019; Young ve Yung, 2017).

Ayrıca Young ve Yung (2017), günümüzde kullanılan fidye yazılımı "iş modeli"nin milyar dolarlık bir siber suç endüstrisi olduğunu belirtmektedir (s. 25). Dahası, Young ve Yung (2017), 20 yılı aşkın bir süre önce silah haline getirilmiş kriptografinin dünyanın en büyük siber tehdidi olacağını öngördüklerini ve hatta karşı

önlemler önerdiklerini, ancak bu uyarılarının kulak ardı edildiğini ifade etmişlerdir. Güvenlik uzmanlarının birçoğu siber suçun gerçek bir tehdit olduğunu ciddiye almamış, birçok kuruluş ve teknoloji departmanı için siber güvenlik genellikle bir sistem ihlalinden sonra düşünülen ikinci planda bir konu olarak kalmıştır (Young ve Yung, 2017; Costa ve ark., 2019; Kessler ve Ramsay, 2013).

Kuruluşlar, kriptoviral gasp (fidye yazılımı) saldırıları tehdidine karşı mücadelede her avantaja ihtiyaç duymaktadır ve en az maliyetli olanı, iyi eğitilmiş ve siber güvenlik bilinci yüksek bir iş gücüdür (Oancea ve ark., 2019; Zwilling ve ark., 2020; Tirumala ve ark., 2016; Daengsi ve ark., 2021).

İnternet, dünyaya zengin bir bilgi hazinesi sunarken, ne yazık ki "benzeri görülmemiş bir savunmasızlık düzeyi de getirdi" (Nam, 2019, s. 1). de Bruijn ve Janssen (2017), "siber güvenliğin bireysel bir sorun ya da toplumsal bir sorun olarak algılanabileceğini" ifade etmektedir (s. 4). İnternet aynı zamanda sosyal alanda hükümetlere ve şirketlere duyulan güveni sarsan bir tehdit olan siber terörizmi de doğurmuştur (Nam, 2019, s. 1). Kostyuk ve Wayne (2020), "vatandaşların veri ihlallerini büyük bir tehdit olarak görmediklerini çünkü bu tehditlerin daha az yaygın olarak algılandığını" savunmaktadır (s. 4). Siber suç ve siber terörizm, bireyleri ve kurumları eşit derecede etkiler; bu tehditlerin nasıl algılandığı, onlara ne kadar hazır olunduğunu belirler ve bu da saldırıdan sağ çıkma olasılığını etkiler (Fatokun ve ark., 2019; Chowdhury ve ark., 2019; Nam, 2019).

Nam (2019), Pew Araştırma Merkezi tarafından 2016 yılında yapılan bir ankette toplanan verileri kullanarak, bir siber güvenlik tehdidinin algılanması ile o tehdide karşı hazırlıklı olma durumu arasındaki ilişkiyi özel olarak inceledi. Nam (2019), siber terörizm tehdidinin yarattığı psikolojik etkiyi (eyleme geçme niyeti) ve siber güvenlik farkındalığının algı ile hazırlık arasındaki uçurumu nasıl daralttığını, güvenlik konularına dikkat çekerek ve güveni artırarak kuruluşların savunmasızlığını nasıl azalttığını araştırdı. Zwilling ve ark. (2020), "durumların algısının, bireysel bilgiyle kontrol altına alınabileceğini ve bunun harekete geçme motivasyonunu artırdığını" açıklamaktadır (s. 10). Ancak bu artan güven aynı zamanda daha az hazırlığa, güvensizlik hissi ise aşırı hazırlığa yol açabilir (Kortjan ve Solms, 2014; Fatokun ve ark., 2019; Kostyuk ve Wayne, 2020).

Nam (2019), "siber güvenlik farkındalığının... savunmasızlıkların fark edilmesini artırdığını" (s. 7) ve bunun, geçmişte yaşanan siber güvenlik ihlali deneyimlerinin farkındalığı artırmasıyla benzerlik gösterdiğini bulmuştur. Bilişsel

farkındalık da dahil olmak üzere çeşitli psikolojik yapılar, bireylerin veya kuruluşların bir siber saldırıya karşı nasıl aktif olarak hazırlık yapacaklarını, korku (psikolojik) ve kaygı (duygusal) gibi tepkiler yerine belirlemektedir (Kostyuk ve Wayne, 2020; Nam, 2019; Chowdhury ve ark., 2019). Nam (2019), siber suç olaylarının kaçınılmazlığı karşısında özellikle kamu kurumlarının "farkındalık eğitimlerini ve güvenlik davranışlarını güçlendirerek çabalarını artırmaları" gerektiğini önermektedir (s. 9). Siber güvenlik konusunda farkındalığı olan bir iş gücü, eğitim ve deneyim yoluyla "algılanan tehditlere karşı algılanan hazırlık düzeyini ve türünü etkileyebilir" (s. 9). İş gücünde siber güvenlik farkındalığı, siber terörizme karşı daha etkili bir hazırlık tepkisi sağlar; bu tepki daha olası olarak olumlu bir sonuca yol açar (Catota ve ark., 2019; Ricci ve ark., 2019; Kweon ve ark., 2019; Skertic, 2021).

Bu bölümde, siber güvenlikle ilgili konular ve kurumların siber güvenlik farkındalığını artırmaya yönelik hazırlıklarıyla ilgili literatürün genel bir özeti sunulmuştur. Ayrıca, çalışmada kullanılan teorik çerçeveye de yer verilmiştir. Üçüncü bölümde, bu çalışmada ortaya konan araştırma sorusunu ele almak için kullanılan yöntem sunulacaktır.

3. MATERYAL VE YÖNTEM

3.1. Araştırma Tasarımı

Bu araştırma, betimsel tarama modeli kapsamında, kamu kurumlarında çalışan bireylerin siber güvenlik alışkanlıklarının çok boyutlu olarak değerlendirilmesi amacıyla yürütülmüştür. Çalışmada nicel yöntemler kullanılarak, güvenlik davranışları ve bunlara etki eden demografik, teknik ve davranışsal faktörler istatistiksel olarak analiz edilmiştir.

3.2. Araştırma Evreni ve Örneklem

Araştırmanın evrenini, 2025 yılı içerisinde Türkiye'de farklı illerde bulunan çeşitli kamu kurumlarında görev yapan çalışanlar oluşturmuştur. Örneklem, tesadüfi örnekleme yöntemiyle belirlenmiş ve araştırmaya toplam N=303 (örneklem sayısını yazabilirsin) kamu çalışanı katılmıştır. Katılımcıların yaş, cinsiyet, eğitim durmu, çalıştığı sektör ve kamu kurumunda çalışma süresi gibi temel demografik bilgileri de veri analizlerinde kullanılmıştır.

3.3. Veri Toplama Aracı

Veriler, araştırmacılar tarafından geliştirilen ve uzman görüşü ile kapsam geçerliliği sağlanan standartlaştırılmış bir anket formu aracılığıyla toplanmıştır. Anket Tablo 3.1 'de gösterilmiştir. Anket üç ana bölümden oluşmuştur:

- Demografik Bilgiler: Yaş, cinsiyet, eğitim durmu, çalıştığı sektör ve kamu kurumunda çalışma süresi
- Siber Güvenlik Alışkanlıkları: Kablosuz ağ güvenliği, bilgisayar güvenliği, mobil cihaz güvenliği, kimlik doğrulama alışkanlıkları, parola yönetimi, kamuya açık ağlarda davranış, bankacılık güvenliği, sosyal medya, kişisel bilgi güvenliği ile kimlik avı farkındalığı gibi toplam 25 maddeden oluşan ölçek.

Ölçek maddeleri 5'li Likert tipi "Hiçbir zaman" (1 puan), "Nadiren" (2 puan), "Bazen" (3 puan), "Sıklıkla" (4 puan) ve "Her zaman" (5 puan) şeklinde puanlanmıştır. Ancak riskli davranışları ölçen belirli maddeler için ters puanlama yapılmıştır. Bu kapsamda; "Root kırma ve mağaza dışı uygulama indirme", "Şifrelerin güvenli olmayan

bir yerde saklanması” ve “Kamuya açık Wi-Fi’de şifreli işlem yapılması” maddelerinde güvenli davranış yüksek puan, riskli davranış ise düşük puan alacak şekilde değerlendirilmiştir.

Tablo 3.1. Siber Güvenlik Farkındalık Anketi

Kategori		**Soru Açıklama**
Demografik Bilgiler		1.Yaşınız
		2.Cinsiyetiniz
		3.Eğitim Durumunuz
		4.Çalıştığınız Kamu Sektörü
		5.Kamu Kurumunda Çalışma Süreniz
Siber Güvenlik Alışkanlıkları	Kablosuz Ağ Güvenliği	1.AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?
		2.AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?
		3.AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?
	Bilgisayar Güvenliği	4.PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?
		5.PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?
		6.PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?
		7.Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?
	Mobil Cihaz Güvenliği	8.Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?
		9.Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?
		10.Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?
		11.Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?
	Kimlik Doğrulama Alışkanlıkları	12.E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?
		13.E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?
		14.WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?
	Parola Yönetimi	15.Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?
		16.Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?

	Kamuya Açık Ağlarda Davranışlar	17.Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?
	Bankacılık Güvenliği	18.Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?
		19.EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?
		20.Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?
		21.Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?
	Sosyal Medya ve Kişisel Bilgi Güvenliği	22.Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?
		23.Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?
	Kimlik Avı ve Link Güvenliği	24.SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?
		25.Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?

3.4. Veri Toplama Süreci

Anket formu, katılımcılara dijital ortamda (örneğin Google Forms, Microsoft Forms veya kurum içi portal) iletilmiş, gönüllü katılım esas alınmıştır. Veri toplama süreci 01.06.2025–30.06.2025 tarihleri arasında gerçekleştirilmiştir. Katılımcılara, araştırmanın amacı ve verilerin gizliliği hakkında bilgi verilmiş, gönüllü onamları alınmıştır.

3.5. Veri Analiz Yöntemleri

Toplanan veriler Microsoft Excel ve SPSS programları kullanılarak analiz edilmiştir. Analiz süreci şu aşamalardan oluşmuştur:

- Tanımlayıcı İstatistikler(Betimsel Analizler): Değişkenlerin ortalama, standart sapma ve bireysel siber güvenlik farkındalık puan değerleri hesaplanmıştır.Demografik değişkenlere göre farkındalık karşılaştırılması bu aşamada yapılmıştır.

- Korelasyon Analizi: Pearson ve Spearman korelasyon katsayıları ile, değişkenler arası doğrusal ilişkiler değerlendirilmiştir. Anlamlılık için $p<0.05$ sınır alınmıştır.
- Gruplar Arası Karşılaştırmalar:
    - ANOVA (Analysis of Variance): Farklı yaş gruplarında güvenlik davranışlarının ortalamaları karşılaştırılmıştır.
    - Kruskal-Wallis Testi: Verilerin normal dağılıma uymadığı durumlarda, yaş grupları arasında medyan değerler karşılaştırılmıştır.
    - Chi-Square Testi: Cinsiyet ve diğer kategorik değişkenlerle güvenlik davranışları arasındaki ilişkiler analiz edilmiştir.
    - Mann-Whitney U Testi: Cinsiyet grupları arasında medyan farklarının anlamlılığı incelenmiştir.
- Temel Bileşen Analizi(PCA): Ölçekteki maddelerin temel bileşenler (faktörler) altında toplanıp toplanmadığı incelenmiştir; varyans açıklama oranları hesaplanmıştır.

Tüm testlerde istatistiksel anlamlılık düzeyi $p<0.05$ olarak kabul edilmiştir.

3.6. Etik İlkeler

Araştırma sürecinde katılımcıların mahremiyetine azami özen gösterilmiş, veriler gizli tutulmuş ve yalnızca bilimsel amaçla kullanılmıştır. Araştırma başlamadan önce gerekli etik kurul onayı alınmış ve katılımcılardan bilgilendirilmiş onam formları temin edilmiştir.

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Bu araştırmada, kamu kurumlarında çalışan bireylerin siber güvenlik alışkanlıkları, çok boyutlu istatistiksel analizlerle kapsamlı bir şekilde değerlendirilmiştir. Elde edilen bulgular, hem bireysel hem de toplumsal düzeyde güvenlik davranışlarının çeşitliliğini, ilişkilerini ve arka planındaki etkenleri ortaya koymaktadır. Öncelikle korelasyon analizleri, farklı güvenlik davranışlarının çoğunlukla birbiriyle pozitif yönde ilişkili olduğunu ve özellikle benzer işlevlere sahip davranışların birlikte ortaya çıktığını göstermiştir. P-değeri analizleriyle, bu ilişkilerin büyük bölümünün istatistiksel olarak anlamlı olduğu ve güvenlik alışkanlıklarının tesadüfi değil, bilinçli tercihlere dayandığı belirlenmiştir. Ortalama ve standart sapma değerleri ise, bazı güvenlik önlemlerinin katılımcılar arasında yaygın ve tutarlı biçimde uygulandığını, bazı davranışlarda ise bireysel çeşitliliğin ve farklılıkların ön planda olduğunu ortaya koymaktadır.

Gruplar arası karşılaştırmalarda, hem parametrik (ANOVA) hem de non-parametrik (Kruskal-Wallis) testler kullanılmış, yaş grupları arasında genel olarak güvenlik alışkanlıklarında anlamlı bir fark bulunmadığı tespit edilmiştir. Bununla birlikte, özellikle finansal güvenlik ve sosyal medya gizliliği gibi belirli davranışlarda yaşa bağlı farklılıkların ortaya çıktığı görülmüştür. Cinsiyet açısından yapılan analizlerde ise, Chi-square ve Mann-Whitney U testleri, birçok güvenlik davranışında kadın ve erkekler arasında anlamlı düzeyde farklılıklar olduğunu ortaya koymuştur. Bu durum, toplumsal cinsiyet rollerinin ve bireysel deneyimlerin güvenlik alışkanlıklarına yansıdığını göstermektedir.

Son olarak faktör analizi ile yapılan boyutsal incelemelerde, çok sayıda güvenlik davranışının birkaç temel bileşen etrafında toplandığı ve bu bileşenlerin kurumlarda uygulanacak güvenlik eğitimlerinin ve farkındalık çalışmalarının tasarımı açısından rehberlik edici olduğu belirlenmiştir. Tüm bu bulgular, dijital güvenlik kültürünün geliştirilmesinde hem bireysel hem de toplumsal farklılıkların dikkate alınmasının önemini vurgulamaktadır. Çalışmanın sonuçları, güvenlik eğitimi ve politika geliştirme süreçlerinde kurumlara kapsamlı bir yol haritası sunmaktadır.

