

Research Article

Received: date: 15.06.2025
Accepted: date: 21.12.2025
Published: date: 31.12.2025

Üniversite Öğretim Elemanlarının Kişisel Siber Güvenlik Farkındalığı

Seda Öztrak^{1*}, Hasan Şahin² Ömer Faruk Efe³

¹Department of Industrial Engineering, Bursa Technical University, Bursa Türkiye; seda1629@gmail.com

²Department of Industrial Engineering, Bursa Technical University, Bursa Türkiye; h.sahin@btu.edu.tr

³Department of Industrial Engineering Bursa Technical University, Bursa Türkiye; omerfarukefe@aku.edu.tr

Orcid: 0009-0007-4109-871X¹ Orcid: 0000-0002-8915-000X² Orcid: 0000-0001-8170-5114³

*Correspondence: seda1629@gmail.com

Öz: Bu araştırmanın amacı, bir devlet üniversitesinde görev yapan öğretim elemanlarının kişisel siber güvenlik farkındalık düzeylerini demografik değişkenler çerçevesinde incelemektir. Çalışma, 2023–2024 bahar yarıyılında görev yapan ve gönüllü olarak katılan 147 akademik personel ile gerçekleştirilmiştir. Veri toplama aracı olarak, “Kişisel Siber Güvenliği Sağlama Ölçeği” ve “Demografik Bilgiler” olmak üzere iki bölümden oluşan bir anket kullanılmıştır. Demografik bilgiler bölümünde 13 maddeye, beş faktörlü yapıdan oluşan ölçekte ise 25 maddeye yer verilmiştir. Elde edilen veriler IBM SPSS programı kullanılarak analiz edilmiştir. Analizler sonucunda, bazı demografik değişkenler açısından kişisel siber güvenlik farkındalığı düzeylerinde istatistiksel olarak anlamlı farklılıklar tespit edilmiştir. Bulgular, üniversitelerde siber güvenlik farkındalığını artırmaya yönelik kurumsal politika ve eğitimlerin önemini ortaya koymaktadır.

Keywords: Siber Güvenlik, Farkındalık, Öğretim Elemanları, Bilgi Güvenliği

Personal Cybersecurity Awareness of University Faculty Members

Abstract: This study aims to examine the personal cybersecurity awareness levels of faculty members working at a public university within the framework of demographic variables. The research was conducted during the 2023–2024 spring semester with the voluntary participation of 147 academic staff members. Data were collected using a questionnaire consisting of two sections: the Personal Cybersecurity Maintenance Scale and a Demographic Information form. The demographic section included 13 items, while the scale consisted of 25 items structured under five factors. The collected data were analyzed using IBM SPSS software. The findings revealed statistically significant differences in personal cybersecurity awareness levels according to certain demographic variables. The results emphasize the importance of institutional policies and training programs aimed at improving cybersecurity awareness in higher education institutions.

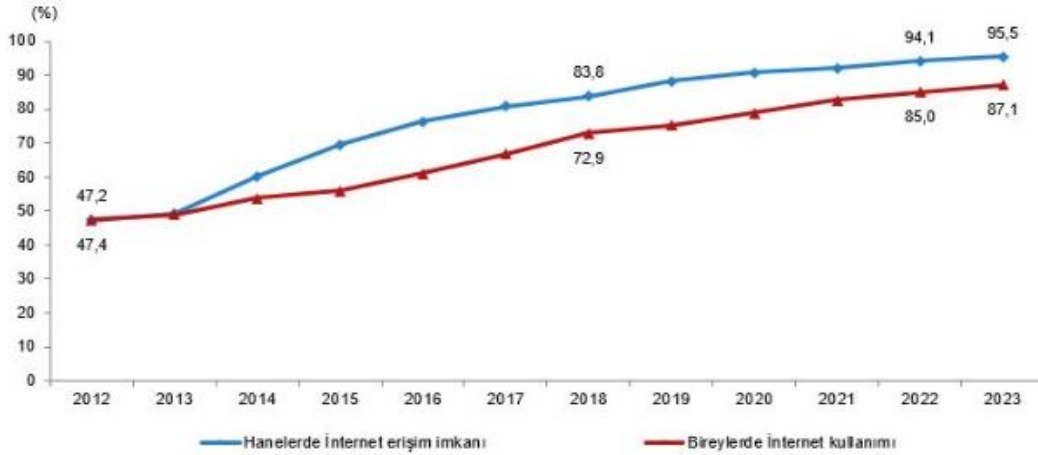
Keywords: Cybersecurity, Awareness, Faculty Members, Information Security

1. Giriş

Bilgi Teknolojilerindeki (BT) hızlı gelişim, bireylerin ve kurumların dijital sistemlere olan bağımlılığını artırmış; bu durum bilgiye erişimi kolaylaştırırken aynı zamanda çeşitli güvenlik risklerini de beraberinde getirmiştir. İnternetin yaygınlaşması, mobil teknolojilerin günlük yaşamın ayrılmaz bir parçası hâline gelmesi ve bulut bilişim uygulamalarının kurumsal yapılarda yoğun biçimde kullanılması, dijital ortamda üretilen ve paylaşılan veri miktarını önemli ölçüde artırmıştır [1,2].

Türkiye İstatistik Kurumu verilerine göre, 2012 yılında internet kullanan bireylerin oranı %47.4 iken bu oran 2023 yılında %87.1'e yükselmiştir. Benzer şekilde, internete erişim imkânına sahip hane oranı aynı dönemde %95.5 seviyesine ulaşmıştır [3]. Bu hızlı dijitalleşme süreci, bireysel ve kurumsal ölçekte siber tehditlere maruz kalma riskini de artırmıştır. BT, bu gelişmeler ve insan yaşamını kolaylaştıran, zenginleştiren yönleri sayesinde, kullanımı artık kaçınılmaz noktada olup, hatta günden güne artış göstermektedir. Şekil 1'de Türkiye İstatistik

Kurumunun verilerini inceleyecek olursak; 2012 yılında internet kullanan bireylerin oranı %47.4 iken, 2023 yılında %39.7 artışla %87.1 seviyesine çıkmıştır. İnternete erişen hane sayısının 2012 yılında %47.2 iken 11 yıl içinde %48.3 artışla %95.5 olduğunu görebiliriz [3].



Şekil 1. 2012-2023 yılları arasında internet erişim imkanı ve bireylerin internet kullanımı

Artan dijital etkileşimle birlikte zararlı yazılımlar, kimlik avı, dolandırıcılık, veri ihlalleri ve yanlış bilgi yayılımı gibi siber tehditler daha yaygın hâle gelmiştir. Bu tehditlere karşı korunma ihtiyacı, siber güvenlik kavramını hem bireyler hem de kurumlar açısından kritik bir konu hâline getirmiştir [4]. Özellikle üniversiteler gibi çok sayıda kullanıcıya, açık ağ yapılarına ve yüksek miktarda akademik veriye sahip kurumlar, siber saldırılar açısından riskli yapılar arasında yer almaktadır.

Üniversite öğretim elemanları, akademik faaliyetleri kapsamında dijital platformları yoğun biçimde kullanmakta; araştırma verileri, kişisel bilgiler ve kurumsal sistemler üzerinden sürekli etkileşim hâlinde bulunmaktadır. Bu durum, öğretim elemanlarının kişisel siber güvenlik farkındalık düzeylerini üniversitelerin genel bilgi güvenliği açısından önemli bir belirleyici hâline getirmektedir.

Bu çalışmada, Bursa Teknik Üniversitesi örneği üzerinden üniversite öğretim elemanlarının kişisel siber güvenlik farkındalık düzeylerinin demografik değişkenler çerçevesinde incelenmesi amaçlanmaktadır. Çalışmanın devamında, araştırmanın yöntemi, elde edilen bulgular ve sonuçlar ayrıntılı biçimde sunulmakta; elde edilen bulguların üniversitelerde siber güvenlik politikalarının geliştirilmesine sağlayabileceği katkılar tartışılmaktadır.