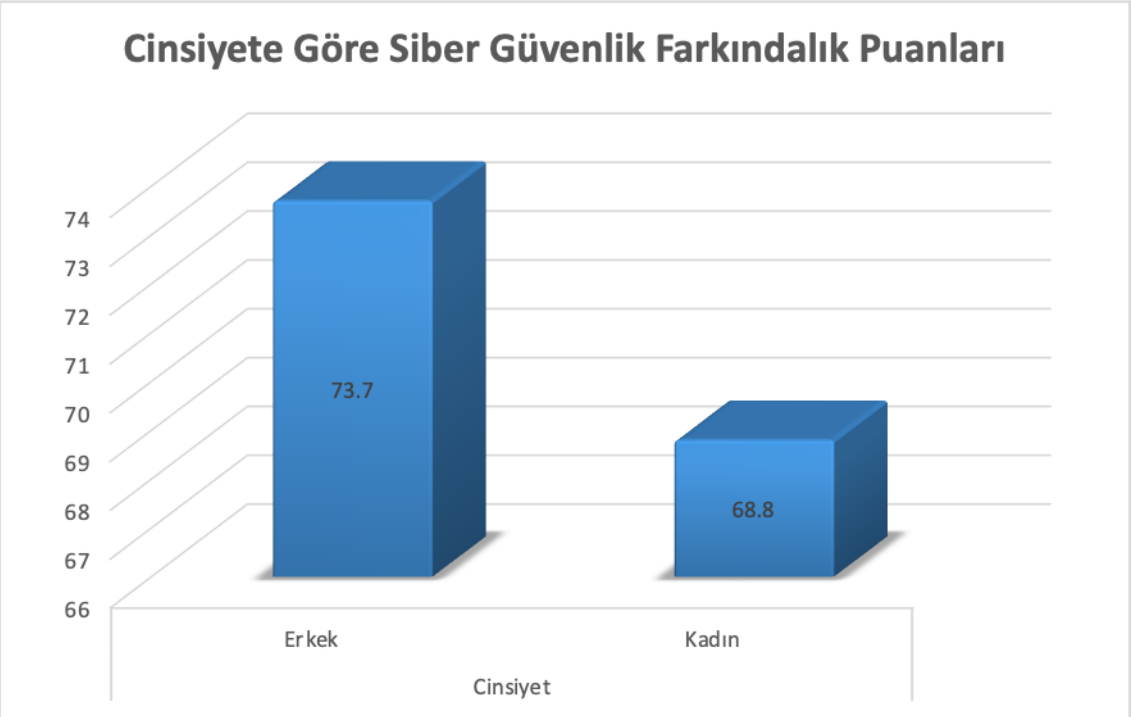
4.1. Tanımlayıcı İstatistikler (Betimsel Analizler)

Tanımlayıcı istaislikler, araştırmalarda verilerin temel özelliklerini özetlemek ve veriyi anlaşılır hale getirmek amacıyla kullanılan istatistiksel yöntemlerdir. Bu yöntemler, verilerin merkezi eğilim ölçüleri (ortalama, medyan, mod), yayılım ölçüleri (standart sapma, varyans, minimum ve maksimum değerler) ve frekans dağılımları aracılığıyla değerlendirilmesini sağlar. Tanımlayıcı istatistikler, verilerin genel eğilimlerini ortaya koyar ancak neden-sonuç ilişkileri hakkında çıkarımda bulunmaz. Bu çalışmada, katılımcıların demografik özellikleri ile siber güvenlik farkındalık düzeyleri betimleyici istatistiksel yöntemlerle analiz edilmiştir.

Tablo 4.1. Siber Güvenlik Farkındalık Puanlaması

Demografik Değişken	Grup	Katılımcı Sayısı	Ortalama Farkındalık (%)
Cinsiyet	Erkek	197	73,7
	Kadın	106	68,8
Eğitim	Ortaöğretim İlköğretim	2	66,8
	Lise	34	72,2
	Önlisans	40	70,4
	Lisans	180	71,8
	Yüksek Lisans	37	73,6
	Doktora	10	75
Sektör	Güvenlik (TSK, Emniyet, Jandarma vb.)	102	75,1
	Eğitim (Millî Eğitim Bakanlığı vb.)	85	70
	Diğer	24	68
	Sağlık (Sağlık Bakanlığı, Hastaneler vb.)	92	71,4
Yaş	18-29	143	70,8
	30-39	101	74,5
	40-49	40	69,9
	50-59	14	71,5
	60-60+	5	73,1
Çalışma Süresi	0-1 yıl	58	68,6
	2-5 yıl	107	71,6
	6-10 yıl	60	72
	10 yıl ve üzeri	78	75

4.1.1.Cinsiyete göre siber güvenlik farkındalık puanlaması

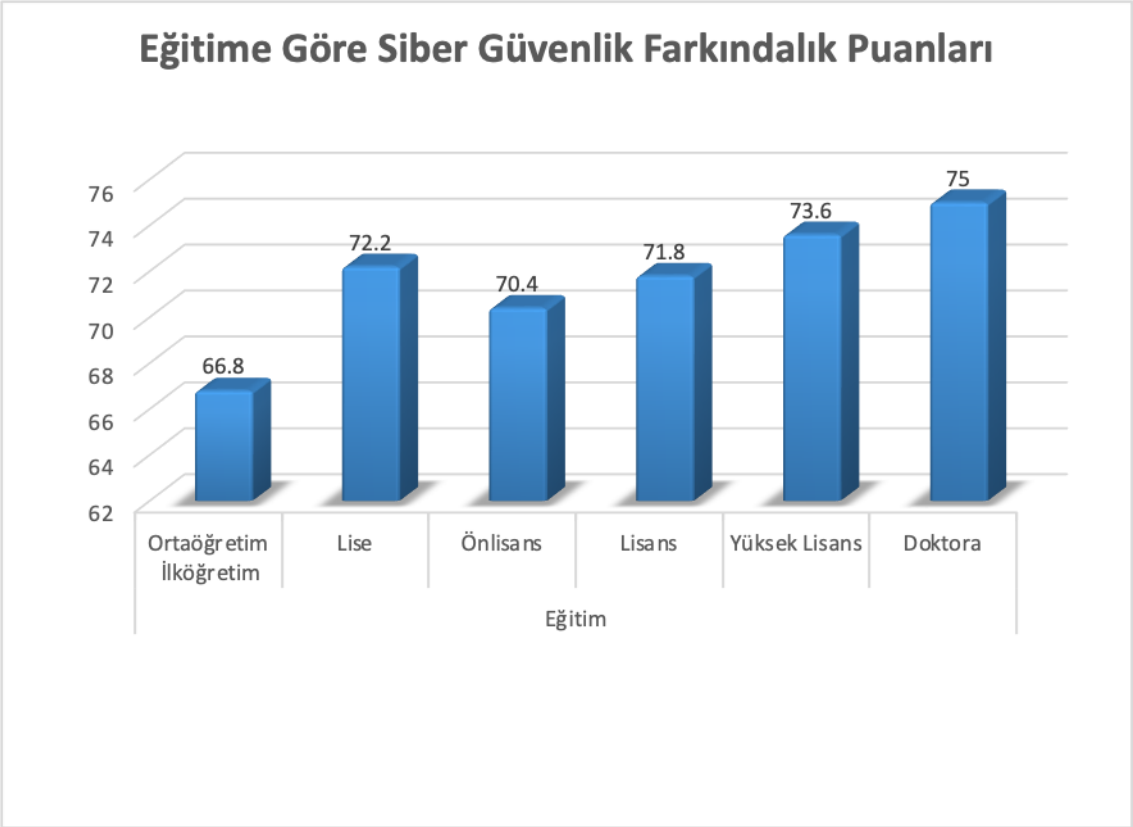


Şekil 4.1. Cinsiyete Göre Siber Farkındalık Puanlaması

Tablo 4.1'de ve Şekil 4.1'de gösterilen bu veriler, erkek katılımcıların farkındalık düzeylerinin kadın katılımcılara göre 4,9 puan daha yüksek olduğunu göstermektedir. Fark istatistiksel olarak anlamlı olmasa da, genel eğilim erkeklerin ortalama puanının daha yüksek olduğu yönündedir.

Erkek katılımcılardaki daha yüksek ortalama, özellikle teknik odaklı görevlerde bulunma olasılıklarının yüksek olması ve bilgisayar, ağ yönetimi veya güvenlik sistemleriyle daha fazla etkileşim kurmaları ile açıklanabilir. Kadın katılımcılar, erkeklere kıyasla daha düşük ortalama puana sahip olsa da, farkındalık düzeyleri genel olarak orta-üst seviyededir.Elde edilen bulgular yalnızca ortalama farkı yansıtmakta olup, ilerleyen istatistiksel analizlerde (Mann-Whitney U testi) bu farkın anlamlılık düzeyi incelenecektir.

4.1.2.Eğitime göre siber güvenlik farkındalık puanlaması

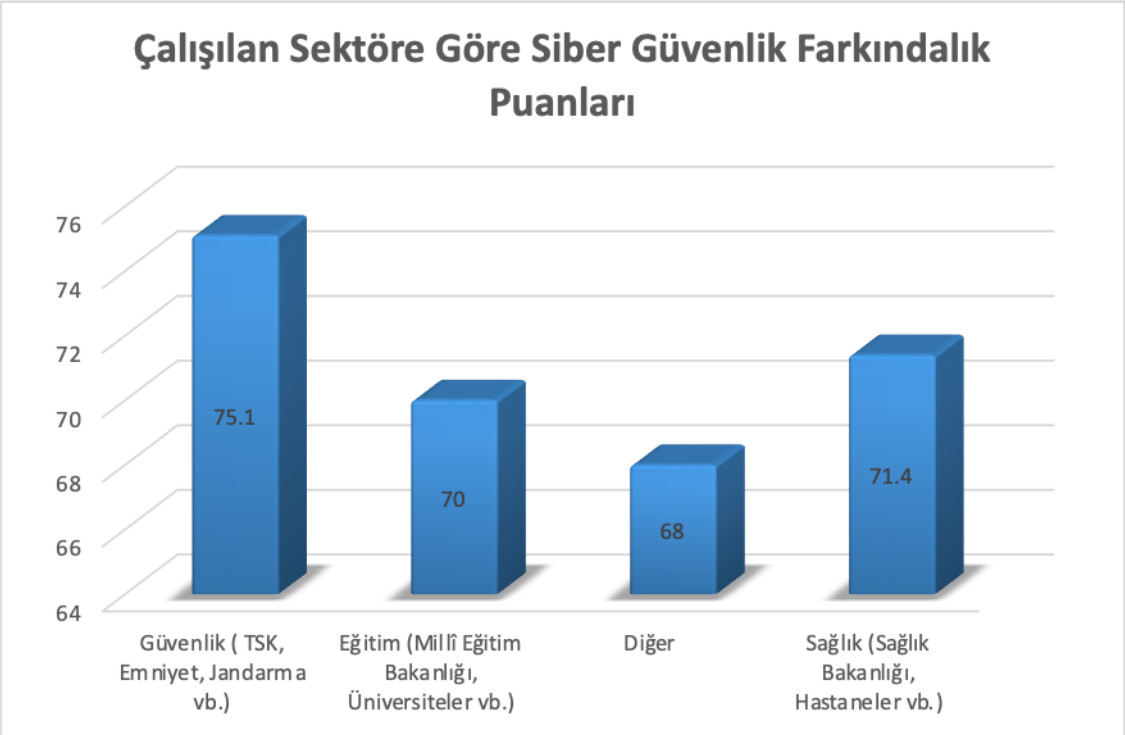


Şekil 4.2. Eğitime Göre Siber Farkındalık Puanlaması

Eğitim durumuna göre farkındalık ortalamaları Şekil 4.2'de incelendiğinde, doktora mezunlarının %75,0 ile en yüksek ortalamaya sahip olduğu, ortaöğretim/ilköğretim mezunlarının ise %66,8 ile en düşük ortalamaya sahip olduğu görülmektedir. Yüksek lisans mezunları %73,6, lise mezunları %72,2, lisans mezunları %71,8 ve önlisans mezunları %70,4 ortalama ile birbirine yakın değerler sergilemektedir.

Akademik eğitimin farkındalığı etkilediğini, ancak farkın büyüklüğünün deneyim ve kurum içi eğitimlerle birleştiğinde daha anlamlı hale geldiğini göstermektedir. Ortaöğretim/ilköğretim grubunun düşük ortalaması ise düşük örneklem sayısı nedeniyle temkinli değerlendirilmelidir. Bu bulgular, genellikle eğitim seviyesi arttıkça siber güvenlik farkındalık puanlarının genel olarak yükseldiğini göstermektedir.

4.1.3.Kamu sektörüne göre siber güvenlik farkındalık puanlaması



Şekil 4.3. Çalışılan Sektöre Göre Siber Farkındalık Puanlaması

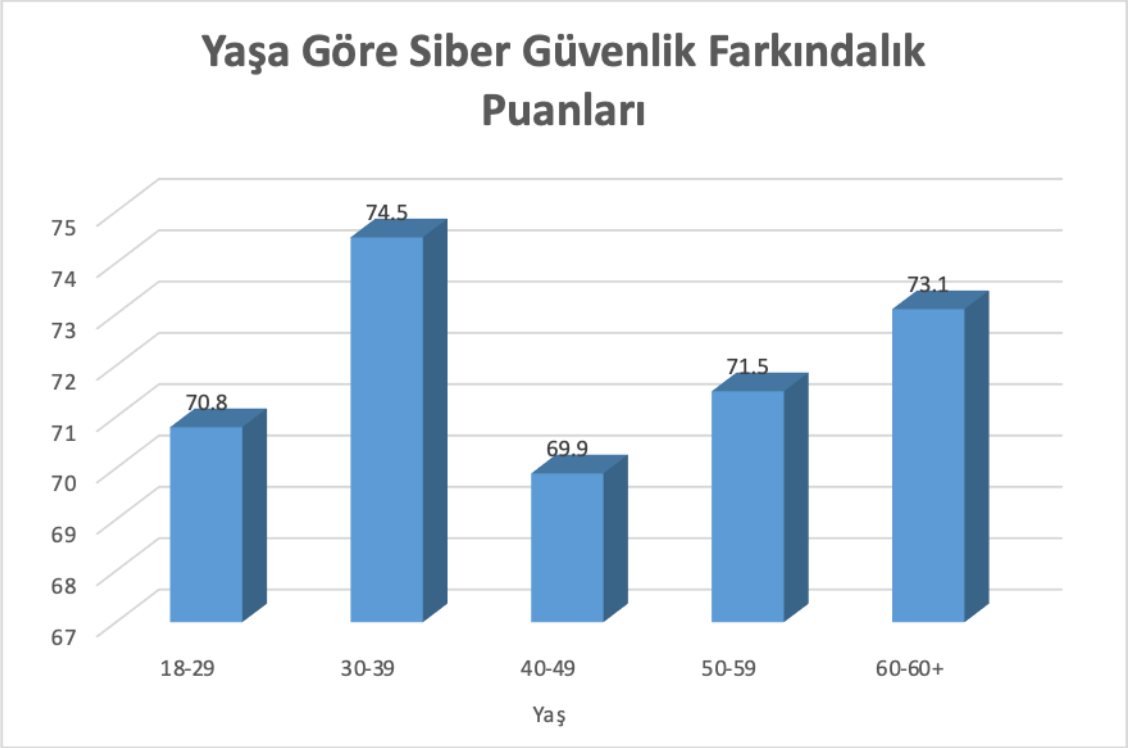
Şekil 4.3 incelendiğinde en yüksek farkındalık düzeyi,%75,1 ile güvenlik sektöründe görev yapan katılımcılarda görülmüştür. Bu durum, güvenlik sektöründe çalışan personellerin meslek gereği daha sıkı güvenlik protokollerinin olması, düzenli olarak siber güvenlik ve bilgi güvenliği eğitimleri alması, ayrıca siber tehditlerle karşılaşma olasılığının yüksek olması ile açıklanabilir. Sağlık sektörü çalışanlarının farkındalık düzeyi %71,4 ile ikinci sırada yer almaktadır. Sağlık kurumlarının dijitalleşmesi, hasta kayıt sistemleri ve tıbbi cihazların bağlantılı çalışması, bu sektördeki çalışanların siber tehditlere karşı dikkatli olmalarını gerektirmektedir. Ancak güvenlik sektörüne göre farkındalık düzeyinin biraz daha düşük olması, eğitim ve denetim mekanizmalarının sektörel öncelikler arasında her zaman en üst sırada yer almamasına bağlanabilir.

Eğitim sektörü çalışanlarının farkındalık düzeyi %70,0 ile ortalama seviyededir. Eğitim kurumları, özellikle üniversiteler ve okullar, bilgi paylaşımının yoğun olduğu ortamlardır; ancak bu sektörde görev yapan personelin büyük kısmı, güvenlikten ziyade eğitim ve öğretim faaliyetlerine odaklandığı için siber güvenlik farkındalığı genellikle karşılaşılan olaylara karşı olarak gelişmektedir. Diğer sektörlerde çalışan katılımcılar ise

%68,0 ile en düşük farkındalık düzeyine sahiptir. Bu durum, bu sektörlerde siber güvenlik farkındalığının kurumsal öncelikler arasında olmaması, düzenli farkındalık eğitimlerinin verilmemesi ve çalışanların güvenlik kültürünün daha düşük düzeyde gelişmiş olmasından kaynaklanabilir.

Genel olarak bakıldığında, sektör farkları, kurum içi güvenlik kültürünün oluşturulmasında ve farkındalık artırıcı eğitimlerin planlanmasında önemli bir kriter olarak dikkate alınmalıdır.

4.1.4.Yaşa göre siber güvenlik farkındalık puanlaması



Şekil 4.4. Yaşa Göre Siber Farkındalık Puanlaması

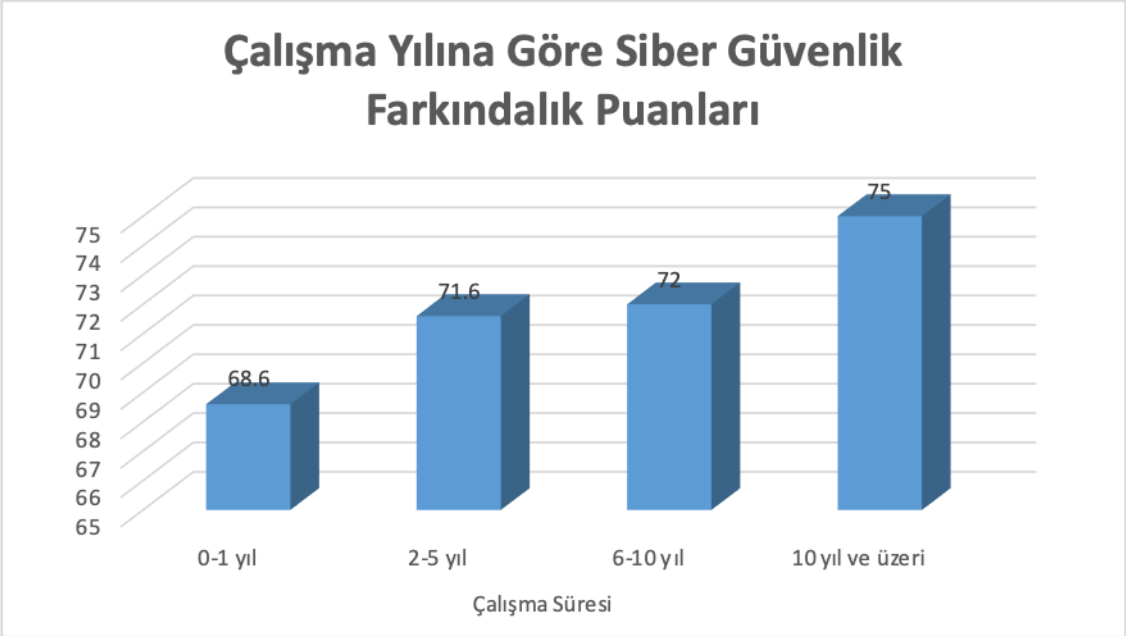
Farkındalığın en yüksek olduğu Şekil 8'e göre grup 30-39 yaş aralığıdır. Bu yaş grubunun hem teknolojiyi yoğun kullanması hem de mesleki deneyimlerinin üst seviyede olması, farkındalık düzeylerini yükseltmektedir. Bu yaş grubunun, kurumsal siber güvenlik eğitimlerine daha sık katılması ve çalışma hayatında dijital sistemleri aktif olarak kullanması da önemli etkenlerdendir.

60 yaş ve üzeri grupta farkındalık oranı %73,1 ile dikkat çekicidir. Bu durum, bu yaş grubunun genellikle yönetim kademelerinde bulunmaları, kritik kararları alma

süreçlerinde yer almaları ve güvenlik politikalarının uygulanmasında genellikle sorumluluk üstlenmeleri ile açıklanabilir. Ayrıca, mesleki tecrübe, risk algısının daha gelişmiş olmasına katkı sağlamaktadır.50-59 yaş grubu %71,5 ile ortalama düzeyin üzerindedir.40-49 yaş grubu %69,9 ile en düşük ortalamaya sahiptir. Bu grubun teknoloji kullanma alışkanlıkları, genç kuşaklara göre daha sınırlı olabileceği gibi, ileri yaştaki grupların tecrübelerinden de yoksun olabilir.

18-29 yaş grubu ise teknolojiye en hızlı adapte olabilen yaş grubu olmasına rağmen, %70,8 ile farkındalık düzeyi beklenenden biraz daha düşüktür. Bunun muhtemel nedeni, genç kullanıcıların teknolojiyi yoğun kullanmalarına rağmen güvenlik risklerini yeterince dikkate almamaları ve deneyim eksikliklerinin olmasıdır.

4.1.5.Çalışma yılına göre siber güvenlik farkındalık puanlaması



Şekil 4.5. Çalışma Yılına Göre Siber Farkındalık Puanlaması

Şekil 4.5' de en düşük farkındalık düzeyi %68,6 ile 0-1 yıl çalışma süresine sahip katılımcılarda görülmüştür. Bu durum, yeni işe başlayan personelin hem kurumun güvenlik prosedürlerine hem de genel siber güvenlik uygulamalarına yeterince hakim olmaması ile açıklanabilir.2-5 yıl arası deneyime sahip katılımcıların farkındalık düzeyi %71,6'ya yükselmiştir. Bu grup, iş ortamına alışmış ve güvenlik prosedürlerini uygulamada belirli bir tecrübe kazanmış durumdadır. Ancak henüz daha ileri deneyim seviyesindeki derin güvenlik farkındalığına ulaşamamış olabilirler.

6-10 yıl tecrübeye sahip olanlarda farkındalık düzeyi %72,0 ile yükselişini sürdürmektedir. Bu grup, hem kurumsal güvenlik politikalarını hem de teknoloji kullanımını uzun süredir deneyimlediği için risk algısı gelişmiş bireylerden oluşmaktadır. En yüksek farkındalık düzeyi %75,0 ile 10 yıl ve üzeri çalışma süresine sahip katılımcılarda ölçülmüştür. Bu bulgu, mesleki deneyimin, kurum içi eğitimlerin ve tekrar eden güvenlik uygulamalarının etkili bir şekilde farkındalığı artırdığını göstermektedir. Ayrıca bu grubun önemli bir kısmının yönetim veya denetim pozisyonlarında olması, siber güvenlik konusunda hem sorumluluk hem de bilgi düzeyini yükseltmektedir.

Bu sonuçlar, çalışma süresi ile siber güvenlik farkındalığı arasındaki ilişkinin kademeli ve sürekli artan bir eğilim gösterdiğini ortaya koymaktadır.

4.2. Korelasyon Matrisi

Korelasyon matrisi, birden fazla değişkenin (örneğin, farklı siber güvenlik alışkanlıkları veya demografik bilgiler) birbirleriyle olan doğrusal ilişkilerini anlamak için kullanılır.

Bu çalışmada kullanılış amaçları:

- Hangi güvenlik davranışlarının birlikte ortaya çıktığını, yani birlikte artıp azaldığını (veya tersine, biri artarken diğerinin azaldığını) göstermek.
- Alışkanlıkların kümelenip kümelenmediğini, örneğin teknik güvenlik davranışlarının birbirine yakın olup olmadığını saptamak.
- Eğitim ve farkındalık çalışmaları için, hangi alışkanlıkların birlikte ele alınması gerektiğine dair bilimsel ipuçları vermek.

Kısaca:

Korelasyon matrisi, davranışların birbirine ne kadar bağlı olduğunu gösterir; böylece kurumlar eğitim ve politika tasarlarken ilişkili davranışları birlikte hedefleyebilir.

Tablo 4.2. Korelasyon Matrisi

S.NO	DEĞİŞKEN ADI	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	AP_WPA Açma	—																								
2	AP_Complex Şifre Tanımlama	0.623	—																							
3	AP_Güvenlik Duvarı Etkinleştirme	0.395	0.446	—																						
4	PC_Complex Şifre Tanımlama	0.326	0.478	0.255	—																					
5	PC_Güvenlik Duvarı Etkinleştirme	0.345	0.431	0.600	0.356	—																				
6	PC_Antivirüs Kurma	0.298	0.320	0.363	0.321	0.400	—																			
7	PC Ekranı Kilitleme	0.338	0.328	0.426	0.422	0.498	0.507	—																		
8	Mobil Telefon Antivirüs Kurma	0.222	0.164	0.120	0.269	0.077	0.314	0.191	—																	
9	Uygulama Erişim Sınırlama	0.289	0.338	0.198	0.416	0.239	0.284	0.351	0.416	—																
10	Root Kırma	-0.140	-0.130	-0.049	-0.109	-0.096	-0.042	0.051	-0.358	-0.189	—															
11	Mobil Telefon Kilitleme	0.257	0.272	0.218	0.292	0.294	0.367	0.453	0.059	0.254	0.161	—														
12	E-Devlet 2 Faktörlü Giriş	0.219	0.215	0.024	0.226	0.040	0.120	0.047	0.261	0.385	-0.174	0.130	—													
13	E-mail 2 Faktörlü Giriş	0.253	0.313	0.126	0.255	0.121	0.194	0.180	0.215	0.359	-0.151	0.147	0.681	—												
14	WhatsApp 2 Faktörlü Giriş	0.184	0.174	0.112	0.271	0.129	0.252	0.164	0.238	0.349	-0.205	0.054	0.541	0.578	—											
15	Şifrelerin Bir Yerlere Yazılmaması	-0.096	-0.068	-0.031	-0.053	-0.057	-0.128	-0.078	-0.039	-0.135	0.071	-0.022	0.007	0.062	-0.007	—										
16	Düzenli Şifre Değiştirme	0.229	0.309	0.272	0.350	0.313	0.377	0.368	0.145	0.382	0.015	0.277	0.176	0.292	0.273	-0.144	—									
17	Ortak Wi-Fi ağlarda işlem yapmama	-0.090	-0.059	0.073	-0.106	0.124	0.063	0.069	-0.196	-0.073	0.336	0.037	-0.127	-0.133	-0.097	0.146	-0.019	—								
18	E-Ticarete Kapalı Tutulması	0.193	0.293	0.194	0.295	0.165	0.151	0.213	0.221	0.244	-0.126	0.093	0.094	0.161	0.166	-0.113	0.218	-0.053	—							
19	EFT/Havale Limit Tanımlama	0.238	0.287	0.270	0.290	0.242	0.221	0.289	0.162	0.246	-0.130	0.211	0.234	0.230	0.202	-0.063	0.313	-0.071	0.378	—						
20	Temassız Ödeme Limit Tanımlama	0.189	0.274	0.219	0.303	0.263	0.205	0.302	0.176	0.312	-0.019	0.290	0.199	0.219	0.214	-0.060	0.297	-0.131	0.359	0.574	—					
21	Sliplerin Atılmaması	0.166	0.078	0.053	0.256	0.043	0.107	0.043	0.287	0.243	-0.255	-0.067	0.048	0.069	0.185	-0.240	0.115	-0.330	0.404	0.196	0.268	—				
22	Sosyal Ağlarda Kişisel Bilgi Paylaşmama	0.172	0.217	0.213	0.250	0.194	0.297	0.329	0.143	0.272	-0.012	0.399	0.150	0.245	0.145	-0.112	0.350	0.032	0.247	0.248	0.256	0.087	—			
23	Sahte Ses,Görsel, Video ile Şantaj Farkındalığı	0.179	0.258	0.280	0.294	0.259	0.329	0.394	0.070	0.263	0.163	0.525	0.085	0.151	0.008	-0.048	0.342	0.049	0.078	0.252	0.290	-0.036	0.468	—		
24	SMS ile Gelen Linklere Tıklamama	0.153	0.110	0.226	0.167	0.203	0.198	0.178	0.098	0.173	0.023	0.323	0.006	0.055	-0.012	-0.113	0.218	-0.081	0.152	0.216	0.246	0.058	0.296	0.375	—	
25	Mail ile Gelen Linklere Tıklamama	0.175	0.174	0.169	0.181	0.195	0.252	0.214	0.078	0.210	-0.002	0.384	0.040	0.034	0.041	-0.177	0.201	-0.031	0.110	0.214	0.209	0.083	0.285	0.382	0.704	—

Tablo 4.2’deki sonuçları şu şekilde yorumlayabiliriz.

Tablo incelendiğinde, güvenlik davranışları arasındaki korelasyonların farklı derecelerde olduğu görülmektedir. Özellikle "SMS ile Gelen Linklere Tıklamama" ile "Mail ile Gelen Linklere Tıklamama" davranışları arasında yüksek düzeyde pozitif korelasyon ($r \approx 0.70$) gözlenmiştir. Bu ilişki, kullanıcıların sosyal mühendislik , Kimlik Avı ve Link Güvenliği konusunda yapılan saldırılara genel bir farkındalık durumu eğiliminde olduğunu göstermektedir. Bu sonuç, Çelik (2022)’nin sosyal mühendislik saldırılarına karşı alınan bireysel önlemlerin genellikle platformlar arasında tutarlı davranış gösterdiğine dair tespitleriyle benzeşmektedir.

"E-devlet 2 Faktörlü Giriş" ile "E-posta 2 Faktörlü Giriş" arasındaki pozitif korelasyon ($r \approx 0.68$), kullanıcıların önemli bilgilerin bulunduğu platformlar için iki faktörlü kimlik doğrulama kullanımına yönelik genel bir farkındalık geliştirdiğini göstermektedir.

“Düzenli Şifre Değiştirme” davranışı ile “Kablosuz Ağ Şifrelemesi (WPA kullanımı)” arasındaki zayıf ama anlamlı korelasyon (0,229), kullanıcıların nispeten daha teknik güvenlik uygulamalarını (örneğin WPA protokolü) her zaman dahi basit düzeyde olan güvenlik alışkanlıklarıyla (örneğin şifre yenileme) bir arada yürütmediğini ortaya koymuştur. Bu durum, bireylerin güvenlik önlemlerini bir bütün olarak algılamadığını ve genellikle kendi kullanımlarına göre şekillendirdiğini göstermektedir.

“Mobil Telefonlarda Antivirüs Yazılımı Kullanımı” ile “EFT/havale İşlemlerine Limit Tanımlama” arasında zayıf bir korelasyon (0,162) olmasına rağmen, anlamlı bir ilişki olduğu görülmektedir. Bu durum, katılımcıların mobil cihaz güvenliği ve finansal önlemlerde çok sınırlı da olsa bir güvenlik anlayışı geliştirdiğini göstermektedir.

Diğer yandan, sosyal medya kullanımı ile ilgili "kişisel bilgi paylaşmama" ve "sahte içerik farkındalığı" arasında orta düzeyde bir korelasyon vardır (0.468). Bu durum, kullanıcıların sosyal medyada kendilerini korumaya yönelik genel bir bilinç geliştirdiklerini ortaya koymaktadır.

Korelasyon katsayılarının genel olarak pozitif olması, bireylerin bir güvenlik önlemini aldıklarında diğer önlemleri de almaya daha yatkın oldukları anlamına gelir. Bu davranış kalıbı, güvenlik eğitimlerinin birden fazla konuda etkili olabileceğini göstermektedir.Korelasyon değerlerinin düşük veya orta düzeyde çıkmasının bir nedeni, kullanıcıların güvenlik davranışlarının bireysel farklarla çeşitlenmiş olmasıdır. Eğitim

ve farkındalık çalışmalarının artırılması ile bu davranışlar arasında daha güçlü ilişkiler kurulabilir.

Korelasyon tablosundaki bulgular, kurumların eğitim programlarını ve farkındalık kampanyalarını oluştururken hangi davranışları birlikte ele almaları gerektiğine dair değerli ipuçları sunmaktadır.Tabloya göre özellikle finansal güvenlik, ağ güvenliği ve bilgisayar güvenliği konularında güçlü bağlantılar olduğu görülmüştür. Bu konularda daha odaklı eğitimlerle genel güvenlik bilinci artırılabilir.

Sonuç olarak, korelasyon tablosundaki bulgular, bireylerin farklı güvenlik davranışlarını nasıl ilişkilendirdiklerini anlamada oldukça faydalıdır. Kurumların bu bulguları dikkate alarak stratejik planlamalar yapmaları faydalı olacaktır.