2. Siber Güvenlik

Teknolojideki hızlı gelişim, internet kullanım oranlarında da önemli bir artışa yol açmıştır. Günümüzde akıllı telefonlar ve bilgisayarlar bireysel yaşamın yanı sıra kamu kurumlarının işleyişinde de vazgeçilmez araçlar hâline gelmiştir. Bu dijital dönüşüm süreci, bireylerin günlük ihtiyaçlarını kolaylaştırırken aynı zamanda sanal ortamın kapsamını ve kullanım yoğunluğunu da artırmıştır. Artan bu dijital etkileşim, “siber uzay” kavramının ortaya çıkmasına neden olmuştur. Siber uzay, en genel tanımıyla internet üzerinden gerçekleşen tüm dijital etkileşimlerin yer aldığı sanal ortam olarak ifade edilmektedir.

Dijital dönüşümün hızlanmasıyla birlikte siber uzayın karmaşıklığı ve ölçeği önemli ölçüde artmış, buna paralel olarak 2000’li yılların başından itibaren “siber güvenlik” kavramı ön plana çıkmıştır. Stallings ve Brown’a göre siber güvenlik; bilgisayar sistemleri, ağlar, cihazlar ve verilerin yetkisiz erişim, değiştirme veya yok etme gibi tehditlere karşı korunmasını amaçlayan teknik ve yönetsel önlemler bütünüdür [5].

Günümüzde üniversiteler, sahip oldukları geniş kullanıcı kitlesi ve yoğun veri üretimi nedeniyle siber suçluların sıklıkla hedef aldığı kurumlar arasında yer almaktadır. Özellikle COVID-19 pandemi sürecinde uzaktan eğitim uygulamalarının yaygınlaşması, üniversitelerin dijital altyapılarını daha kritik hâle getirmiştir. Bu süreç, üniversitelerde teknoloji kullanımının yalnızca destekleyici değil, zorunlu bir unsur olduğunu açıkça ortaya koymuştur.

Üniversite öğretim elemanlarının mesleki ve akademik faaliyetlerinde internet ve dijital teknolojilerden yararlanması kaçınılmazdır. Akademik personelin birden fazla cihazla kampüs ağlarına erişmesi, üniversitelerin siber güvenlik risklerini artıran unsurlar arasında yer almaktadır. Üniversitelerin birbirine bağlı

ağ yapıları ve açık erişim politikaları, eğitim ve araştırma süreçlerini desteklerken aynı zamanda siber tehditlere karşı kırılganlığı da artırmaktadır. Bu bağlamda bireysel siber güvenlik farkındalığı, kurumsal güvenliğin önemli bir bileşeni hâline gelmektedir.

Teknolojik hizmetlerin çeşitlenmesi ve siber uzayın genişlemesi, internetin ilk kullanılmaya başlandığı dönemlerde öngörülemeyen yeni tehdit türlerinin ortaya çıkmasına neden olmuştur. Bu tehditler karşısında siber güvenlik önlemleri, yalnızca günümüz için değil, gelecekte de vazgeçilmez bir gereklilik olarak değerlendirilmektedir.

2.1. Siber Tehditler

Bilgi teknolojilerinde birçok farklı tehdit türü bulunmaktadır. Bu tehditler genel olarak iç tehditler ve dış tehditler olmak üzere iki ana kategoride sınıflandırılabilir. Dış tehditler, saldırıyı gerçekleştiren kişinin kurum dışından olması ve çeşitli siber saldırı yöntemleri kullanarak sistemlere zarar vermeyi amaçlamasıyla ortaya çıkmaktadır. İç tehditler ise bireysel kullanıcı hataları, kurum içindeki kötü niyetli çalışanlar, yetkisiz erişimler ve mevcut güvenlik açıkları gibi nedenlerden kaynaklanabilmektedir. Kurumlar ve bireyler, siber güvenlik stratejilerini oluştururken hem iç hem de dış tehditleri dikkate almalı ve buna uygun önlemler geliştirmelidir. Dış tehditlerin önlenmesi, iç tehditlere kıyasla daha zor olmakla birlikte, bireysel ve kurumsal önlemlerin yetersizliği ciddi güvenlik risklerine yol açabilmektedir.

Siber korsanlar, siber uzayda saldırı planlayan ve gerçekleştiren kişileri ifade etmektedir. Bu kişiler yetenek ve amaçlarına göre Beyaz Şapkalı, Siyah Şapkalı ve Gri Şapkalı korsanlar olarak sınıflandırılmaktadır. Beyaz şapkalı korsanlar, sistemlerdeki güvenlik açıklarını tespit ederek bu açıkların giderilmesine katkı sağlayan etik uzmanlardır. Siyah şapkalı korsanlar ise kötü niyetle sistemlere izinsiz erişim sağlayan, veri çalmayı veya zarar vermeyi amaçlayan bireylerdir. Gri şapkalı korsanlar, etik ve etik dışı yöntemleri birlikte kullanabilen; genellikle sisteme doğrudan zarar vermeyen ancak izinsiz erişim gerçekleştirebilen kişiler olarak tanımlanmaktadır.

Yöntemlerine göre sınıflandırıldığında siber korsanlar; kimlik avı saldırganları, fiziksel saldırganlar ve zararlı yazılım geliştiricileri olmak üzere üç grupta ele alınmaktadır. Kimlik avı saldırganları, kişisel ve hassas bilgilere erişebilmek amacıyla sahte e-postalar veya web siteleri gibi araçlar kullanmaktadır. Fiziksel saldırganlar, ağ altyapısına veya sistemlere doğrudan fiziksel müdahalede bulunabilmektedir. Zararlı yazılım geliştiricileri ise virüsler, solucanlar ve truva atları gibi zararlı yazılımlar aracılığıyla bilgi çalma, sistem bozma veya botnet oluşturma gibi faaliyetlerde bulunmaktadır.

Özellikle üniversitelerde akademisyenler ve öğrencilerin telefon, bilgisayar ve tablet gibi farklı cihazlarla ağa bağlanması, büyük ve karmaşık bir bilişim altyapısı oluşturmaktadır. Kendi cihazlarını kullanan kullanıcı sayısının fazla olması, üniversiteleri siber korsanlar açısından daha cazip hedefler hâline getirmektedir. Binlerce eş zamanlı erişimin bulunduğu kampüs ağları, saldırıların başarıya ulaşma olasılığını da artırmaktadır. Üniversitelerde öğrencilerin, akademik personelin ve idari çalışanların araştırma verilerinin ele geçirilmesi önemli saldırı nedenlerinden biridir. Akademisyenlerin iletişim bilgilerinin, özellikle e-posta adreslerinin üniversite web sitelerinde açık şekilde paylaşılması, oltalama e-postaları ve spam mesajlar yoluyla gerçekleştirilen saldırıların artmasına neden olmaktadır. Ayrıca akademik çalışmalar, ülkeler arası siber casusluk faaliyetlerine de konu olabilmektedir. Bilimsel araştırmaları ele geçirmek isteyen devletler veya organizasyonlar, siber saldırı yöntemleri kullanarak bu çalışmalara erişmeyi hedefleyebilmektedir. Bu nedenle üniversiteler, siber saldırıların öncelikli hedefleri arasında yer almaktadır [6].

2.2. Siber Saldırı Yöntemleri

Siber saldırı yöntemleri, amaç ve etki düzeylerine göre farklılık göstermektedir. Genel olarak pasif saldırılar bilgi toplamaya yönelikken, aktif saldırılar doğrudan sistemlere müdahale ederek zarar vermeyi hedeflemektedir. Bu çalışmada ele alınan saldırı türleri aktif saldırılar kapsamında değerlendirilmiştir. Günümüzde sıklıkla karşılaşılan başlıca siber saldırı yöntemleri aşağıda açıklanmaktadır.

- Fidyeye yazılımı (Ransomware): Fidyeye yazılımları, bilgisayar sistemlerini veya sistemlerde bulunan dosyaları (fotoğraflar, belgeler vb.) şifreleyerek erişilemez hâle getirmekte ve bu dosyaların tekrar kullanılabilmesi için fidye talep etmektedir. Bu tür saldırılar ciddi veri kayıplarına ve hizmet kesintilerine yol açabilmektedir [7].
- Truva atı (Causus Yazılımlar): Truva atları, görünüşte zararsız veya yararlı gibi görünen dosyaların içerisine gizlenmiş zararlı yazılımlardır. Kullanıcı tarafından indirildiğinde etkinleşerek güvenlik

açıklarını hedef alır ve sisteme sızmaya çalışır. Bilgi çalma, sistem bozma, botnet oluşturma gibi çeşitli kötü amaçlı faaliyetlerde kullanılabilir [8].

- Kimlik avı (Phishing): Kimlik avı saldırıları, kötü niyetli kişi veya grupların kullanıcıları yanıltarak kişisel ve hassas bilgilerini ele geçirmeyi amaçladığı yöntemlerdir. Bu saldırılar genellikle sahte e-postalar, kısa mesajlar veya telefon aramaları aracılığıyla gerçekleştirilmekte; kullanıcıların güven duygusu istismar edilmektedir [9].
- Dağıtılmış Hizmet Engelleme Saldırıları (DDoS): DDoS saldırıları, bir hizmeti veya ağı aşırı trafikle yükleyerek çalışamaz hâle getirmeyi amaçlamaktadır. Bu saldırılar genellikle birden fazla kaynaktan gelen yüksek miktarda trafikle hedef sistemlerin aşırı yüklenmesine neden olmaktadır [10].
- Ortadaki Adam (Man In The Middle Attack): Bu saldırı türünde saldırgan, iletişim hâlindeki iki taraf arasındaki veri akışını ele geçirerek verileri izleyebilir veya değiştirebilir. Salırgan, sahte yanıtlar göndererek iletilen bilgileri kendi amaçları doğrultusunda manipüle edebilmektedir.
- Zararlı yazılım enjeksiyonu (Injection Attacks): Zararlı yazılım enjeksiyonu saldırıları, web uygulamalarına kötü amaçlı kod enjekte edilmesi yoluyla gerçekleştirilir. Özellikle SQL enjeksiyonu yoluyla veritabanına erişim sağlanarak veri çalınabilir veya veriye zarar verilebilir. Ayrıca JavaScript enjeksiyonlarıyla kullanıcı oturumlarının ele geçirilmesi ve sistem komutlarının çalıştırılması mümkün hâle gelmektedir [11].
- Paket Çözümleme (Sniffing): Paket çözümleme saldırılarında, ağ trafiği içerisindeki veri paketleri yakalanarak analiz edilir ve bu yolla hassas bilgilere erişilmeye çalışılır. Şifrelenmemiş ağ trafiği üzerinden e-postalar, kullanıcı adları ve parolalar ele geçirilebilmektedir. Kurum ağlarında yeterli güvenlik önlemleri alınmadığında bu tür saldırılar ciddi riskler oluşturmaktadır [5].
- Kimlik sahteciliği (Spoofing): Kimlik sahteciliği saldırılarında saldırganlar, gerçek kimliklerini gizleyerek başka bir kullanıcı, cihaz veya ağ kaynağı gibi davranmaktadır. IP adresi gizleme, e-posta başlıklarını değiştirme veya sahte web sitesi oluşturma gibi yöntemlerle ağ trafiği yönlendirilebilmekte ya da kullanıcılar yanıltılabilmektedir [5].
- Güvenlik açıklarından yararlanma (Exploiting Security Vulnerabilities): Bu saldırı türü, yazılım veya sistemlerde bulunan güvenlik açıklarının saldırganlar tarafından istismar edilmesiyle gerçekleşmektedir. Hatalı kodlamalar veya güncellenmeyen yazılımlar, saldırganların sisteme yetkisiz erişim sağlamasına olanak tanımaktadır [12].
- Şifre kırma (Brute Force): Şifre kırma saldırılarında, sistemlere erişim sağlamak amacıyla olası tüm parola kombinasyonları sistematik olarak denenmektedir. Zayıf veya kısa parolalar, bu tür saldırılara karşı daha savunmasızdır [8].
- Sosyal mühendislik saldırıları: Sosyal mühendislik saldırıları, teknik zafiyetlerden ziyade insan faktörünü hedef almaktadır. Salırganlar; korku, aciliyet duygusu oluşturma, güven kazanma veya otoriteyi taklit etme gibi yöntemlerle kullanıcıları manipüle ederek istedikleri bilgilere erişim sağlamaktadır [13].

2.3. Önlemler (Precautions)

Siber güvenliğin temelini gizlilik, bütünlük ve erişilebilirlik ilkeleri oluşturmaktadır. Etkili bir siber güvenlik yaklaşımı, yalnızca teknik önlemlerle sınırlı kalmamalı; yönetsel, örgütsel ve bireysel boyutları kapsayan bütüncül bir bakış açısıyla ele alınmalıdır. Bu bağlamda, kurum genelinde tüm paydaşların siber güvenlik farkındalığını benimsemesi kritik önem taşımaktadır.

Alınacak önlemlerin başında kurumsal düzeyde bütünlüğün sağlanması gelmektedir. Özellikle üst yönetim ve bilgi işlem birimlerinin siber güvenlik konusundaki hassasiyeti, sürdürülebilir bir güvenlik altyapısının oluşturulmasında belirleyici rol oynamaktadır. Güncel ve sürekli değişen tehditlere karşı hazırlıklı olabilmek için, riskleri önceden tanımlayan ve düzenli olarak güncellenen bir güvenlik altyapısının kurulması gerekmektedir [14].

Siber güvenlik ihlallerinin önemli bir kısmı bireysel ihmallerden kaynaklanmaktadır. Bu nedenle kullanıcıların temel siber güvenlik uygulamalarını günlük alışkanlık hâline getirmeleri gerekmektedir. Güvenlik duvarlarının aktif hâle tutulması, uçtan uca şifreleme kullanımı, iki aşamalı kimlik doğrulama sistemlerinin etkinleştirilmesi ve akıllı filtreleme mekanizmalarının uygulanması bireysel düzeyde alınabilecek temel

önlemler arasında yer almaktadır. Ayrıca kullanılan cihazlardaki yazılımların güncel tutulması ve düzenli veri yedekleme işlemlerinin yapılması olası saldırılara karşı koruma sağlamaktadır [15].

Üniversite ortamlarında akademisyenler, idari personel ve öğrencilerin kullandıkları parolaların güçlü olması ve belirli aralıklarla değiştirilmesi gerekmektedir. Kurumsal web sayfalarında çalışanlara ait kişisel bilgilerin mümkün olduğunca sınırlı düzeyde paylaşılması, ortalama (phishing) saldırılarına karşı koruyucu bir önlem olarak değerlendirilmektedir. Kullanıcıların şüpheli e-postaları açmaması ve bu tür durumlarda ilgili birimlerle iletişime geçmeleri önem taşımaktadır.

Ağ güvenliğinin sağlanması amacıyla güvenlik duvarları, saldırı tespit sistemleri (IDS) ve saldırı önleme sistemleri (IPS) gibi ağ güvenlik çözümlerinin kullanılması önerilmektedir. Ağ trafiğinin düzenli olarak izlenmesi, olası tehditlerin erken aşamada tespit edilmesine katkı sağlamaktadır [16]. Ayrıca veri yedekleme süreçlerinin düzenli şekilde yürütülmesi, veri kaybı durumlarında iş sürekliliğinin korunmasını desteklemektedir.