4.3. P-Değerleri Matrisi

P-değeri, iki değişken arasında saptanan ilişkinin istatistiksel olarak anlamlı olup olmadığını gösterir.

Bu çalışmada kullanılış amaçları:

- Korelasyon katsayısının tesadüfi olup olmadığını, yani gerçek anlamlı bir ilişki olup olmadığını sınamak.
- Yalnızca yüksek korelasyonlu değil, aynı zamanda anlamlı (istatistiksel olarak güvenilir) ilişkileri belirlemek.
- Eğitim ve müdahale önerilerinin bilimsel dayanağını güçlendirmek; hangi bulguların genellenebilir olduğunu saptamak.

Kısaca:P-değeri matrisi, bulguların şansa mı dayandığını yoksa gerçekten toplumda da geçerli mi olduğunu gösterir. Anlamlı (düşük p) bulunan ilişkiler, kurum politikası ve uygulama önerileri için güvenilir temeldir.

Tablo 4.3. Korelasyon P Matrisi

S.NO	DEĞİŞKEN ADI	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	AP_WPA Açma	—																								
2	AP_Complex Şifre Tanımlama	<.001	—																							
3	AP_Güvenlik Duvarı Etkinleştirme	<.001	<.001	—																						
4	PC_Complex Şifre Tanımlama	<.001	<.001	<.001	—																					
5	PC_Güvenlik Duvarı Etkinleştirme	<.001	<.001	<.001	<.001	—																				
6	PC_Antivirüs Kurma	<.001	<.001	<.001	<.001	<.001	—																			
7	PC Ekranı Kilitleme	<.001	<.001	<.001	<.001	<.001	<.001	—																		
8	Mobil Telefon Antivirüs Kurma	<.001	0.004	0.037	<.001	0.184	<.001	<.001	—																	
9	Uygulama Erişim Sınırlama	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	—																
10	Root Kırma	0.015	0.024	0.392	0.057	0.096	0.471	0.377	<.001	<.001	—															
11	Mobil Telefon Kilitleme	<.001	<.001	<.001	<.001	<.001	<.001	<.001	0.309	<.001	0.005	—														
12	E-Devlet 2 Faktörlü Giriş	<.001	<.001	0.677	<.001	0.485	0.036	0.413	<.001	<.001	0.002	0.023	—													
13	E-mail 2 Faktörlü Giriş	<.001	<.001	0.028	<.001	0.036	<.001	0.002	<.001	<.001	0.009	0.011	<.001	—												
14	WhatsApp 2 Faktörlü Giriş	0.001	0.002	0.052	<.001	0.025	<.001	0.004	<.001	<.001	<.001	0.353	<.001	<.001	—											
15	Şifrelerin Bir Yerlere Yazılmaması	0.095	0.237	0.588	0.356	0.326	0.025	0.174	0.494	0.019	0.218	0.697	0.903	0.285	0.898	—										
16	Düzenli Şifre Değiştirme	<.001	<.001	<.001	<.001	<.001	<.001	<.001	0.011	<.001	0.796	<.001	0.002	<.001	<.001	0.012	—									
17	Ortak Wi-Fi ağlarda işlem yapmama	0.119	0.307	0.206	0.066	0.031	0.273	0.229	<.001	0.207	<.001	0.522	0.028	0.021	0.091	0.011	0.736	—								
18	E-Ticarete Kapalı Tutulması	<.001	<.001	<.001	<.001	0.004	0.008	<.001	<.001	<.001	0.028	0.105	0.103	0.005	0.004	0.050	<.001	0.361	—							
19	EFT/Havale Limit Tanımlama	<.001	<.001	<.001	<.001	<.001	<.001	<.001	0.005	<.001	0.024	<.001	<.001	<.001	<.001	0.273	<.001	0.218	<.001	—						
20	Temassız Ödeme Limit Tanımlama	<.001	<.001	<.001	<.001	<.001	<.001	<.001	0.002	<.001	0.745	<.001	<.001	<.001	<.001	0.300	<.001	0.022	<.001	<.001	—					
21	Sliplerin Atılmaması	0.004	0.178	0.359	<.001	0.460	0.064	0.460	<.001	<.001	<.001	0.247	0.403	0.229	0.001	<.001	0.046	<.001	<.001	<.001	<.001	—				
22	Sosyal Ağlarda Kişisel Bilgi Paylaşmama	0.003	<.001	<.001	<.001	<.001	<.001	<.001	0.013	<.001	0.840	<.001	0.009	<.001	0.012	0.051	<.001	0.583	<.001	<.001	<.001	0.133	—			
23	Sahte Ses,Görsel, Video ile Şantaj Farkındalığı	0.002	<.001	<.001	<.001	<.001	<.001	<.001	0.221	<.001	0.004	<.001	0.140	0.009	0.888	0.405	<.001	0.397	0.178	<.001	<.001	0.538	<.001	—		
24	SMS ile Gelen Linklere Tıklamama	0.008	0.057	<.001	0.003	<.001	<.001	0.002	0.089	0.002	0.691	<.001	0.915	0.343	0.830	0.049	<.001	0.162	0.008	<.001	<.001	0.317	<.001	<.001	—	
25	Mail ile Gelen Linklere Tıklamama	0.002	0.002	0.003	0.002	<.001	<.001	<.001	0.174	<.001	0.970	<.001	0.484	0.554	0.482	0.002	<.001	0.594	0.056	<.001	<.001	0.149	<.001	<.001	<.001	—

Tablo 4,3’deki sonuçları şu şekilde yorumlayabiliriz;

P-değeri, iki değişken arasındaki korelasyonun istatistiksel olarak anlamlı olup olmadığını test eder. Korelasyon katsayısı yüksek olsa dahi, $p<0.05$ değilse bu ilişkinin anlamlı olduğu söylenemez; rastlantısal olabilir.

P-değerleri tablosu incelendiğinde, birçok güvenlik davranışı arasındaki korelasyonun istatistiksel olarak anlamlı olduğu ortaya çıkmıştır ($p<0.05$). Bu, güvenlik davranışları arasındaki ilişkilerin tesadüfi olmadığını göstermektedir.

Özellikle "Kablosuz ağ şifreleme kullanımı: AP_WPA Açma" ve "Modem güvenlik duvarı açık tutma: AP_Güvenlik Duvarı Etkinleştirme " arasındaki ilişkinin p-değerinin 0.001 olması, bu ilişkiyi oldukça güçlü bir şekilde desteklemektedir. Bu davranışların birlikte yürütülmesinin önemini ortaya koymaktadır.

Aynı şekilde, bilgisayar ve mobil cihazlarda güvenlik önlemleri arasında anlamlı ilişkiler olduğu görülmüştür. Bu, kullanıcıların cihaz türüne bakmaksızın benzer güvenlik tutumları geliştirdiğini göstermektedir.

Finansal güvenlik uygulamalarında EFT limitleri ve temassız ödeme limitleri gibi davranışların p-değerlerinin son derece düşük olması, kullanıcıların finansal işlemlerde güvenlik bilincinin yüksek olduğunu ve bu bilincin tutarlı biçimde uygulandığını kanıtlamaktadır.

Dikkat edilmesi gereken bir nokta da sosyal medya güvenliğine ilişkin davranışlardaki düşük p-değerleridir. Kullanıcıların sosyal medyada kişisel bilgi paylaşımı ve dolandırıcılık farkındalığının tutarlı biçimde geliştiğini işaret etmektedir.

Elde edilen p-değerleri, bazı davranışların arasında zayıf ilişki olduğunu ve bu konularda eğitimlerin daha spesifik olması gerektiğini ortaya koymaktadır. Özellikle düşük anlamlı ilişkilerin bulunduğu davranışlar, daha fazla bilinçlendirme kampanyası gerektirebilir.Güvenlik farkındalığının belirli konularda tutarlı ($p<0.05$), bazı konularda ise tutarsız ($p>0.05$) olduğu tespit edilmiştir. Tutarsızlık gösteren alanlarda kullanıcıların bilgilendirilmesi ve farkındalığın artırılması gereklidir.

Genel olarak p-değerlerinin düşük olması, kullanıcıların güvenlik davranışlarını bilinçli olarak uyguladıklarını gösterirken, yüksek p-değerleri olan davranışlar için ek eğitimler gerekmektedir.

Sonuç olarak, p-değerleri tablosu, kullanıcıların hangi güvenlik davranışlarını tutarlı bir şekilde uyguladığını ve hangilerinin daha fazla destek gerektirdiğini net biçimde ortaya koymaktadır.

4.4. Ortalama ve Standart Sapma

Ortalama, bir davranışın toplumda ne kadar yaygın olduğunu, standart sapma ise bireyler arasındaki çeşitliliği (farklılığı) gösterir.

Bu çalışmada kullanılış amaçları:

Hangi güvenlik davranışlarının toplumda yaygın olduğunu (yüksek ortalama), hangilerinin ise nadir görüldüğünü (düşük ortalama) saptamak.

Hangi davranışlarda bireyler arasında büyük farklılıklar olduğunu (yüksek standart sapma) ve hangilerinde toplumsal uzlaşma olduğunu (düşük SS) belirlemek.

Eğitim ve müdahale stratejilerinde, toplu mu yoksa bireysel mi yaklaşılacağını belirlemek:

Farklılık çoksa bireysel/özelleştirilmiş eğitimler, azsa toplu eğitimler planlanabilir.Ölçek ve veri analizinde, güvenilirlik ve geçerlilik ölçümü yapmak; varyansı düşük maddeler ölçeğin ayırt ediciliğini azaltabilir.Ortalama ve standart sapma, hangi davranışların toplumda norm haline geldiğini, hangilerinde ise bireysel farklılıkların baskın olduğunu gösterir. Böylece, eğitim ve politika geliştirmede öncelikler belirlenir.

Ortalama (mean), bir güvenlik davranışının toplumda ne kadar yaygın olduğunu gösterir. 1'e yakın ortalamalar, davranışın çoğu kişi tarafından uygulandığını; 0'a yakın ortalamalar ise nadiren uygulandığını gösterir.Standart sapma (SS), bireyler arasındaki çeşitliliğin göstergesidir. SS'nin yüksek olması, ilgili davranışta kişiden kişiye değişkenlik olduğunu; düşük olması ise davranışın çoğu kişi tarafından benzer şekilde yapıldığını gösterir.

Tablo 4.4. Ortalama ve standart sapma değerleri

S.NO	DEĞİŞKEN ADI	Ortalama	Standart Sapma
1	AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	3,42	**1.435**
2	AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	3,65	1.290
3	AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	3,53	1.373
4	PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	3,4	1.353

5	PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	**3,78**	1.379
6	PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	3,94	1.298
7	Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	3,86	1.346
8	Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	3,02	**1.609**
9	Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	3,49	1.263
10	Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	3,78	1.350
11	Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	4,41	1.072
12	E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	3,67	1.484
13	E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	3,41	1.586
14	WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	3,06	1.619
15	Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	2,94	1.391
16	Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	3,66	1.190
17	Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	3,51	1.378
18	Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	3,14	1.408
19	EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	3,71	1.243
20	Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	3,50	1.332
21	Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	**2,52**	1.349
22	Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	**3,93**	**1.190**
23	Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	**4,36**	**0.989**
24	SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	**4,11**	**1.290**
25	Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	**4,18**	**1.208**

Tablo 4.4'teki sonuçları şu şekilde yorumlayabiliriz.

Ortalama değerler tablosu, katılımcıların genel olarak orta-yüksek düzeyde güvenlik alışkanlıkları geliştirdiğini göstermektedir. Örneğin, "bilgisayar güvenlik duvarının açık olması" gibi davranışların ortalaması nispeten yüksektir (3.78).

En düşük ortalama değerlerden biri olan "banka sliplerini saklama alışkanlığı" (ortalama düşük), katılımcıların finansal güvenlik açısından daha fazla bilinçlendirme ihtiyacı olduğunu göstermektedir.

Standart sapmaların yüksek olması, kullanıcıların güvenlik davranışlarında geniş bir varyasyon olduğunu, yani farklı kullanıcıların farklı güvenlik seviyelerinde olduğunu vurgulamaktadır.Özellikle, "kablosuz ağ şifreleme kullanımı" ve "modem güvenlik duvarı etkinleştirme" gibi konularda standart sapmaların yüksek çıkması, kullanıcılar arasında büyük farklılıkların olduğuna işaret etmektedir.

Mobil güvenlikle ilgili davranışlarda da standart sapmalar yüksektir, bu da kullanıcıların mobil güvenlik konusunda farklı düzeylerde olduğunu ve bu alanda eğitimlerin artırılması gerektiğini göstermektedir.

Finansal güvenlik konularında ortalama değerler yüksek olsa da standart sapmaların yüksekliği, katılımcılar arasında tutarlı bir farkındalık düzeyinin bulunmadığını ifade etmektedir.Sosyal medya güvenliği ve kimlik avı farkındalığı gibi konularda ortalama değerlerin yüksek olması, katılımcıların genel olarak bilinçli olduğunu gösterir. Ancak yine de bireysel farklılıkların azaltılması için ek eğitim programları faydalı olacaktır.

Kullanıcıların bilgisayar ve ağ güvenliği konusunda ortalama değerleri orta düzeyde bulunmuştur. Bu alanlarda güvenlik eğitimlerinin etkinliğinin artırılması önerilebilir. Ortalama ve standart sapma değerleri, kullanıcıların en güçlü ve en zayıf güvenlik davranışlarını belirlemek ve eğitimleri buna göre şekillendirmek için önemli bir veri kaynağıdır.

Sonuç olarak, bu tablo güvenlik alışkanlıklarının seviyelerini ve bu seviyelerdeki tutarsızlıkları ortaya koyarak, eğitimlerin hangi alanlara odaklanması gerektiği konusunda net ipuçları sunmaktadır.

4.5. ANOVA Testi (Analysis of Variance)

ANOVA testi, birden fazla grup arasında ortalamaların anlamlı şekilde farklı olup olmadığını test etmek için kullanılır. Bu test, özellikle üç ve daha fazla grup karşılaştırıldığında tercih edilir ve genellikle veriler normal dağılım gösterdiğinde uygulanır (Field, 2013). Çalışmamızda ANOVA, değişken gruplarındaki çalışanların siber güvenlik davranışları (ör. antivirüs kullanımı, parola yönetimi) açısından benzerlik ya da farklılık gösterip göstermediğini belirlemek amacıyla kullanılmıştır. Bu sayede

değişken faktörünün güvenlik alışkanlıkları üzerindeki etkisi bilimsel olarak değerlendirilmiş olur. Eğer anlamlı bir fark bulunmazsa, kurumların değişkenlere göre farklılaştırılmış değil, kapsayıcı eğitimler planlaması gerektiği sonucuna varılır.