Kurum bünyesinde geliştirilen veya dışarıdan temin edilen yazılım ve uygulamaların düzenli olarak güvenlik testlerinden geçirilmesi gerekmektedir. Siber güvenlik testleri ve denetimleri, sistemlerdeki zayıflıkların belirlenmesine ve gerekli önlemlerin zamanında alınmasına olanak tanımaktadır [17]. Bununla birlikte, siber güvenlik farkındalığının artırılması amacıyla kullanıcılara yönelik düzenli eğitimlerin verilmesi, bireylerin tehditleri tanıma ve doğru tepki verme becerilerini geliştirmektedir.

Sürekli gelişen ve değişen dijital tehdit ortamında, özellikle üniversiteler gibi bilgi yoğun kurumlarda siber güvenlik farkındalığının kurumsal bir kültür hâline getirilmesi gerekmektedir. Küçük görünen ihmallerin dahi ciddi güvenlik ihlallerine yol açabileceği göz önünde bulundurularak, bireysel bilinçlenme ve kurumsal önlemler birlikte ele alınmalıdır.

3. Uygulama

Bu çalışmada nicel araştırma yöntemi kullanılmıştır. Araştırmanın evrenini, 2023–2024 eğitim-öğretim yılında Bursa Teknik Üniversitesi'nde görev yapan akademik personel oluşturmaktadır. Çalışmada, olasılıksız örnekleme yöntemlerinden gönüllü örnekleme tekniği kullanılmış ve toplam 147 akademik personelden veri toplanmıştır.

Katılımcılara araştırmanın amacı, gizlilik ilkeleri ve gönüllülük esasları hakkında bilgi verilmiş; veriler çevrim içi anket formu aracılığıyla toplanmıştır. Katılımcıların yaş dağılımında özellikle 31–40 yaş grubunun öne çıktığı görülmektedir. Bu durum, araştırma bulgularının genellenebilirliğini sınırlayan bir unsur olarak değerlendirilmiş ve sınırlılıklar bölümünde ayrıca ele alınmıştır.

Araştırmada kullanılan anket formu, demografik bilgilere ilişkin sorular ile Kişisel Siber Güvenliği Sağlama Ölçeği maddelerinden oluşan iki bölüm halinde hazırlanmıştır. Elde edilen veriler, öğretim elemanlarının kişisel siber güvenlik farkındalık düzeyleri ile demografik değişkenler arasındaki ilişkileri belirlemek amacıyla analiz edilmiştir.

Araştırma, Bursa Teknik Üniversitesi Etik Kurulu'nun 2024/12 sayılı kararı ile etik açıdan uygun bulunmuştur.

3.1. Evren ve Örneklem

Araştırmanın evrenini, Bursa Teknik Üniversitesi'nde 2023–2024 eğitim-öğretim yılında görev yapan Profesör (n=78), Doçent (n=83), Doktor Öğretim Üyesi (n=141), Öğretim Görevlisi (n=90) ve Araştırma Görevlisi (n=176) unvanlarına sahip toplam 568 akademik personel oluşturmaktadır.

Araştırmanın örneklemini ise üniversitede görev yapan farklı unvan gruplarından gönüllü olarak katılım sağlayan 147 öğretim üyesi ve öğretim elemanı oluşturmuştur. Çalışma grubuna ait demografik özellikler Tablo 1'de sunulmuştur.

Tablo 1 incelendiğinde, cinsiyet dağılımı açısından erkek öğretim elemanlarının (%60.54) daha yüksek oranda temsil edildiği görülmektedir. Yaş dağılımı bakımından ise 31–40 yaş aralığındaki katılımcıların (%43.54) çalışmaya daha fazla katılım gösterdiği belirlenmiştir. Katılımcıların büyük bir kısmı Mühendislik ve Doğa Bilimleri Fakültesi'nde (%57.14) görev yapmaktadır.

Veriler incelendiğinde dikkat çeken bir diğer bulgu, antivirüs yazılımı kullanım oranının (%70.07) yüksek olmasıdır. Bu durum, katılımcıların kişisel ve cihaz güvenliğine önem verdiklerini göstermektedir. Buna karşılık, siber güvenlik eğitimi alma oranının (%21.09) görece düşük olduğu tespit edilmiştir.

Tablo 1. Çalışma grubunun demografik bilgilere göre sayıları ve yüzdelikleri

Değişken	Kategori	n	%
Cinsiyet	Kadın	58	39.46
	Erkek	89	60.54
Yaş	≤30	38	25.85
	31–40	64	43.54
	41–50	36	24.49
	≤51	9	6.12
Unvan	Prof. Dr.	15	10.20
	Doç. Dr.	26	17.69
	Dr. Öğr. Üyesi	30	20.41
	Öğr. Görevlisi	21	14.29
	Arş. Görevlisi	55	37.41
Görev Yapılan Birim (Fakülte/Enstitü)	Mühendislik ve Doğa Bilimleri	84	57.14
	Denizcilik	5	3.40
	İnsan ve Toplum Bilimleri	13	8.84
	Mimarlık ve Tasarım	7	4.76
	Orman	15	10.20
	Koordinatörlük	2	1.36
	Diğer	21	14.29
Antivirüs Yazılım Kullanma Durumu	Evet	103	70.07
	Hayır	44	29.93
Siber Güvenlik Eğitimi Alma Durumu	Evet	21	14.29
	Hayır	126	85.71
Siber Saldırıya Uğrama Durumu	Evet	31	21.09
	Hayır	116	78.91
Günlük İnternet Kullanım Durumu	6 saat ve altı (≤6)	79	53.74
	6 saat üstü (6<)	68	46.26
İnternet Kullanım Yılı	20 yıl ve altı (≤20)	101	68.71
	20 yıl üstü (20<)	46	31.29

3.2. Veri Toplama Araçları

Araştırmada veri toplama aracı olarak, Erol ve ark. (2015) tarafından geliştirilen Kişisel Siber Güvenliği Sağlama Ölçeği kullanılmıştır. Ölçek, bireylerin çevrim içi ortamlardaki siber güvenlik davranışlarını ölçmeyi amaçlamakta olup beş faktör ve toplam 25 maddeden oluşmaktadır. Ölçeğin alt boyutları; kişisel gizliliği koruma, ödeme bilgilerini koruma, güvenilmeyenden kaçınma, iz bırakmama ve önlem alma şeklindedir. Ölçekte yer alan 10 madde ters puanlanmıştır.

Katılımcılar, her bir maddeyi “1 = Hiçbir zaman” ile “5 = Her zaman” arasında değişen 5’li Likert tipi bir derecelendirme üzerinden değerlendirmiştir. Ölçeğin geliştirildiği çalışmada toplam Cronbach’s Alpha güvenirlik katsayısı 0.91 olarak raporlanmış; alt boyutlara ait güvenirlik katsayılarının ise 0.78–0.88 aralığında olduğu belirtilmiştir. Bu değerler, ölçeğin yüksek düzeyde güvenirliğe ve yapı geçerliğine sahip olduğunu göstermektedir [18].

Bu araştırma kapsamında elde edilen veriler IBM SPSS 29.0.2.0 programı kullanılarak analiz edilmiştir. Ölçeğin bu çalışma için hesaplanan güvenirlik katsayısı Cronbach’s Alpha (α) = 0.786 olarak bulunmuştur. Bu değer, ölçeğin yüksek düzeyde güvenilir olduğunu göstermektedir. Ölçeğe ilişkin güvenirlik istatistikleri Tablo 2’de sunulmuştur [19].