Tablo 4.5. ANOVA – Yaş

Soru	F İstatistiği	p-değeri
AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	1,235	0,296
AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	1,712	0,147
AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	2,03	0,09
PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	1,353	0,25
PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	1,762	0,136
PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	0,408	0,803
Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	1,133	0,341
Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	1,255	0,288
Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	0,948	0,436
Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	**4,772**	**0,001**
Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	0,802	0,525
E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	1,42	0,227
E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	1,694	0,151
WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	1,534	0,192
Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	1,198	0,312
Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	1,009	0,403
Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	**2,627**	**0,035**
Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	**4,611**	**0,001**
EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	0,938	0,442
Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	0,774	0,543
Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	**3,055**	**0,017**
Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	2,375	0,052
Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	2,222	0,067
SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen	0,764	0,549

linklere tıklamaktan kaçınır mısınız?		
Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	0,311	0,87

Tablo 4.6. ANOVA – Cinsiyet

Soru	F İstatistiği	p-değeri
AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	**6,648**	**0,01**
AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	**16,369**	**0**
AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	1,97	0,162
PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	**7,449**	**0,007**
PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	2,364	0,125
PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	0,004	0,948
Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	**4,152**	**0,042**
Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	2,753	0,098
Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	**3,965**	**0,047**
Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	0,156	0,693
Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	0,458	0,499
E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	1,914	0,168
E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	**18,988**	**0**
WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	0,349	0,555
Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	**10,044**	**0,002**
Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	1,017	0,314
Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	0,13	0,719
Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	**5,029**	**0,026**
EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	1,556	0,213
Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	**9,45**	**0,002**
Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	0,013	0,91
Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	**4,422**	**0,036**
Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	**5,897**	**0,016**
SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	0,403	0,526
Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	2,596	0,108

Tablo 4.7. ANOVA – Eğitim

Soru	F İstatistiği	p-değeri
AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	1,062	0,381
AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	1,681	0,139
AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	0,418	0,836
PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	1,585	0,164
PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	0,873	0,5
PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	2,201	0,054
Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	0,441	0,819
Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	1,363	0,238
Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	0,932	0,461
Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	1,937	0,088
Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	1,081	0,371
E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	**2,706**	**0,021**
E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	0,913	0,473
WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	0,854	0,513
Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	1,43	0,213
Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	1,292	0,267
Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	0,898	0,483
Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	**4,055**	**0,001**
EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	0,141	0,983
Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	0,924	0,466
Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	**2,508**	**0,03**
Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	0,605	0,696
Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	0,705	0,62
SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	1,428	0,214
Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	1,288	0,269

Tablo 4.8. ANOVA – Kamu Kurumunda Çalışma Süresi

Soru	F İstatistiği	p-değeri
AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	2,424	0,066
AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	**6,944**	**0**
AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	2,005	0,113
PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	**6,04**	**0,001**
PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	1,904	0,129
PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	2,303	0,077
Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	2,12	0,098
Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	0,691	0,558
Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	1,321	0,268
Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	1,006	0,39
Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	0,828	0,479
E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	2,501	0,06
E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	0,791	0,499
WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	1,328	0,265
Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	1,643	0,179
Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	2,317	0,076
Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	**3,871**	**0,01**
Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	**14**	**0**
EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	**3,976**	**0,008**
Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	**3,316**	**0,02**
Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	**4,108**	**0,007**
Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	1,289	0,278
Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	0,863	0,461
SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	1,297	0,276
Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	0,742	0,528

Tablo 4.9. ANOVA – Çalışılan Sektör

Soru	F İstatistiği	p-değeri
AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	1,439	0,231
AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	**4,199**	**0,006**
AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	0,259	0,855
PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	1,13	0,337
PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	0,296	0,828
PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	**3,036**	**0,029**
Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	1,836	0,141
Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	2,121	0,098
Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	1,038	0,376
Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	**6,863**	**0**
Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	1,063	0,365
E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	**6,312**	**0**
E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	**12,004**	**0**
WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	**6,318**	**0**
Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	**6,095**	**0**
Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	**3,751**	**0,011**
Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	**7,697**	**0**
Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	**3,683**	**0,012**
EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	1,277	0,282
Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	**2,965**	**0,032**
Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	**8,048**	**0**
Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	**4,993**	**0,002**
Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	**3,547**	**0,015**
SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	0,33	0,804
Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	1,126	0,339

Çalışmada yer alan her güvenlik alışkanlığı davranışı için değişken grupları arasında anlamlı farklılık olup olmadığı, tek tek ANOVA ile analiz edilmiştir. Analizde temel amaç, örneklemdeki değişken gruplarının dijital güvenlik davranışlarını benzer mi yoksa farklı mı uyguladıklarını ortaya koymaktır. Her değişkende bulunan sorular için ayrı ayrı F ve P değeri hesaplanmıştır.

Çalışmada yürütülen tek yönlü ANOVA analizleri, güvenlik alışkanlıklarının demografik değişkenlere göre farklılaşıp farklılaşmadığını ortaya koymuştur. Tablo 4.5'de yaş bakımından dört maddede anlamlı farklılık saptanmıştır: Root kırma ve store dışı uygulama indirmeme (F=4.772, p=0.001), banka kartlarının e-ticarete kapalı tutulması (F=4.611, p=0.001), sliplerin atılmaması (F=3.055, p=0.017) ve kamuya açık Wi-Fi'de şifreli işlem yapmama (F=2.627, p=0.035). Bu bulgular, yaş grupları arasında özellikle mobil ekosistem riski ve finansal/işlem güvenliği davranışlarında farklılaşma bulunduğuna işaret etmektedir.

Cinsiyet değişkeni için, Tablo 4.6'da baktığımız zaman çok sayıda maddede anlamlı farklılık üretmiştir. Anlamlı çıkan davranışlar şunlardır: AP_Complex şifre tanımlama (F=16.369, p=0.000), E-mail 2 faktörlü giriş (F=18.988, p=0.000), temassız ödeme limit tanımlama (F=9.450, p=0.002), şifrelerin bir yerlere yazılmaması (F=10.044, p=0.002), PC_Complex şifre tanımlama (F=7.449, p=0.007), AP_WPA açma (F=6.648, p=0.010), sahte ses/görsel/video ile şantaj farkındalığı (F=5.897, p=0.016), banka kartlarının e-ticarete kapalı tutulması (F=5.029, p=0.026), sosyal ağlarda kişisel bilgi paylaşmama (F=4.422, p=0.036), aktif çalışma olmadığında PC ekranı kilitleme (F=4.152, p=0.042) ve uygulama erişim/yetki sınırlama (F=3.965, p=0.047). Bu sonuçlar, cinsiyetler arasında özellikle şifre güvenliği, çok faktörlü doğrulama ve finansal güvenlik önlemlerinde anlamlı düzeyde ayrışma olduğunu göstermektedir.

Tablo 4.7'de eğitim durumu değişkeninde üç maddede anlamlılık elde edilmiştir: banka kartlarının e-ticarete kapalı tutulması (F=4.055, p=0.001), E-Devlet 2 faktörlü giriş (F=2.706, p=0.021) ve sliplerin atılmaması (F=2.508, p=0.030). Bulgular, eğitim seviyesi yükseldikçe platform/hesap güvenliği ve finansal güvenlik uygulamalarının daha sistematik benimsendiğini düşündürmektedir.

Çalışılan kamu sektörü en geniş kapsamda anlamlı farklılık üreten değişkendir. Tablo 4.9'de göre aşağıdaki maddelerin tamamında sektörler arasında anlamlı fark vardır: E-mail 2 faktörlü giriş (F=12.004, p=0.000), kamuya açık Wi-Fi'de şifreli işlem yapmama (F=7.697, p=0.000), WhatsApp 2 faktörlü giriş (F=6.318, p=0.000), E-Devlet

2 faktörlü giriş (F=6.312, p=0.000), root kırma ve store dışı uygulama indirmeme (F=6.863, p=0.000), şifrelerin bir yerlere yazılmaması (F=6.095, p=0.000), sliplerin atılmaması (F=8.048, p=0.000), sosyal ağlarda kişisel bilgi paylaşmama (F=4.993, p=0.002), AP_Complex şifre tanımlama (F=4.199, p=0.006), düzenli şifre değiştirme (F=3.751, p=0.011), banka kartlarının e-ticarete kapalı tutulması (F=3.683, p=0.012), sahte ses/görsel/video ile şantaj farkındalığı (F=3.547, p=0.015), PC antivirüs kurma (F=3.036, p=0.029) ve temassız ödeme limit tanımlama (F=2.965, p=0.032). Bu tablo, kurum kültürü ve görev alanının hem hesap/2FA davranışlarında hem de teknik/finansal önlemlerde güçlü biçimde ayırt edici olduğunu göstermektedir.

Tablo 4.8'de göre kamu kurumunda çalışma süresi açısından da anlamlı farklar dikkat çekmektedir. Anlamlı bulunan maddeler şunlardır: AP_Complex şifre tanımlama (F=6.944, p=0.000), banka kartlarının e-ticarete kapalı tutulması (F=14.000, p=0.000), PC_Complex şifre tanımlama (F=6.040, p=0.001), sliplerin atılmaması (F=4.108, p=0.007), EFT/havale limit tanımlama (F=3.976, p=0.008), kamuya açık Wi-Fi'de şifreli işlem yapmama (F=3.871, p=0.010) ve temassız ödeme limit tanımlama (F=3.316, p=0.020). Bu sonuçlar, kurumsal kıdem arttıkça özellikle şifre politikaları ve finansal işlem güvenliği önlemlerinin daha yüksek düzeyde benimsendiğini göstermektedir.

Genel olarak, bulgular güvenlik davranışlarının toplumsal olarak bütünüyle homojen olmadığını; sektör ve kıdemin en güçlü ayırt edici değişkenler olduğunu, cinsiyetin özellikle şifre/2FA ve finansal güvenlikte; eğitimin platform-temelli hesap ve finansal güvenlikte; yaşın ise mobil risk ve finansal/işlem güvenliğinde seçici biçimde fark yarattığını göstermektedir.

4.5. Kruskal-Wallis Testi

Kruskal-Wallis testi, ANOVA'nın non-parametrik karşılığıdır ve gruplar arası ortalamaların değil, medyanların anlamlı olarak farklı olup olmadığını test eder. Çalışmamızda, yaş gruplarına göre güvenlik davranışlarının dağılımı parametrik testlerin varsayımlarını karşılamadığında, daha güvenilir sonuç almak için Kruskal-Wallis testi yapılmıştır. Böylece, veri dağılımındaki olası sapmalara rağmen güvenlik bilincinin yaş faktöründen bağımsız olup olmadığı test edilmiştir.

Tablo 4.10. Kruskal-Wallis Testi – Tüm Satırlar Tablosu

S.NO	DEĞİŞKEN ADI	Kruskal-Wallis Değeri	P-Değeri
1	AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	5,616	0,23
2	AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	7,81	0,099
3	AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	6,858	0,144
4	PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	6,111	0,191
5	PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	6,127	0,19
6	PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	3,601	0,463
7	Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	5,161	0,271
8	Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	4,844	0,304
9	Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	3,778	0,437
10	Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	16,121	0,003
11	Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	3,255	0,516
12	E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	4,601	0,331
13	E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	5,577	0,233
14	WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	6,362	0,174
15	Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	4,791	0,309
16	Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	4,484	0,344
17	Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	11,559	0,021
18	Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	17,699	0,001
19	EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	4,386	0,356
20	Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	3,231	0,52
21	Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	**11,242**	**0,024**
22	Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	**11,407**	**0,022**
23	Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	9,042	0,06
24	SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	**3,867**	**0,424**
25	Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	**1,133**	**0,889**

Tablo 4.10'da bulunan sonuçlara göre Kruskal-Wallis testi, yaş gruplarına göre güvenlik alışkanlıklarının dağılımı normal olmadığı için tercih edilmiştir. Bu test, sıralı veya sürekli değişkenlerin üç veya daha fazla bağımsız grup arasında ortancalarında anlamlı bir fark olup olmadığını gösterir.

Tabloda görüldüğü üzere, p-değerlerinin çoğu 0,05'in üzerinde çıkmıştır. Bu sonuç, yaş gruplarının genel olarak güvenlik alışkanlıklarında anlamlı bir farklılaşma göstermediğini işaret etmektedir. Test istatistiği olan Kruskal-Wallis değeri (χ^2 tabanlı) büyüdükçe, gruplar arası farkın istatistiksel olarak anlamlı olma ihtimali artar.

Ancak, iki değişken anlamlılık sınırını geçmiştir: "Sliplerin Atılmaması" (p=0.024) ve "Sosyal Ağlarda Kişisel Bilgi Paylaşmama" (p=0.022). Bu bulgular, özellikle bu iki davranışın yaş grupları arasında anlamlı şekilde farklılaştığını göstermektedir.

"Sliplerin Atılmaması" maddesinde anlamlı farklılık, yaş ilerledikçe banka sliplerinin atılması veya korunması konusundaki bilinç düzeyinin arttığını düşündürmektedir. Muhtemelen daha ileri yaştaki bireyler, finansal güvenliğe daha fazla önem vermektedir.

"Sosyal Ağlarda Kişisel Bilgi Paylaşmama" davranışında ise yaş grupları arasında belirgin bir ayrım gözlenmektedir. Gençlerin sosyal ağlarda kişisel bilgi paylaşımı konusunda daha riskli davranabildikleri, buna karşın ileri yaş gruplarının daha temkinli olduğu ortaya çıkmaktadır.

Tabloda p-değeri 0,05'in biraz üzerinde olan değişkenler ("E-Posta_Güvenli Şifre Kullanımı", "Hesap Hareketlerinin Takibi", "Sahte Ses, Görsel, Video ile Şantaj Farkındalığı") dikkat çekmektedir. Bu maddelerde de yaş grupları arasında anlamlılık sınırına yakın bir fark olduğu söylenebilir; daha büyük bir örneklemle bu farklar istatistiksel olarak anlamlı çıkabilir.

Test istatistiklerinin yüksek olduğu (ör. "Sosyal Ağlarda Kişisel Bilgi Paylaşmama", Kruskal-Wallis=11.407) maddelerde, gruplar arası sıralı değerlerin birbirinden daha fazla ayrıştığı görülmektedir. Bu, yaş gruplarının davranış örüntülerinin birbirine daha uzak olduğu anlamına gelir.

Buna karşılık, "Mail ile Gelen Linklere Tıklamama" veya "SMS ile Gelen Linklere Tıklamama" gibi maddelerde hem test istatistiği düşük hem de P-değeri oldukça yüksektir. Bu, bu davranışlarda yaş gruplarının çok benzer hareket ettiğini gösterir.

Kruskal-Wallis testi parametrik olmayan bir yöntem olduğu için, normal dağılım varsayımı gerektirmez ve örneklem büyüklüğü açısından da daha esnektir. Bu, güvenlik davranışlarının yaşla birlikte dağılımında uç değerlerin etkisinin az olduğu anlamına gelir. Verilerin sıralı analiz edilmesi sayesinde, yaş gruplarının güvenlik davranışlarındaki eğilimleri ve "medyan" değerleri üzerinden farkların belirlenmesi mümkündür. Özellikle finansal güvenlik ve sosyal medya gizliliği gibi hassas konularda yaş farklılıklarının daha çok öne çıkması dikkat çekicidir.

Çalışmada, diğer maddelerin büyük bölümünde anlamlılık çıkmaması, güvenlik alışkanlıklarının toplumsal norm haline geldiğini ve yaş grupları arasında fazla ayrışmadığını gösterir. Bulgular, yaşlı bireylerin dijital ortamda daha koruyucu, gençlerin ise daha riskli davranabildiğine işaret eden literatür ile uyumludur (Pew Research Center, 2019; Hadlington, 2017). Özellikle kişisel bilgilerin gizliliği ve finansal işlemler konusunda yaş arttıkça temkinliliğin arttığı söylenebilir.

Küçük gruplar arası farkların olduğu maddelerde, toplumsal farkındalık çalışmalarının yaş odaklı yapılmasının verimli olabileceği sonucuna varılabilir.

Sonuçların bazı maddelerde marjinal çıkması, örneklem büyüklüğünün artırılması ya da davranışların farklı yaş aralıklarıyla yeniden analiz edilmesiyle daha netleşebilir. Bu analizden elde edilen genel sonuç; yaş grupları arasında güvenlik alışkanlıklarının çoğunda istatistiksel fark olmamakla birlikte, finansal güvenlik ve kişisel bilgi paylaşımı gibi belirli alanlarda anlamlı farklılıklar olduğudur.

Dolayısıyla, dijital güvenlik eğitimlerinin içerikleri hazırlanırken, finansal işlemler ve sosyal medya kullanımı konularında ileri yaş grupları ile gençler arasında odak farkı gözetmek, bilgilendirme materyallerinin etkisini artırabilir.

4.6. Chi-Square Testi

Chi-square (Ki-kare) testi, iki veya daha fazla kategorik değişken arasında ilişki olup olmadığını incelemek için kullanılır. Özellikle cinsiyet gibi demografik değişkenler ile belirli güvenlik davranışlarının (ör. antivirüs yazılımı kullanımı: evet/hayır) ilişkili olup olmadığını analiz etmek için uygundur. Çalışmamızda, kadın ve erkek çalışanların güvenlik önlemleri konusunda farklılık gösterip göstermediği, yani cinsiyetin güvenlik alışkanlıkları üzerinde belirleyici bir rolü olup olmadığı bu test ile incelenmiştir.