Tablo 2. Ölçeğin Cronbach alfa güvenirlik katsayısı

Cronbach Alfa (α)	Cronbach Alfa (standartlaştırılmış)	Madde Sayısı
0.786	0.786	25

3.3. Veri Analizi ve Yorumlanması

Normal dağılım varsayımını sağlamayan 15 katılımcının verileri analiz kapsamı dışında bırakılmıştır. Tablo 3'te, cinsiyet değişkeni ile ölçeğin alt boyutları arasındaki ilişkiyi belirlemek amacıyla gerçekleştirilen bağımsız örneklem t-testi sonuçları sunulmaktadır. Yapılan analizler sonucunda, yalnızca iz bırakmama alt boyutunda cinsiyete bağlı olarak istatistiksel açıdan anlamlı bir fark tespit edilmiştir ($t = 2.05$; $p < 0.05$). Bu bulgu, erkek katılımcıların dijital ortamda iz bırakmamaya yönelik davranış düzeylerinin kadın katılımcılara kıyasla daha yüksek olduğunu göstermektedir.

Ölçeğin diğer alt boyutlarında ise cinsiyete göre istatistiksel olarak anlamlı bir farklılık bulunmamıştır ($p > 0.05$).

Tablo 3. Cinsiyete göre siber güvenlik farkındalığı alt boyutlarının bağımsız örneklem t-testi sonuçları

Değişken	Cinsiyet	n	Ort.	SS	t	df	p
Kişisel gizliliği koruma	Erkek	78	39.86	5.24	0.66	130	0.512
	Kadın	54	39.19	5.05			
Güvenilmeyenden kaçınma	Erkek	78	17.65	2.75	-1.18	130	0.239
	Kadın	54	18.13	1.87			
Önlem alma	Erkek	78	18.28	3.54	1.40	130	0.163
	Kadın	54	17.39	3.69			
Ödeme bilgilerini koruma	Erkek	78	8.87	1.53	0.21	130	0.837
	Kadın	54	8.81	1.61			
İz bırakmama	Erkek	78	14.86	2.44	2.05	130	0.043
	Kadın	54	13.89	2.99			

Tablo 4'te, yaş değişkeninin ölçek alt boyutlarıyla olan ilişkisini incelemek amacıyla tek yönlü varyans analizi (ANOVA) uygulanmıştır. Analiz sonuçlarına göre, yaş değişkeni ile kişisel gizliliği koruma ve güvenilmeyenden kaçınma alt boyutları arasında istatistiksel olarak anlamlı farklılıklar tespit edilmiştir.

Buna karşın, önlem alma, ödeme bilgilerini koruma ve iz bırakmama alt boyutlarında yaş gruplarına göre anlamlı bir farklılık bulunmamıştır ($p > 0.05$). Elde edilen bulgular, yaş ilerledikçe kişisel gizliliği koruma farkındalığının arttığını; daha genç katılımcıların ise güvenilmeyen kaynaklardan kaçınma davranışlarında daha düşük ortalama puanlara sahip olduğunu göstermektedir.

Tablo 4. Siber güvenlik farkındalığının yaş gruplarına göre ANOVA analizi sonuçları

Değişken	Yaş	n	Ort.	F	p
Kişisel gizliliği koruma	≤30	35	37.09	4.47	0.005
	31-40	58	39.59		
	41-50	33	41.85		
	≥51	6	41.67		
Güvenilmeyenden kaçınma	≤30	35	18.46	3.04	0.031
	31-40	58	17.52		
	41-50	33	18.18		
	≥51	6	15.67		
Önlem alma	≤30	35	17.54	1.38	0.251
	31-40	58	17.48		
	41-50	33	18.94		
	≥51	6	18.67		
Ödeme bilgilerini koruma	≤30	35	8.49	1.79	0.153
	31-40	58	8.78		
	41-50	33	9.33		
	≥51	6	9.00		
İz bırakmama	≤30	35	14.14	1.45	0.233
	31-40	58	14.22		
	41-50	33	15.30		
	≥51	6	14.00		

Tablo 5’te, yaş grupları arasındaki farklılıkların hangi gruplar arasında ortaya çıktığını belirlemek amacıyla Hochberg post-hoc testi uygulanmıştır. Analiz sonuçlarına göre, kişisel gizliliği koruma alt boyutunda 41–50 yaş grubundaki katılımcıların, 30 yaş ve altı gruba kıyasla istatistiksel olarak anlamlı düzeyde daha yüksek ortalama puana sahip olduğu belirlenmiştir ($p=0.003$). Güvenilmeyenden kaçınma alt boyutunda ise 51 yaş ve üzeri katılımcılar ile 30 yaş ve altı katılımcılar arasında bir fark gözlenmiş olmakla birlikte, bu fark istatistiksel olarak sınırda anlamlılık düzeyinde bulunmuştur ($p=0.052$).

Elde edilen bulgular, yaş değişkeninin siber güvenlik farkındalığı üzerinde etkili bir faktör olabileceğine işaret etmektedir. Özellikle yaşın ilerlemesiyle birlikte kişisel verilerin korunmasına yönelik farkındalığın arttığı ve güvenilmeyen dijital kaynaklardan kaçınma davranışlarının güçlendiği görülmektedir.

Tablo 5. Kişisel gizliliği koruma ve güvenilmeyenden kaçınma alt boyutlarına ilişkin Hochberg post-hoc testi sonuçları

Alt Boyut	Karşılaştırılan Gruplar	Ort. Fark (I–J)	Std. Hata	p
Kişisel gizliliği koruma	41–50 yaş – ≤ 30 yaş	4.76	1.35	0.003
Güvenilmeyenden kaçınma	51 yaş ve üzeri – ≤ 30 yaş	2.79	1.05	0.052

Tablo 6’da, unvan değişkenine göre ölçek alt boyutları arasındaki varyansların homojenliğini değerlendirmek amacıyla Levene testi uygulanmıştır. Analiz sonuçlarına göre, yalnızca “ödeme bilgilerini koruma” alt boyutunda varyanslar arasında istatistiksel olarak anlamlı bir farklılık tespit edilmiştir ($p=0.004$).

Tablo 6. Unvan değişkenine göre siber güvenlik farkındalığının Levene varyans homojenliği testi sonuçları

Alt Boyut	Levene İstatistiği	df ₁	df ₂	p
Kişisel gizliliği koruma	0.724	4	127	0.577
Güvenilmeyenden kaçınma	0.342	4	127	0.849
Önem alma	1.633	4	127	0.170
Ödeme bilgilerini koruma	4.018	4	127	0.004
İz bırakmama	1.726	4	127	0.148

Tablo 7’de sunulan Welch testi sonuçlarına göre, unvan grupları arasında istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($p=0.160$). Bu bulgu, öğretim elemanlarının unvan düzeylerine göre (Prof. Dr., Doç. Dr., Dr. Öğr. Üyesi, Öğr. Gör. ve Arş. Gör.) ödeme bilgilerini koruma farkındalık düzeylerinin birbirine benzer olduğunu göstermektedir. Dolayısıyla, unvan değişkeninin bu alt boyut üzerinde anlamlı bir etkisinin bulunmadığı söylenebilir.

Tablo 7. Unvana göre ödeme bilgilerini koruma alt boyutuna ilişkin Welch analizi sonuçları

Değişken	Unvan	n	Ort.	SS	F	df ₁	df ₂	p
Ödeme Bilgilerini Koruma	Prof. Dr.	12	9.42	0.90	1.68	4	50.00	0.160
	Doç. Dr.	23	8.87	1.18				
	Dr. Öğr. Üyesi	28	9.21	1.37				
	Öğr. Görevlisi	21	8.43	2.11				
	Arş. Görevlisi	48	8.67	1.64				
	Toplam	132	8.85	1.56				

Tablo 8’de yer alan ANOVA testi sonuçlarına göre, unvan değişkeni açısından yalnızca kişisel gizliliği koruma alt boyutunda istatistiksel olarak anlamlı bir fark saptanmıştır ($p<0.05$). Diğer alt boyutlar (güvenilmeyenden kaçınma, önem alma, ödeme bilgilerini koruma ve iz bırakmama) açısından ise unvan değişkenine göre anlamlı bir farklılık bulunmamıştır ($p>0.05$).

Tablo 8. Siber güvenlik farkındalığının unvana göre ANOVA analizi sonuçları

Değişken	Unvan	n	Ort.	F	p
Kişisel gizliliği koruma	Prof. Dr.	12	42	3.389	0.011
	Doç. Dr.	23	40.52		
	Dr. Öğr. Üyesi	28	41.82		

	Öğr. Görevlisi	21	38.33		
	Arş. Görevlisi	48	37.77		
Güvenilmeyenden kaçınma	Prof. Dr.	12	16.83	2.038	0.093
	Doç. Dr.	23	17.43		
	Dr. Öğr. Üyesi	28	18.35		
	Öğr. Görevlisi	21	17.09		
	Arş. Görevlisi	48	18.33		
Önlem alma	Prof. Dr.	12	19.41	1.376	0.246
	Doç. Dr.	23	18.69		
	Dr. Öğr. Üyesi	28	18.17		
	Öğr. Görevlisi	21	17.47		
	Arş. Görevlisi	48	17.20		
İz bırakmama	Prof. Dr.	12	15.25	0.657	0.623
	Doç. Dr.	23	14.86		
	Dr. Öğr. Üyesi	28	14.60		
	Öğr. Görevlisi	21	14.09		
	Arş. Görevlisi	48	14.14		

Tablo 8’de saptanan anlamlı farklılığın hangi unvan grupları arasında ortaya çıktığını belirlemek amacıyla Tablo 9’da Post-Hoc testlerinden Hochberg analizi uygulanmıştır. Analiz sonuçlarına göre, kişisel gizliliği koruma alt boyutunda Dr. Öğretim Üyesi unvanına sahip katılımcılar ile Araştırma Görevlisi unvanına sahip katılımcılar arasında, Dr. Öğretim Üyeleri lehine istatistiksel olarak anlamlı bir farklılık bulunduğu görülmüştür ($p<0.05$).

Tablo 9. Kişisel gizliliği koruma faktörüne ilişkin Hochberg post-hoc analizi sonuçları

(I) Unvan	(J) Unvan	Ortalama Fark (I-J)	Std. Hata	p
Prof. Dr	Doç. Dr	1.478	1.985	0.998
	Dr. Öğr. Üyesi	0.179	1.923	1.000
	Öğr. Görevlisi	3.667	2.017	0.516
	Arş. Görevlisi	4.229	1.799	0.183
Doç. Dr.	Dr. Öğr. Üyesi	-1.300	1.568	0.994
	Öğr. Görevlisi	2.188	1.682	0.880
	Arş. Görevlisi	2.751	1.413	0.418
Dr. Öğr. Üyesi	Öğr. Görevlisi	3.488	1.609	0.274
	Arş. Görevlisi	4.051	1.325	0.027
Öğr. Görevlisi	Arş. Görevlisi	0.563	1.458	1.000

Tablo 10’da yer alan ANOVA testi sonuçlarına göre, görev yapılan birim değişkeni ile siber güvenlik farkındalığının hiçbir alt boyutu arasında istatistiksel olarak anlamlı bir fark saptanmamıştır ($p>0.05$). Bu bulgu, öğretim elemanlarının görev yaptıkları fakülte veya birimlere göre siber güvenlik farkındalığı düzeylerinin benzer olduğunu göstermektedir.

Güvenilmeyenden kaçınma alt boyutu için varyansların homojen dağılmaması nedeniyle ANOVA analizine dâhil edilmemiştir. Bu alt boyut, varsayımlar doğrultusunda Levene testi ile ayrıca değerlendirilmiştir.

Tablo 10. Siber güvenlik farkındalığının görev yapılan birime göre ANOVA analizi sonuçları

Değişken	Birim	n	Ort.	F	p
Kişisel gizliliği koruma	Denizcilik	5	37.60	0.97	0.443
	Diğer	21	37.47		
	İnsan ve Toplum Bilimleri	11	39.36		
	Koordinatörlük	2	40.00		
	Mimarlık ve Tasarım	5	43.20		

Önlem alma	Mühendislik ve Doğa Bilimleri	75	40.04	1.26	0.270
	Orman	13	39.84		
	Denizcilik	5	16.2		
	Diğer	21	17.19		
	İnsan ve Toplum Bilimleri	11	16.72		
	Koordinatörlük	2	19.00		
	Mimarlık ve Tasarım	5	20.20		
	Mühendislik ve Doğa Bilimleri	75	1.97		
	Orman	13	19.38		
	Denizcilik	5	9.00		
Ödeme bilgilerini koruma	Diğer	21	8.00	1.73	0.110
	İnsan ve Toplum Bilimleri	11	9.09		
	Koordinatörlük	2	10.00		
	Mimarlık ve Tasarım	5	8.80		
	Mühendislik ve Doğa Bilimleri	75	9.08		
	Orman	13	8.46		
	Denizcilik	5	15.00		
İz bırakmama	Diğer	21	14.09	0.274	0.940
	İnsan ve Toplum Bilimleri	11	13.90		
	Koordinatörlük	2	15.50		
	Mimarlık ve Tasarım	5	14.20		
	Mühendislik ve Doğa Bilimleri	75	14.62		
	Orman	13	14.30		
	Denizcilik	5	15.00		

Tablo 11’de, görev yapılan birime göre güvenilmeyenden kaçınma faktörüne ilişkin varyans homojenliğini test etmek amacıyla Levene testi uygulanmıştır. Analiz sonuçlarına göre, gruplar arasında istatistiksel olarak anlamlı bir farklılık tespit edilmiştir ($p < 0.05$). Bu nedenle varyans eşitliği varsayımı sağlanamadığından, gruplar arasındaki farkın incelenmesi amacıyla Welch testi uygulanmıştır.

Tablo 11. Görev yapılan birime göre güvenilmeyenden kaçınma faktörü için Levene testi sonuçları

Değişken	Levene İstatistiği	df ₁	df ₂	p
Güvenilmeyenden kaçınma	2.322	6	125	0.037

Tablo 11’de yapılan analiz sonucunda varyansların homojen olmadığı belirlenmiştir (Levene $p < 0.05$). Bu nedenle, görev yapılan birime göre karşılaştırmalar Tablo 12’de Welch testi kullanılarak gerçekleştirilmiştir.

Tablo 12. Görev Yapılan Birime Göre Güvenilmeyenden Kaçınma Faktörünün Welch Testi Sonuçları

Değişken	Welch İstatistiği	df ₁	df ₂	p
Güvenilmeyenden kaçınma	5.257	6	11.016	0.009

Tablo 13’te, Welch testi sonucunda elde edilen anlamlılığın hangi gruplar arasında ortaya çıktığını belirlemek amacıyla Games–Howell post-hoc testi uygulanmıştır. Analiz sonuçlarına göre, Denizcilik biriminde görev yapan katılımcıların güvenilmeyenden kaçınma düzeylerinin, diğer birimlerde görev yapan katılımcılara kıyasla istatistiksel olarak anlamlı düzeyde daha yüksek olduğu belirlenmiştir ($p < 0.05$).

Ayrıca, Mimarlık biriminde görev yapan katılımcıların güvenilmeyenden kaçınma farkındalık düzeylerinin, hem Diğer birimlerde hem de Mühendislik ve Doğa Bilimleri Fakültesi biriminde görev yapan katılımcılara kıyasla anlamlı biçimde daha yüksek olduğu saptanmıştır ($p < 0.05$). Diğer birimler arasındaki karşılaştırmalarda ise istatistiksel olarak anlamlı bir farklılık tespit edilmemiştir ($p > 0.05$).