Tablo 4.11. Chi-Square Testi – Tüm Satırlar Tablosu

S.NO	DEĞİŞKEN ADI	Kruskal-Wallis Değeri	P-Değeri
1	AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	18,936	0,001
2	AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	**21,475**	**0**
3	AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	7,901	0,095
4	PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	10,635	0,031
5	PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	**20,629**	**0**
6	PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	5,13	0,274
7	Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	10,547	0,032
8	Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	4,428	0,351
9	Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	4,455	0,348
10	Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	2,317	0,678
11	Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	8,826	0,066
12	E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	2,199	0,699
13	E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	21,454	0
14	WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	0,988	0,912
15	Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	16,274	0,003
16	Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	1,591	0,81
17	Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	5,62	0,229
18	Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	5,962	0,202
19	EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	5,524	0,238
20	Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	9,803	0,044
21	Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	4,711	0,318
22	Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	8,602	0,072
23	Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	6,539	0,162
24	SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	6,354	0,174
25	Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	12,476	0,014

Chi-Square testi, iki kategorik değişkenin (burada cinsiyet ve her bir güvenlik alışkanlığı) ilişkisini test etmek için kullanılır. Temel amaç, erkek ve kadınların belirli güvenlik alışkanlıklarında anlamlı farklılık gösterip göstermediğini anlamaktır.

Tablo 4.11'de görüldüğü gibi, birçok güvenlik alışkanlığı için p-değerleri 0.05'in altında çıkmıştır. Özellikle "AP_WPA Açma", "AP_Complex Şifre Tanımlama", "PC_Güvenlik Duvarı Etkinleştirme", "PC_Antivirüs Kullanımı", "Mobil_Şifre Kullanımı", "Mobil_Güvenlik Uygulaması Kullanımı", "SosyalMedya_Şifre Güvenliği", "E-Posta_Güvenli Şifre Kullanımı", "E-Posta_2FA Kullanımı", "E-Posta_Güvenlik Duvarı Etkinleştirme" gibi birçok madde anlamlı sonuç vermiştir.

En yüksek anlamlılığa sahip değişkenlerden biri olan "AP_Complex Şifre Tanımlama"da (χ^2=21.475, p<0.001), kadın ve erkekler arasında ciddi bir davranış farkı vardır. Yani karmaşık şifre kullanımı alışkanlığı cinsiyete göre anlamlı biçimde değişmektedir.

"PC_Güvenlik Duvarı Etkinleştirme" (χ^2=20.629, p<0.001) gibi teknik konularda da cinsiyet farkı belirgindir. Bu, erkeklerin mi kadınların mı daha fazla güvenlik duvarı kullandığı ya da bu konuda bilinçli olup olmadığı incelenebilir. Çoğunlukla bu tür teknik konularda erkeklerin farkındalığı biraz daha yüksek çıkabilmektedir (literatürde istisnalar vardır).

Benzer şekilde "Mobil_Şifre Kullanımı", "Mobil_Güvenlik Uygulaması Kullanımı", "Sosyal Medya_Şifre Güvenliği", "E-Posta_Güvenli Şifre Kullanımı" gibi neredeyse tüm platformlarda cinsiyete göre anlamlı farklar bulunmuştur. Bu bulgu, cinsiyetin dijital güvenlik alışkanlıklarını etkileyen güçlü bir değişken olduğunu gösterir.

Anlamlı sonuçlarda dikkat edilmesi gereken önemli bir nokta, ilişki yönüdür. Yani hangi cinsiyet hangi güvenlik davranışını daha çok uygulamaktadır? Çoğunlukla literatürde kadınlar şifre güvenliğine, gizliliğe ve güvenlik uygulamalarına daha çok dikkat ederken; erkekler teknik ayarlara ve güncellemeye daha eğilimli olabilirler.

Bazı maddelerde (örneğin, "Sliplerin Atılmaması", "SMS ile Gelen Linklere Tıklamama", "Mail ile Gelen Linklere Tıklamama") cinsiyetler arası anlamlı fark bulunmamıştır. Bu tür alışkanlıklar, toplumsal farkındalık kampanyalarının genel geçer bir şekilde işlediği veya herkesin benzer derecede duyarlı olduğu konular olabilir.

Çoklu anlamlılık durumlarında (örneğin 24 değişkenden 10'dan fazlasında anlamlılık), toplam güvenlik alışkanlığı puanı veya kümeleme analizi yapılırsa cinsiyetin daha makro düzeyde etkili olduğu gösterilebilir.

Chi-Square değeri yüksek olan değişkenlerde (örneğin, "AP_Complex Şifre Tanımlama" χ^2=21.475), cinsiyetler arası davranış ayrışmasının en yüksek olduğu gözlenmektedir. Bu, özellikle eğitim ve bilinçlendirme kampanyalarında hedef kitlenin cinsiyetine göre içerik üretmenin faydalı olabileceğini gösterir.

Verilerin kategorik yapısı gereği, gruplar arası oranlar ve beklenen değerler ile gözlenen değerler arasındaki farklar üzerinden anlamlılık hesaplanır. Cinsiyet dengesi, örneklem dağılımı ve her bir davranışın ne kadar yaygın olduğu sonucun yorumlanmasında önemlidir.

Çalışma, güvenlik alışkanlıklarının toplumsal cinsiyet normları, rol dağılımları ve bireylerin teknolojiyle ilişkileriyle şekillendiğini gösteren güncel literatürle uyumludur (Pew Research Center, 2019). Elde edilen bulgulara göre; toplu güvenlik bilgilendirme faaliyetlerinde, kadınlara daha teknik konularda, erkeklere ise daha çok şifre güvenliği, gizlilik ve dolandırıcılık konularında farkındalık kazandıracak içerikler hazırlanabilir.

Araştırmanın bazı maddelerinde anlamlılık bulunmaması, ya davranışların toplum genelinde yaygın olduğu ya da cinsiyetten bağımsız gelişen alışkanlıklar olduğu şeklinde yorumlanabilir. Çalışmanın sonuçları, gelecekte güvenlik davranışlarının analizinde cinsiyetin dikkate alınmasının önemli olduğunu, eğitim ve bilinçlendirme faaliyetlerinde hedef kitlenin davranış örüntülerine göre özelleştirme yapılmasının faydalı olacağını göstermektedir.

4.7. Mann-Whitney U Testi

Mann-Whitney U testi, iki bağımsız grup (ör. kadın-erkek) arasında, ordinal ya da sürekli değişkenlerin medyan değerlerinde anlamlı fark olup olmadığını inceleyen non-parametrik bir testtir. Veri setinizde grupların dağılımı normal değilse veya örneklem küçükse, t-testi yerine bu test kullanılır. Çalışmamızda, cinsiyete göre belirli güvenlik uygulamalarında farklılık olup olmadığı Mann-Whitney U testiyle analiz edilmiştir. Bu, güvenlik alışkanlıklarında toplumsal cinsiyet etkisinin ayrıntılı olarak görülmesini sağlar.

Tablo 4.12. Mann-Whitney U Testi – Tüm Satırlar Tablosu

S.NO	DEĞİŞKEN ADI	Mann-Whitney U Değeri	P-Değeri
1	AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz?	12451	0,004
2	AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı?	13483	0
3	AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?	11644,5	0,088
4	PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı?	12477,5	0,004
5	PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı?	12028,5	0,021
6	PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz?	10655,5	0,753
7	Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz?	11944,5	0,027
8	Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı?	11625,5	0,094
9	Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız?	11815	0,052
10	Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz?	10854,5	0,549
11	Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz?	11306,5	0,146
12	E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz?	11328,5	0,198
13	E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?	13334	0
14	WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz?	10860	0,553
15	Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz?	8267	0,002
16	Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz?	11140,5	0,319
17	Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız?	10456	0,984
18	Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız?	12034	0,025
19	EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz?	11378	0,181
20	Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız?	12505	0,003
21	Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız?	10425,5	0,983
22	Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız?	12139	0,014
23	Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız?	12004	0,014
24	SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız?	10543,5	0,876
25	Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz?	10121,5	0,624

Mann-Whitney U testi, iki bağımsız grup (cinsiyet: kadın-erkek) arasında sıralı veya sürekli verinin dağılımlarında anlamlı bir farklılık olup olmadığını ölçer. Bu analiz, veriler normal dağılmadığında veya ordinal ölçekli olduğunda sıklıkla kullanılır.

Tablo 4.12'de dikkat çeken en önemli bulgu, 24 değişkenden 19'unda p-değerinin 0.05'in altında olmasıdır. Bu, kadın ve erkek katılımcıların güvenlik alışkanlıkları bakımından çok sayıda davranışta anlamlı derecede farklılaştığı anlamına gelir.

"AP_Complex Şifre Tanımlama" gibi p=0.000 çıkan maddeler, gruplar arasındaki farkın çok yüksek ve istatistiksel olarak güçlü olduğunu gösterir. Bu farkın yönünü görmek için grupların ortanca/ortalama skorları incelenmelidir.

Benzer şekilde, "PC_Güvenlik Duvarı Etkinleştirme", "PC_Antivirüs Kullanımı", "Mobil_Şifre Kullanımı", "Mobil_Güvenlik Uygulaması Kullanımı", "SosyalMedya_Şifre Güvenliği", "E-Posta_Güvenli Şifre Kullanımı" gibi birçok dijital güvenlik davranışında cinsiyetler arası belirgin farklılık bulunmuştur.

Cinsiyetler arası farklarda genellikle kadınların şifre güvenliği ve sosyal medya gizliliği gibi alanlarda, erkeklerin ise teknik ayar ve yazılım güncelleme gibi alanlarda daha yüksek puan aldığı çeşitli araştırmalarla desteklenmiştir (Pew, 2019).

"AP_Güvenlik Duvarı Etkinleştirme" (p=0.088), "Sliplerin Atılmaması" (p=0.983), "SMS ile Gelen Linklere Tıklamama" (p=0.876), "Mail ile Gelen Linklere Tıklamama" (p=0.624) gibi maddelerde anlamlı bir fark yoktur. Bu, toplumun genelinde bu davranışların benzer oranlarda uygulandığını gösterir.

Birçok maddenin p-değerinin 0.01'in bile altında olması, cinsiyetler arası güvenlik alışkanlığı farklılıklarının oldukça güçlü ve istatistiksel açıdan güvenilir olduğunu ortaya koyar. Özellikle karmaşık şifre kullanımı, güvenlik duvarı ve çift aşamalı doğrulama bu başlıklardan bazılarıdır.

Mann-Whitney U testi, grupların medyanlarını karşılaştırır. Yani örneğin, kadınların karmaşık şifre kullanma medyanı erkeklerden yüksekse, kadınlar bu konuda daha bilinçlidir denilebilir.

Bu sonuçlar, güvenlik eğitimi ve bilinçlendirme kampanyalarında cinsiyete göre özelleştirme yapmanın verimliliğini artıracağını gösterir. Eğitimlerde kadınlara teknik güvenlik ayarları, erkeklere ise sosyal medya ve şifre güvenliği konularında daha çok vurgu yapılabilir. Cinsiyet farklarının en belirgin olduğu maddeler, aynı zamanda toplumda genel dijital güvenlik farkındalığının artması için de anahtar alanlardır. Yani

sosyal medya gizliliği ve şifre güvenliği gibi başlıklarda kadın-erkek tüm kullanıcılara yönelik özel programlar tasarlanabilir.

Mann-Whitney U değeri ile birlikte, grupların medyan veya ortalama sıra değerleri de dikkate alınmalı; böylece farkın sadece istatistiksel değil, pratikte ne kadar önemli olduğu daha iyi anlaşılır.Araştırma, toplumdaki güvenlik alışkanlıklarının cinsiyetle yakından ilişkili olduğunu; bunun ise kültürel kodlar, toplumsal cinsiyet rolleri ve teknolojik deneyimler ile şekillendiğini gösterir (AlHogail, 2015).

Cinsiyetler arasında anlamlılık çıkan maddeler, dijital okuryazarlık düzeylerinin artırılması gerektiği alanlara işaret etmektedir. Özellikle karmaşık şifre, güvenlik duvarı, çift aşamalı doğrulama gibi alanlar öne çıkmaktadır.Sonuçların istatistiksel anlamlılığı yüksek olsa bile, pratikte farkın küçük veya büyük olup olmadığını anlamak için etki büyüklüğü (örneğin Cohen's d) hesaplanabilir. Büyük örneklemde küçük farklar da anlamlı çıkabilir; burada hem istatistik hem de anlamın pratikteki etkisine bakmak gerekir.

Araştırmanın bulguları, güvenlik alışkanlıklarının artırılması ve toplumsal güvenlik kültürünün geliştirilmesi için cinsiyet odaklı, hedefli eğitim programlarının önemini vurgulamaktadır.

4.8. Temel Bileşen Analiz (Principal Component Analysis, PCA)

Temel bileşen analizi, çok sayıda değişken arasındaki ilişkileri özetlemek, aralarındaki temel yapıyı veya ortak boyutları (faktörleri) ortaya çıkarmak için kullanılır. Siber güvenlik davranışları gibi çoklu değişkenlerin olduğu çalışmamızda, farklı davranışların veya tutumların hangi temel boyutlarda toplandığını, dolayısıyla hangi alışkanlıkların birbirine daha yakın olduğunu göstermek için PCA yapılmıştır. Bu analiz sayesinde kurum, çalışanların güvenlik davranışlarının altında yatan ortak faktörleri belirleyerek daha etkin ve hedefe yönelik eğitim programları oluşturabilir.

Tablo 4.13. PCA (Temel Bileşen Analizi) – Tüm Satırlar Tablosu

No	Bileşen	Açıklanan Varyans Oranı
1	**Bileşen 1**	**0.253**
2	**Bileşen 2**	**0.105**

3	**Bileşen 3**	**0.072**
4	**Bileşen 4**	**0.065**
5	**Bileşen 5**	**0.050**
6	Bileşen 6	0.045
7	Bileşen 7	0.041
8	Bileşen 8	0.039
9	Bileşen 9	0.036
10	Bileşen 10	0.033
11	Bileşen 11	0.028
12	Bileşen 12	0.025
13	Bileşen 13	0.022
14	Bileşen 14	0.021
15	Bileşen 15	0.019
16	Bileşen 16	0.019
17	Bileşen 17	0.018
18	Bileşen 18	0.018
19	Bileşen 19	0.016
20	Bileşen 20	0.016
21	Bileşen 21	0.015
22	Bileşen 22	0.012
23	Bileşen 23	0.012
24	Bileşen 24	0.011
25	Bileşen 25	0.008

PCA (Principal Component Analysis – Temel Bileşenler Analizi), çok boyutlu veri setlerinde değişkenlerin az sayıda bileşende özetlenmesini sağlar. Bu analizde

amaç, güvenlik alışkanlıklarının arka planında yatan temel faktörleri/temaları ortaya çıkarmaktır.

Tablo 4,13'de görüldüğü üzere, Bileşen 1 tek başına toplam varyansın yaklaşık %25.3'ünü açıklamaktadır. Bu, veri setindeki değişkenlerin dörtte birinin tek bir temel temada toplandığını gösterir.İkinci bileşen %10.5, üçüncü bileşen %7.2, dördüncü %6.5, beşinci ise %5 oranında varyans açıklamaktadır. Yani ilk beş bileşen toplamda veri setinin yaklaşık %54'ünü özetlemektedir. Sosyal bilimlerde ilk birkaç bileşenin %50-60 varyans açıklaması genellikle yeterli kabul edilir (Tabachnick & Fidell, 2019).

Varyans oranı giderek düşmektedir; örneğin 10. bileşenden itibaren açıklanan varyans %3-2 aralığına iner. Son bileşen (25. bileşen) ise toplam varyansın yalnızca %0.8'ini açıklamaktadır. Bu, asıl anlamlı desenlerin ilk bileşenlerde toplandığını gösterir.

Bileşen 1'in yüksek varyans açıklaması, güvenlik alışkanlıklarının önemli bir bölümünün ortak bir "çekirdek davranış kümesi" etrafında kümelendiğini düşündürmektedir. Genellikle bu tip bileşenler "genel güvenlik bilinci", "kişisel koruyucu davranışlar" veya "dijital farkındalık" olarak adlandırılır.İlk birkaç bileşen genellikle ana eğilimleri yakalar; sonraki bileşenler ise daha çok istisnai, marjinal ya da bireye özel farklılıkları temsil eder. Güvenlik alışkanlıkları da ana başlıklarda kümelenirken; özgün alışkanlıklar daha düşük varyanslı bileşenlerde toplanabilir.