Tablo 13. Güvenilmeyenden kaçınma faktörüne göre Games–Howell testi sonuçları

(I) Birim	(J) Birim	Ortalama Fark (I–J)	Std. Hata	p
Denizcilik	Diğer	2.638	0.715	0.02

Diğer	Mimarlık	-2.838	0.641	0.003
Mimarlık	Mühendislik ve Doğa Bilimleri	1.880	0.385	0.001

Tablo 14’te, antivirüs kullanımı değişkeni ile ölçek alt boyutları arasındaki ilişkiyi incelemek amacıyla bağımsız örneklem t-testi uygulanmıştır. Analiz sonuçlarına göre, önlem alma alt boyutunda antivirüs kullanan katılımcılar ile kullanmayanlar arasında, antivirüs kullananlar lehine istatistiksel olarak anlamlı bir fark bulunmuştur ($p<0.05$). Buna karşılık, kişisel gizliliği koruma, güvenilmeyenden kaçınma, ödeme bilgilerini koruma ve iz bırakmama alt boyutlarında antivirüs kullanım durumuna göre anlamlı bir farklılık tespit edilmemiştir ($p>0.05$).

Tablo 14. Siber güvenlik farkındalığının antivirüs kullanımı durumuna göre T-testi sonuçları

Değişken	Antivirüs Kullanımı	n	Ort.	SS	t	df	p
Kişisel gizliliği koruma	Hayır	42	38.45	5.54	-1.575	84.042	0.119
	Evet	90	40.11	5.33			
Güvenilmeyenden kaçınma	Hayır	42	17.71	2.54	-0.432	130	0.667
	Evet	90	17.91	2.38			
Önlem alma	Hayır	42	15.57	3.00	-5.667	130	<0.001
	Evet	90	19.01	3.14			
Ödeme bilgilerini koruma	Hayır	42	8.73	1.87	-0.499	63.100	0.620
	Evet	90	8.90	1.39			
İz bırakmama	Hayır	42	14.59	2.57	0.385	130	0.701
	Evet	90	14.40	2.77			

Tablo 15’te, siber güvenlik eğitimi alma değişkeni ile ölçek alt boyutları arasındaki ilişkiyi incelemek amacıyla bağımsız örneklem t-testi uygulanmıştır. Analiz sonuçlarına göre, siber güvenlik eğitimi alma durumuna bağlı olarak ölçeğin hiçbir alt boyutunda istatistiksel olarak anlamlı bir farklılık tespit edilmemiştir ($p>0.05$). Bu bulgu, siber güvenlik eğitimi alan ve almayan öğretim elemanlarının kişisel siber güvenlik farkındalık düzeylerinin benzer olduğunu göstermektedir.

Tablo 15. Siber güvenlik farkındalığının siber eğitim alma durumuna göre T-testi sonuçları

Değişken	Eğitim Alma	n	Ort.	SS	t	df	p
Kişisel gizliliği koruma	Hayır	114	39.62	5.77	-1.645	130	0.102
	Evet	18	39.33	5.95			
Güvenilmeyenden kaçınma	Hayır	114	17.82	2.45	-0.950	130	0.344
	Evet	18	18	2.37			
Önlem alma	Hayır	114	17.92	3.58	-1.270	130	0.206
	Evet	18	17.83	3.89			
Ödeme bilgilerini koruma	Hayır	114	8.96	1.43	-0.521	130	0.603
	Evet	18	8.11	2.11			
İz bırakmama	Hayır	114	14.42	2.69	-1.216	130	0.226
	Evet	18	14.66	2.84			

Tablo 16’da, siber saldırıya maruz kalma değişkeni ile ölçek alt boyutları arasındaki ilişkiyi incelemek amacıyla bağımsız örneklem t-testi uygulanmıştır. Analiz sonuçları, siber saldırıya maruz kalma durumuna göre ölçeğin hiçbir alt boyutunda istatistiksel olarak anlamlı bir farklılık bulunmadığını göstermektedir ($p>0.05$). Bu bulgu, siber saldırıya maruz kalan ve kalmayan öğretim elemanlarının kişisel siber güvenlik farkındalık düzeylerinin benzer olduğunu ortaya koymaktadır.

Tablo 16. Siber güvenlik farkındalığının siber saldırıya maruz kalma durumuna göre bağımsız örneklem T-Testi sonuçları

Değişken	Saldırıya Uğrama	n	Ort.	SS	t	df	p
----------	------------------	---	------	----	---	----	---

Kişisel gizliliği koruma	Hayır	102	39.74	5.83	0.592	130	0.555
	Evet	30	39.03	5.60			
Güvenilmeyenden kaçınma	Hayır	102	17.68	2.57	-1.418	130	0.158
	Evet	30	18.40	1.77			
Önlem alma	Hayır	102	17.88	3.76	-0.202	130	0.841
	Evet	30	18.033	3.4			
Ödeme bilgilerini koruma	Hayır	102	8.92	1.59	0.993	130	0.323
	Evet	30	8.46	1.42			
İz bırakmama	Hayır	102	14.29	2.93	-1.319	130	0.190
	Evet	30	15.03	1.77			

Tablo 17’de, günlük internet kullanımı değişkeninin ölçek alt boyutları ile olan ilişkisini belirlemek amacıyla bağımsız örneklem t-testi uygulanmıştır. Analiz sonuçlarına göre, yalnızca ödeme bilgilerini koruma alt boyutunda istatistiksel olarak anlamlı bir fark saptanmıştır ($p<0.05$). Söz konusu farkın, günlük internet kullanım süresi 6 saatten fazla olan katılımcılar lehine gerçekleştiği görülmektedir. Diğer alt boyutlar açısından günlük internet kullanım süresine göre istatistiksel olarak anlamlı bir farklılık bulunmamıştır ($p>0.05$).

Tablo 17. Siber güvenlik farkındalığının günlük internet kullanımına göre T-testi sonuçları

Değişken	Günlük İnternet Kullanımı	n	Ort.	SS	t	df	p
Kişisel gizliliği koruma	≤ 6 saat	67	39.25	6.05	-0.665	130	0.508
	> 6 saat	65	39.92	5.49			
Güvenilmeyenden kaçınma	≤ 6 saat	67	17.77	2.52	-0.346	130	0.730
	> 6 saat	65	17.92	2.35			
Önlem alma	≤ 6 saat	67	17.417	3.33	-1.620	130	0.108
	> 6 saat	65	18.430	3.83			
Ödeme bilgilerini koruma	≤ 6 saat	67	8.567	1.67	-2.137	127.063	0.035
	> 6 saat	65	9.138	1.39			
İz bırakmama	≤ 6 saat	67	14.597	2.60	0.580	130	0.563
	> 6 saat	65	14.323	2.82			

Tablo 18’de, yıllık internet kullanım süresi değişkeni ile ölçek alt boyutları arasındaki ilişkiyi incelemek amacıyla bağımsız örneklem t-testi uygulanmıştır. Yapılan analizler sonucunda, yıllık internet kullanım süresine göre ölçeğin hiçbir alt boyutunda istatistiksel olarak anlamlı bir farklılık tespit edilmemiştir ($p>0.05$). Bu bulgu, yıllık internet kullanım süresinden bağımsız olarak öğretim elemanlarının siber güvenlik farkındalık düzeylerinin benzer olduğunu göstermektedir.