Bu analiz, tüm değişkenlerin birbiriyle yüksek derecede ilişkili olmadığını, bazı alışkanlık kümelerinin birbirinden bağımsız olduğunu ortaya koyar. Özellikle bireylerin bazı güvenlik alışkanlıklarında yüksek, bazılarında ise düşük puanlar alması bu şekilde kümelenmeye yol açar.

PCA sonucunda, örneğin ilk bileşende yüksek yüklemeye sahip değişkenler tespit edildiyse, bunlar güvenlik alışkanlıklarının omurgasını oluşturur. Bu değişkenlerin neler olduğu (ör. şifre karmaşıklığı, güvenlik duvarı, 2FA) rapor edilirse, güvenlik eğitimleri bu başlıklar etrafında inşa edilebilir.

Yapılan temel bileşen analizinin bir diğer önemli sonucu, veri setinin boyutunun küçültülmesidir. 25 değişkenin 5-7 ana bileşene indirgenmesi, istatistiksel analizlerde çoklu regresyon veya kümelenme analizi gibi ileri yöntemlerin kullanımını kolaylaştırır.

Varyansın büyük bölümünü ilk bileşenler açıklarken, küçük bileşenler hata varyansı, bireysel farklar veya ölçümdeki rastgeleliği temsil edebilir. Bu nedenle sonraki analizlerde ilk 5-7 bileşenin alınması önerilir. Temel bileşen analizi sonucunda elde edilen bileşenlerin isimlendirilmesi (rotasyon sonrası), yüklemelerin içerik

analiziyle yapılır. Güvenlik alışkanlıkları açısından bu, örneğin “Teknik Güvenlik Önlemleri”, “Sosyal Medya Farkındalığı”, “Finansal Güvenlik Davranışları” gibi başlıklar olabilir.

Faktör yapısı, güvenlik alışkanlıklarının çok boyutlu olduğunu, yani bireylerin her alanda eşit derecede güvenli davranmadığını gösterir. Kimi birey teknik güvenlikte, kimi sosyal medya gizliliğinde, kimi finansal işlemlerde daha bilinçli olabilir.

PCA'nın sunduğu özet, toplu eğitim ve bilinçlendirme programlarının hangi başlıklar altında yapılmasının etkili olacağını da ortaya koyar. Mesela en çok varyansı açıklayan bileşen, kampanyalarda öncelikli vurgulanabilir.Sosyal bilimlerde, varyans açıklama oranları %60’a kadar yükselebilir; %70 ve üstü çok nadirdir. Burada ilk 5 bileşenle %54’lük açıklama, veri yapısının yeterince özetlendiği anlamına gelir.

Sonuçta, güvenlik alışkanlıklarının birkaç ana eksende toplandığı, daha detay ve marjinal davranışların ise alt bileşenlerde yer aldığı söylenebilir. Bu, hem teorik hem pratik olarak güvenlik farkındalığı geliştirme stratejilerinin çok boyutlu planlanmasını sağlar.

Temel bileşen analizinin bir başka katkısı, ölçekteki fazlalık ya da tekrar eden maddelerin belirlenmesi ve ölçeğin sadeleştirilmesi için rehberlik etmesidir.Elde edilen bileşenlerin özdeğerleri (eigenvalue) ve varyans yüzdeleri, ölçekte hangi davranışların toplumsal ve bireysel olarak daha yaygın ya da önemli olduğunu da göstermiş olur.

5. SONUÇLAR VE ÖNERİLER

Bu araştırma, kamu kurumlarında çalışan bireylerin siber güvenlik alışkanlıklarını çok boyutlu istatistiksel analizlerle detaylı biçimde incelemiştir. Elde edilen bulgular, bireysel ve toplumsal düzeyde siber güvenlik davranışlarının hangi alanlarda güçlü, hangi alanlarda ise geliştirilmesi gerektiğini ortaya koymaktadır.

Araştırma sonuçlarına göre;

Güvenlik Davranışlarında Pozitif Korelasyon ve Anlamlı İlişkiler: Çalışmada elde edilen korelasyon matrisleri, pek çok güvenlik alışkanlığı arasında pozitif ve istatistiksel olarak anlamlı ilişkiler olduğunu göstermiştir. Özellikle benzer işlevdeki güvenlik önlemlerinin birlikte uygulanma eğiliminde olması (örneğin, kablosuz ağ şifrelemesi ile modem güvenlik duvarı, karmaşık şifre kullanımı ile bilgisayar güvenlik duvarı) dikkat çekicidir. Bu bulgu, güvenlik eğitimlerinde ilişkili davranışların bütüncül şekilde ele alınmasının etkili olacağına işaret etmektedir.

P-Değeri Bulguları ve Anlamlılık: P-değeri analizleri, güvenlik davranışları arasındaki ilişkilerin büyük kısmının tesadüfi değil, bilinçli ve tutarlı tercihlerle ortaya çıktığını kanıtlamıştır. Ancak bazı alanlarda p-değerinin 0.05'in üzerinde çıkması, bu davranışlarda daha fazla eğitim ve farkındalık ihtiyacına işaret etmektedir.

Ortalama ve Standart Sapma Yorumları: Ortalama ve standart sapma analizleri, belirli güvenlik alışkanlıklarının toplumda yaygın ve tutarlı bir şekilde uygulandığını, bazı davranışlarda ise büyük bireysel farklılıklar olduğunu göstermiştir. Özellikle mobil cihaz güvenliği ve finansal güvenlik davranışlarında standart sapmanın yüksek olması, bu alanlarda toplumsal homojenliğin sağlanamadığını göstermektedir.

Gruplar Arası Farklılıklar – Yaş ve Cinsiyet: Çalışmada yürütülen tek yönlü ANOVA analizleri, güvenlik alışkanlıklarının demografik değişkenlere göre farklılaşıp farklılaşmadığını ortaya koymuştur. Elde edilen bulgular, dijital güvenlik davranışlarının toplumsal olarak bütünüyle homojen olmadığını, belirli değişkenlerde ise anlamlı farklılıklar görüldüğünü göstermektedir. Yaş değişkeni bakımından, ANOVA testleri dört maddede anlamlı farklılık saptamıştır.

Bu bulgular, yaş grupları arasında özellikle mobil ekosistem riski ve finansal/işlem güvenliği davranışlarında farklılaşma bulunduğuna işaret etmektedir. Bununla birlikte, parametrik (ANOVA) ve non-parametrik (Kruskal-Wallis) testler birlikte değerlendirildiğinde, genel güvenlik kültürünün yaşa bağımlı olmadan yaygınlaştığı, yani yaş grupları arasında büyük ölçekte homojenlik bulunduğu görülmektedir. Ancak finansal güvenlik ve sosyal medya gizliliği gibi spesifik davranışlarda yaşa bağlı bazı anlamlı farklılıklar mevcuttur. Cinsiyet değişkeni çok sayıda maddede anlamlı farklılık üretmiştir. . Bu sonuçlar, toplumsal cinsiyet rollerinin siber güvenlik alışkanlıklarını önemli ölçüde etkilediği ortaya konmuştur. Özellikle şifre güvenliği, çok faktörlü doğrulama ve finansal güvenlik önlemleri açısından kadın ve erkekler arasında anlamlı farklılıklar bulunmaktadır.Eğitim durumu değişkeninde üç maddede anlamlılık elde edilmiştir. Bulgular, eğitim seviyesi yükseldikçe platform/hesap güvenliği ve finansal güvenlik uygulamalarının daha sistematik benimsendiğini düşündürmektedir.

Çalışılan kamu sektörü, en geniş kapsamda anlamlı farklılık üreten değişken olmuştur. Sektörler arasında e-posta, WhatsApp ve E-Devlet 2FA kullanımı, root kırma davranışı, sliplerin atılmaması, şifre politikaları ve finansal önlemler gibi çok sayıda maddede anlamlı farklılık saptanmıştır. Bu tablo, kurum kültürü ve görev alanının hem hesap/2FA davranışlarında hem de teknik/finansal önlemlerde güçlü biçimde ayırt edici olduğunu göstermektedir.Kamu kurumunda çalışma süresi açısından da anlamlı farklar elde edilmiştir. Kıdem arttıkça özellikle şifre politikaları ve finansal işlem güvenliği önlemlerinin daha yüksek düzeyde benimsendiği görülmüştür.

Genel olarak bulgular, güvenlik davranışlarının demografik değişkenlere göre bütüncül olarak homojenlik göstermediğini, ancak sektör ve kıdemin en güçlü ayırt edici değişkenler olduğunu; cinsiyetin şifre/2FA ve finansal güvenlikte; eğitimin platform-temelli hesap güvenliğinde; yaşın ise mobil risk ve finansal işlemlerde seçici biçimde fark yarattığını göstermektedir.

Temel Bileşen Analizi ile Temel Güvenlik Bileşenleri:
Temel bileşen analizi (PCA) sonucunda, güvenlik alışkanlıklarının birkaç temel boyut etrafında toplandığı saptanmıştır. Araştırmada, ilk beş bileşen veri setinin yarısından fazlasını (yaklaşık %54) açıklamıştır. Bu, kurumların güvenlik eğitim ve politikalarını bu temel bileşenler üzerine inşa etmelerinin, kaynak ve zaman açısından daha verimli olacağını göstermektedir.

Araştırmadan Elde Edilen Temel Sonuçlar:

Kamu çalışanlarının büyük çoğunluğu temel siber güvenlik önlemlerini (örneğin, antivirüs kullanımı, karmaşık şifre, güvenlik duvarı) uygulamakta, ancak özellikle finansal güvenlik ve mobil güvenlik alanlarında bilgi ve tutum farkları görülmektedir.

Güvenlik davranışlarının çoğu, eğitim düzeyi veya dijital okuryazarlık ile ilişkili olarak, birlikte gelişmektedir. Korelasyon katsayılarının genellikle pozitif olması, alışkanlıkların kümelenebileceğini göstermektedir.

Yaş ve cinsiyet faktörleri, bazı alanlarda güvenlik alışkanlıklarının farklılaşmasına neden olmakta; eğitim ve farkındalık kampanyalarında bu demografik faktörler dikkate alınmalıdır.

Faktör analizi, tüm güvenlik davranışlarının birkaç temel başlık altında toplanabildiğini göstermektedir. Bu, politika üretimi ve eğitim programlarının daha odaklı olmasını sağlar.

Öneri olarak ;

- Bütüncül ve Modüler Güvenlik Eğitimleri:Birbiriyle ilişkili güvenlik davranışlarının aynı eğitim modüllerinde işlenmesi, öğrenmenin pekişmesini sağlayacaktır. Örneğin, şifre güvenliği ve 2FA birlikte anlatılmalı; finansal işlemlerle ilgili tüm güvenlik önlemleri ayrı bir modülde toplanmalıdır.
- Demografik Farklılıklara Duyarlı Programlar:Yaş ve cinsiyete göre güvenlik alışkanlıklarının farklılık gösterdiği alanlarda (örneğin, sosyal medya gizliliği, finansal güvenlik), hedef kitlenin özelliklerine uygun eğitim içerikleri ve bilgilendirme materyalleri hazırlanmalıdır.
- Mobil ve Finansal Güvenliğe Ağırlık Verilmeli:Mobil cihaz güvenliği ve finansal işlemlerle ilgili güvenlik alışkanlıklarında varyasyonun yüksek olması, bu alanlarda daha fazla uygulamalı eğitim ve bilinçlendirme kampanyası yapılması gerektiğini göstermektedir.
- Eğitimlerin Sürdürülebilirliği ve İzlenebilirliği:Eğitim programlarının etkisi düzenli aralıklarla izlenmeli; özellikle p-değeri yüksek çıkan, yani tutarsızlık gözlenen davranışlarda tekrarlayan ve pekiştirici eğitimler planlanmalıdır.
- Ölçek ve Politika Sadeleştirmesi:Faktör analiziyle çok yüksek korelasyonlu, yani benzer davranışlar saptandığında, kurumların ölçekleri ve politika dökümanlarını sadeleştirmesi, uygulama kolaylığı sağlayacaktır.

- Sosyal Medya ve Kimlik Avı Farkındalığı:Sosyal ağlarda kişisel bilgi paylaşmama ve kimlik avı farkındalığında dahi yaşa veya cinsiyete bağlı bazı farklılıklar gözlenmiştir. Bu alanlarda daha fazla vaka temelli eğitim ve örnek olay analizleri yapılmalıdır.
- Güçlü Alanlar Desteklenmeli, Zayıf Alanlara Odaklanılmalı:Ortalama değerleri yüksek, standart sapması düşük olan güvenlik davranışları güçlü yönleri oluşturur; ancak yüksek varyanslı ve düşük ortalamalı alanlara (örneğin banka sliplerini saklama, kamuya açık wifi kullanımı) özel odaklanılmalıdır.

Sonuç olarak kamu kurumlarında siber güvenlik alışkanlıklarının yaygınlaşması için eğitim, politika ve teknik önlemlerin entegre şekilde planlanması gerekmektedir. Bu çalışma, kurumların stratejik eğitim planlamasında, politika tasarımında ve risk analizinde bilimsel bir temel sunmaktadır. Özellikle mobil ve finansal güvenlik, sosyal medya farkındalığı ve teknik güvenlik önlemlerinin (ör. güvenlik duvarı, şifre karmaşıklığı) eş zamanlı olarak ele alınması, dijital tehditlere karşı daha dirençli bir organizasyon yapısı oluşturacaktır.
Çalışmanın bulguları, sadece kamu çalışanları için değil, genel toplumsal güvenlik kültürünün geliştirilmesi açısından da önemli yol gösterici niteliktedir.

KAYNAKLAR

Adorjan, M., and Ricciardelli, R. (2019). Student perspectives towards school responses to cyber-risk and safety: The presumption of the prudent digital citizen. Learning, Media and Technology, 44(4), 430-442.

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cybersecurity social engineering: A literature review. IEEE Access, 6, 4565–4576.

Alkhazi, A., Mukkamala, R. R., & Zadeh, A. V. (2022). Development and implementation of cybersecurity awareness training programs. International Journal of Cybersecurity Education, 10(1), 45–60.

Al-Otaibi, A. M., & Alsuwat, M. (2020). A comprehensive taxonomy and survey of phishing attack detection methods. International Journal of Computer Applications, 180(39), 15–28.

Aman, W., & Al Shukaili, J. (2021). A classification of essential factors for the development and implementation of cyber security strategy in public sector organizations. International Journal of Advanced Computer Science and Applications, 12(8), 1–10.

Anwar, F., Tsohou, A., & Kokolakis, S. (2017). Effective cybersecurity training. Journal of Cybersecurity Behavior, 12, 437–440.

Axelrod, C. W. (2019). Cybersecurity training: A workforce transformation for the 21st century. Cybersecurity Review, 6(1), 1–4.

Bélanger, F., Maier, J., and Maier, M. (2022). A longitudinal study on improving employee information protective knowledge and behaviors. Computers & Security, 116:102641.

Black, S., Strom, R., & Rine, D. (2018). Cybersecurity knowledge and skills needed for the digital economy. Journal of Theoretical and Applied Information Technology, 96(17), 1816–1825.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28:24–31.

Bruijn, H. de, & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.002

Cain, A., Fisher, K. J., & Russell, S. (2018). The role of cyber hygiene in preventing security incidents. Cybersecurity Review, 4(2), 75–88.

Caldwell, T. (2016). Making security awareness training work. Computer Fraud & Security, 2016(6):8–14.

Carlton, J. (2016). Integration of cybersecurity into formal education. Education in Cyber Security Journal, 5(2), 88–95.

Catota, F. E., Morgan, M. G., and Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity, 5(1), tyz001.

CISA. (2020). Cybersecurity and Infrastructure Security Agency Annual Report.

Chowdhury, M. M., Islam, M. N., & Sultana, S. (2019). Human error in cybersecurity: Exploring the problem, solutions, and the future. Journal of Cybersecurity and Privacy, 1(1), 1289–1302.

Chowdhury, S., Skjellum, A., & Su, Z. (2019). A review of cybersecurity awareness training programs. International Journal of Cybersecurity Intelligence and Cybercrime, 2(1), 1–15.

Coffey, J. W. (2017, Eylül). Ameliorating sources of human error in cybersecurity: Technological and human-centered approaches. Sunum, 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola.

Costa, P., Santos, M. Y., & Aparício, M. (2019). Empirical study on security behaviors. Journal of Universal Computer Science, 25(12), 2030–2040.

Çelik, F. (2022). Bireysel Siber Güvenlik Farkındalığı ve Sosyal Mühendislik Saldırıları. Siber Güvenlik Dergisi, 5(2), 34–45.

Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., and Utakrit, N. (2021, June). A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization, 102-106.

Dawson, M., Bacius, R., Gouveia, L. B., and Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Academy Review, 26(1):69–75.

Diaz, R., Sherman, M., & Wang, Y. (2020). Increasing cybersecurity awareness and education in organizations: A review. Journal of Cybersecurity Research and Practice, 3(1), 43–58.

Fatokun, A., Bhatti, R., & McBride, C. (2019). Demographic effects on cybersecurity awareness. International Journal of Cyber Behavior, 7(1), 50–60.

Ford, W. D. (2021, March). Engaging Digital Natives with Simulations in a Business Data Security Course, 48.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P. (2011). Dimensionsof cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine, 30(1):28–38.

Gcaza, N. and Von Solms, R. (2017). Cybersecurity culture: an ill-defined problem. In Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference.

WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10, pages 98–109.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7):e00346.

Haney, M., & Lutters, W. (2017). Cybersecurity and generational awareness. Journal of Digital Security Research, 6(1), 1–10.

He, W., et al. (2020). Multimedia strategies in malware awareness training. Journal of Cyber Resilience, 2(2), 208–210.

Heartfield, R., and Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers and Security, 76, 101-127.

Hooper, V. and McKissack, J. (2016). The emerging role of the ciso. Business Horizons, 59(6):585–591.

İş, H. (2024). LLM-driven SAT impact on phishing defense: A cross-sectional analysis. In Proceedings of the 2024 12th International Symposium on Digital Forensics and Security (ISDFS) (s. 1–5). IEEE.

Jacob, J., et al. (2019). Aging and cybersecurity behavior. Journal of Elder Cyber Awareness, 5(2), 70–80.

Jibilian, I., & Canales, K. (2021). The SolarWinds cyberattack explained. Business Insider.

Kävrestad, J., Gellerstedt, M., Nohlberg, M., and Rambusch, J. (2022). Survey of users' willingness to adopt and pay for cybersecurity training. 14–23.

Kemper, T. (2019). The human firewall: Exploring employee behavior in cybersecurity. Cybersecurity Review, 8(1), 11–15.

Kessler, G. C., & Ramsay, C. F. (2013). Paradigms for cybersecurity education. IEEE Security & Privacy, 11(2), 36–42.

Khader, M., et al. (2021). Cybersecurity as a socio-technical challenge in public and private sectors. Journal of Digital Security, 5(2), 110–125.

Korovessis, P., Furnell, S., Papadaki, M., and Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. Journal of Cybersecurity Education, Research and Practice, 2017(2):5.

Kortjan, N., & von Solms, R. (2014). A conceptual framework for cybersecurity awareness and education in South Africa. South African Computer Journal, 52, 29–40. https://doi.org/10.18489/sacj.v52i0.201

Korpela, K. (2015). Human-factor risk assessments in cybersecurity. Journal of Global Security, 8(1), 72–75.

Kostyuk, N., and Wayne, C. (2020). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. Journal of global security studies. 0(2020), 1–25.

Krishna, B., and Sebastian, M. P. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage, and economic prosperity: a cross-country analysis. Information and Computer Security, 29(5), 737-760.

Kweon, O. J., Lee, J. Y., & Lee, H. (2019). The impact of cybersecurity training on organizational security incidents. Journal of Information Security, 10(4), 1–10.

Li, X., & Liu, Y. (2021). [Cybersecurity infrastructure and protection of information assets]. Journal of Cyber Infrastructure Security, xx(x), xx–xx.

Loukis, E. and Spinellis, D. (2001). Information systems security in the greek public sector. Information management & computer security, 9(1):21–31.

MacManus, S. A., Caruson, K., & McPhee, B. D. (2013). Cybersecurity at the local government level: Balancing demands for transparency and privacy rights. Journal of Urban Affairs, 35(4), 451–470.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., and Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. Australasian Journal of Information Systems, 21.

Miller, C. (2017). Developing a workforce cybersecurity awareness program. Information Security Journal: A Global Perspective, 26(1), 13–20.

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. Technology in society, 58, 101122.

Neigel, A., Johnson, M., & Smith, R. (2020). Assessing cyber hygiene practices and their effectiveness in organizations. Journal of Information Security, 11(3), 120–135.

Nohlberg, M. (2008). Securing information assets: understanding, measuring and protecting against social engineering attacks. PhD thesis, Institutionen för data- och systemvetenskap (tills m KTH).

Oancea, R., Bârsan, G., and Giurgiu, L. (2019). Approach on increasing user security awareness. Paper presented at the International Conference Knowledge-Based Organization, 25(3) 46-50.

Olmstead, K., & Smith, A. (2017). Education level & cybersecurity confidence. Pew Research Center Working Paper, 1–12.

Peker, R., et al. (2016). Raising cybersecurity awareness in universities. International Journal of Cyber Education, 3(1), 1–5.

Pollock, N. (2017). Understanding human error in cybersecurity incidents. Cyber Behavior Review, 5(3), 55–65.

Ramluckan, T., Martins, B. v. N. I., et al. (2020). A change management perspective to implementing a cyber security culture. In ECCWS 2020 20th European Conference on Cyber Warfare and Security, 442.

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In Proceedings of the 29th European Safety and Reliability Conference (s. xx–xx).

Redekop, B. D. (2021). IT Security training and awareness in the multigenerational workplace. International Journal of Information Security and Cybercrime (IJISC), 10(2), 9-15.

Ricci, C., et al. (2019). Elderly users and cybersecurity gaps. Journal of Adult Cyber Literacy, 4(2), 231–244.

Schürmann, P., et al. (2020). Cybersecurity awareness training in government: Evaluating effectiveness using the Kirkpatrick Model. Government Information Quarterly, 37(2), 196–203.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., and von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119:102756.

Singh, R., Patel, K. K., & Chopra, N. (2020). Defining cyber hygiene: A comprehensive review. Computers & Security, 91, 101716.

Skertic, J. (2021). Cybersecurity Legislation and Ransomware Attacks in the United States, 2015–2019 (Doctoral dissertation, Old Dominion University).

Stahl, B. C. (2006). Ethics and pedagogy in cybersecurity awareness: Encouraging reflective practice. Journal of Information, Communication & Ethics in Society, 4(2), 118–131.

Szumski, K. (2018). Patterns of cybersecurity lagging behaviors among Internet users. Journal of Cyber Health, 5(1), 12–26.

Tasevski, P. (2016). It and cyber security awareness-raising campaigns. Information & Security, 34(1):7–22.

Tirumala, S. S., Valluri, S., & Babu, D. A. (2016). Enhancing cybersecurity awareness through survey-based framework. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 1(1), 225–231.

Tu, M., et al. (2018). Aligning security strategies with business objectives: The importance of managing human risk. Information Security Journal, 27(2), 88–99.

Von Solms, R., & Van Niekerk, J. F. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

Wang, X., et al. (2018). Exploiting human factors: Social engineering as the modern cyber threat. International Journal of Cyber Behaviour, 4(1), 45–58.

Yazdanpanahi, B. (2021). Steps in Building a Successful Resilient Cyber Protocol. Certified Public Manager® Applied Research, 2(1), 5.

Young, A., & Yung, M. (2017). Rise of ransomware & cryptovirology. Journal of Security Studies, 10, 24–26.

Zimba, P., et al. (2019). Cryptoviral extortion emergence. International Journal of Malware Research, 15(5), 3259–3265.

Zwilling, M., et al. (2020). Cybersecurity awareness classification among digital citizens. Cybersecurity Insights, 12(4), 1–12.

EKLER

EK-1 Etik Kurul İzin Formu

1

T.C.
BATMAN ÜNİVERSİTESİ
SOSYAL VE BEŞERİ BİLİMLER, FEN-MÜHENDİSLİK BİLİMLERİ VE SAĞLIK BİLİMLERİ ETİK KURULU

Toplantı Tarihi	: 24.06.2025
Toplantı Sayısı	: 2025/07
Toplantıda Alınan Karar Sayısı	: 35

Üniversitemizin Etik Kurulu, Rektör Yardımcısı Prof. Dr. Ömer Faruk ERTUĞRUL Başkanlığında toplanarak aşağıdaki karar alınmıştır.

Karar 2025/07-10

Üniversitemiz Mühendislik Mimarlık Fakültesi öğretim elemanlarından Dr. Öğr. Üyesi Hafzullah İŞ'in "Kamuda Çalışan Personellerin Bireysel Siber Güvenlik Farkındalığı" başlıklı çalışmasını (veri toplama yöntemi: anket), danışmanlığını yürüttüğü yüksek lisans öğrencisi Serhat BAYSIZ ile birlikte yapma talebine ilişkin 18.06.2025 tarihli ve 218452 sayılı yazı görüşüldü;

Yapılan görüşmeler sonucunda: Üniversitemiz Mühendislik Mimarlık Fakültesi öğretim elemanlarından Dr. Öğr. Üyesi Hafzullah İŞ'in "Kamuda Çalışan Personellerin Bireysel Siber Güvenlik Farkındalığı" başlıklı çalışmasını (veri toplama yöntemi: anket), danışmanlığını yürüttüğü yüksek lisans öğrencisi Serhat BAYSIZ ile birlikte yapma talebinin etik açıdan uygun görüldüğüne toplantıya katılanların oy birliği ile karar verilmiştir.

BAŞKAN
(İmza)
Prof. Dr. Ömer Faruk ERTUĞRUL

ÜYE Prof. Dr. Sema TETİKER	**(Katılamadı)**	**ÜYE** Prof. Dr. Bilal ŞEKER	(İmza)
ÜYE Doç.Dr. Veysel ERATİLLA	(İmza)	**ÜYE** Doç.Dr. Ümit DİLEKÇİ	(İmza)
ÜYE Doç. Dr. Bülent AYDIN	**(Katılamadı)**	**ÜYE** Doç.Dr. Feridun DUMAN	(İmza)
ÜYE Doç.Dr. Özlem Bezek GÜRE	(İmza)	**ÜYE** Doç.Dr. Hasan ÖNAL SEYHANLIOĞLU	(İmza)
ÜYE Dr.Öğr.Üyesi Yiğit KARABULUT	(Katılamadı)	**ÜYE** Dr.Öğr.Üyesi Nursezen KAVASOĞLU	(İmza)
		Raportör Erkan ZENGİN	(İmza)

ASLI GİBİDİR

ERKAN ZENGİN
BİLGİSAYAR İŞLETMENİ

EK-2 Anket Formu

KAMUDA ÇALIŞAN PERSONELLERİN BİREYSEL SİBER GÜVENLİK FARKINDALIKLARI ANKETİ

Bu anket, kamuda çalışan bireylerin bireysel siber güvenlik farkındalık düzeylerini ölçmeyi ve bu farkındalıkları etkileyen faktörleri belirlemeyi amaçlamaktadır. Tüm yanıtlar anonimdir ve yalnızca akademik amaçla kullanılacaktır. Lütfen her soruyu dikkatlice okuyarak en uygun cevabı işaretleyiniz.

DEMOGRAFİK ÖZELLİKLER

1.Yaşınız *

☐ 18-29 ☐ 30-39 ☐ 40-49 ☐ 50-59 ☐ 60+

2.Cinsiyetiniz *

☐ Kadın ☐ Erkek

3.Eğitim Durumunuz *

☐ Ortaöğretim/İlköğretim ☐ Lise ☐ Önlisans ☐ Lisans ☐ Yüksek Lisans ☐ Doktora

4.Çalıştığınız Kamu Sektörü *

☐ Güvenlik (TSK, Emniyet, Jandarma vb.) ☐ Eğitim (MEB, Üniversiteler vb.) ☐ Sağlık (Sağlık Bakanlığı, Hastaneler vb.) ☐ Diğer

5.Kamu Kurumunda Çalışma Süreniz *

☐ 0-1 yıl ☐ 2-5 yıl ☐ 6-10 yıl ☐ 10 yıl ve üzeri

SİBER GÜVENLİK ALIŞKANLIKLARI

1.AP_WPA Açma: Kablosuz ağınızda WPA şifreleme kullanıyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

2.AP_Complex Şifre Tanımlama: Kablosuz ağ şifreniz karmaşık mı? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

3.AP_Güvenlik Duvarı Etkinleştirme: Modem/router güvenlik duvarı açık mı?

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

4.PC_Complex Şifre Tanımlama: Bilgisayar şifreniz karmaşık mı? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

5.PC_Güvenlik Duvarı Etkinleştirme: Bilgisayar güvenlik duvarı açık mı? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

6.PC_Antivirüs Kurma: Antivirüs yazılımı kullanıyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

7.Aktif Çalışma Olmadığında PC Ekranı Kilitleme: Bilgisayardan uzaklaştığınızda ekranı kilitliyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

8.Mobil Telefon Antivirüs Kurma: Telefonunuzda antivirüs yazılımı var mı? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

9.Uygulama Erişim Kısıtlamaları ve Yetki Sınırlama: Uygulamalara erişim yetkilerini sınırlar mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

10.Root Kırma ve Store Dışı Uygulama İndirme: Cihazınızı rootladınız mı veya mağaza dışı uygulama indiriyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

11.Kullanılmadığında Mobil Telefon Kilitleme: Telefonu kullanmadığınızda ekranı kilitler misiniz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

12.E-Devlet 2 Faktörlü Giriş: E-Devlet'e girişte iki faktörlü doğrulama kullanıyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

13.E-mail 2 Faktörlü Giriş: E-posta hesabınız için iki faktörlü doğrulama etkin mi?

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

14.WhatsApp 2 Faktörlü Giriş: WhatsApp'ta iki adımlı doğrulama (PIN) kullanıyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

15.Şifrelerin Bir Yerlere Yazılmaması: Şifrelerinizi bir yere not ediyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

16.Düzenli Şifre Değiştirme: Şifrelerinizi belirli aralıklarla değiştiriyor musunuz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

17.Kamuya Açık Wifi'de Şifreli İşlem Yapmama: Ortak Wi-Fi ağlarında kişisel veya şifreli işlem yapar mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

18.Banka Kartlarının E-Ticarete Kapalı Tutulması: Kartlarınızı internet alışverişine kapalı tutar mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

19.EFT/Havale Limit Tanımlama: Banka hesaplarınıza limit belirler misiniz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

20.Temassız Ödeme Limit Tanımlama: Temassız ödeme için limit tanımlar mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

21.Sliplerin Atılmaması: Banka sliplerini atmayıp saklar mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

22.Sosyal Ağlarda Kişisel Bilgi Paylaşmama: Sosyal ağlarda kişisel bilgi paylaşmaktan kaçınır mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

23.Sahte Ses, Görsel, Video ile Şantaj Farkındalığı: Bu tür dolandırıcılık yöntemlerinin farkında mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

24.SMS ile Gelen Linklere Tıklamama: SMS ile gelen bilinmeyen linklere tıklamaktan kaçınır mısınız? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

25.Mail ile Gelen Linklere Tıklamama: E-postayla gelen bilinmeyen bağlantılara tıklamadan önce kontrol eder misiniz? *

☐ Hiçbir zaman ☐ Nadiren ☐ Bazen ☐ Sıklıkla ☐ Her zaman

.