Tablo 18. Siber güvenlik farkındalığının internet kullanım yılına göre T-testi sonuçları

Değişken	Yıllık internet kullanımı	n	Ort.	SS	t	df	p
Kişisel gizliliği koruma	≤ 20 yıl	90	39.02	5.47	-1.645	130	0.102
	> 20 yıl	42	40.78	6.26			
Güvenilmeyenden kaçınma	≤ 20 yıl	90	17.71	2.47	-0.950	130	0.344
	> 20 yıl	42	18.14	2.33			
Önlem alma	≤ 20 yıl	90	17.64	3.75	-1.270	130	0.206
	> 20 yıl	42	18.50	3.24			
Ödeme bilgilerini koruma	≤ 20 yıl	90	8.80	1.64	-0.521	130	0.603
	> 20 yıl	42	8.95	1.37			
İz bırakmama	≤ 20 yıl	90	14.26	2.89	-1.216	130	0.226
	> 20 yıl	42	14.88	2.22			

4. Tartışma ve Sonuç

Bu araştırmada, Kişisel Siber Güvenlik Farkındalığı Ölçeği demografik değişkenler doğrultusunda değerlendirilmiş ve yapılan istatistiksel analizler sonucunda çeşitli anlamlı bulgular elde edilmiştir. Ölçekte yer alan 25 madde, beş alt boyut (faktör) kapsamında ele alınmış; gruplar arası ve grup içi karşılaştırmalar gerçekleştirilmiştir. Öğretim üyeleri ve öğretim elemanlarının cinsiyet, yaş, unvan, görev yapılan birim, antivirüs yazılımı kullanma durumu, siber güvenlik eğitimi alma durumu, siber saldırıya maruz kalma durumu, günlük internet kullanım süresi ve internet kullanım yılı değişkenleri siber güvenlik farkındalığı bağlamında incelenmiştir.

Cinsiyet değişkenine ilişkin analiz sonuçları, yalnızca iz bırakmama alt boyutunda anlamlı bir farklılık olduğunu göstermiştir. Bulgulara göre erkek katılımcıların bu alt boyutta siber güvenlik farkındalık düzeyleri kadın katılımcılara kıyasla daha yüksektir. Bu sonuç, erkeklerin çevrim içi gizlilik ve kişisel veri paylaşımı konularında daha temkinli davrandığını ortaya koyan önceki çalışmalarla paralellik göstermektedir [20]. Erkeklerin dijital ortamlarda risk algılarının daha yüksek olması ve kişisel bilgilerin korunmasına yönelik davranışsal duyarlılıkları, bu farklılığın temel nedenleri arasında değerlendirilebilir. Dolayısıyla söz konusu farkın, toplumsal cinsiyet rolleriyle ilişkili risk algısı ve psikososyal hassasiyet farklılıklarından kaynaklandığı düşünülmektedir.

Yaş değişkenine ilişkin analizlerde, kişisel gizliliği koruma alt boyutunda 31–40 yaş aralığındaki katılımcıların, 30 yaş ve altındaki katılımcılara kıyasla daha yüksek farkındalık düzeyine sahip olduğu belirlenmiştir. Bu durum, orta yaş grubundaki bireylerin dijital ortamlarda daha uzun süreli deneyime sahip olmaları ve artan mesleki sorumluluk bilinci ile açıklanabilir.

Unvan değişkeni açısından elde edilen bulgular, kişisel gizliliği koruma faktöründe Dr. Öğretim Üyesi unvanına sahip katılımcıların, Araştırma Görevlilerine kıyasla daha yüksek siber güvenlik farkındalığına sahip olduğunu göstermektedir. Bu farklılığın, doktora düzeyindeki akademisyenlerin araştırma etiği, veri gizliliği ve akademik sorumluluk konularında daha fazla eğitim ve farkındalık kazanmış olmalarından kaynaklandığı değerlendirilmektedir. Literatürde de akademik kıdem ve eğitim düzeyinin dijital farkındalığı artırdığına yönelik bulgular mevcuttur. Nitekim Yerby, Koohang ve Paliszkievicz (2019), bireylerin çevrim içi risk algılarının bilgi güvenliği davranışlarıyla doğrudan ilişkili olduğunu ve bu ilişkinin eğitim düzeyi arttıkça daha belirgin hâle geldiğini vurgulamıştır [21].

Görev yapılan birim değişkenine göre yapılan analizler, güvenilmeyenden kaçınma alt boyutunda Denizcilik Fakültesi katılımcılarının Diğer birimlerde çalışanlara göre; Mimarlık Fakültesi katılımcılarının ise hem Diğer birimler hem de Mühendislik ve Doğa Bilimleri Fakültesi katılımcılarına kıyasla daha yüksek farkındalık düzeyine sahip olduğunu ortaya koymuştur. Bu fakültelerde kullanılan teknik sistemlerin çeşitliliği ve uygulama yoğunluğu, veri güvenliği konularında daha yüksek dikkat gerektirmektedir. Öte yandan Mühendislik ve Doğa Bilimleri Fakültesi katılımcılarında beklenenin aksine daha düşük farkındalık düzeylerinin gözlenmesi, teknik yeterliliğin zaman zaman aşırı özgüvene yol açarak risklerin hafife alınmasına neden olabileceği şeklinde yorumlanabilir [22].

Antivirüs yazılımı kullanan katılımcıların önlem alma alt boyutundaki puanlarının anlamlı biçimde daha yüksek olması, teknik koruma araçlarını aktif biçimde kullanan bireylerin siber güvenlik bilincini davranışa dönüştürme eğilimlerinin daha güçlü olduğunu göstermektedir. Benzer şekilde, günlük internet kullanım süresi altı saatin üzerinde olan katılımcıların ödeme bilgilerini koruma alt boyutunda daha yüksek farkındalık düzeyine sahip olmaları, dijital ortamda daha uzun süre vakit geçiren bireylerin siber tehditlerle daha sık karşılaşmaları sonucu öğrenilmiş bir dikkat geliştirdiklerine işaret etmektedir.

Buna karşın siber güvenlik eğitimi alma durumu, siber saldırıya maruz kalma durumu ve internet kullanım yılı değişkenleri açısından anlamlı bir farklılık saptanmamıştır. Bu durum, üniversite düzeyinde verilen siber güvenlik eğitimlerinin yeterince sistematik ve davranış odaklı olmamasından kaynaklanabilir. Siber güvenlik eğitimlerinin etkili olabilmesi için yalnızca bilgi aktarımına değil, davranış değişikliğini hedefleyen uygulamalı ve etkileşimli içeriklere odaklanılması gerekmektedir.

Araştırma bulguları, öğretim üyeleri ve öğretim elemanlarının siber güvenlik farkındalık düzeylerinin bazı demografik değişkenlere göre anlamlı farklılıklar gösterdiğini ortaya koymaktadır. Bu doğrultuda üniversite yönetimlerinin, bireysel farkındalığı artırmanın yanı sıra kurumsal siber direnç kapasitesini güçlendirmeye yönelik bütüncül politikalar geliştirmesi önem arz etmektedir. Üniversite bünyesinde zorunlu siber güvenlik

farkındalık eğitimlerinin uygulanması; bu eğitimlerin phishing (oltalama) simülasyonları, güçlü parola oluşturma uygulamaları ve veri ihlali senaryoları gibi etkileşimli modüller içermesi önerilmektedir. Eğitim içeriklerinin yaş ve unvan farklılıklarına göre yapılandırılması, farkındalığın davranışa dönüşmesini destekleyebilir.

Bilgi İşlem Daire Başkanlığı tarafından yürütülen bilgi güvenliği politikalarının kullanıcı düzeyinde uygulanabilir hâle getirilmesi; parola politikaları, e-posta güvenliği, harici bellek kullanımı ve kişisel cihazların kampüs ağına erişim kurallarının netleştirilmesi gerekmektedir. Ayrıca iki aşamalı kimlik doğrulama, otomatik güvenlik uyarıları ve şüpheli bağlantı tespit sistemleri gibi teknik önlemlerin yaygınlaştırılması önerilmektedir. Her fakültede bir "Siber Güvenlik Temsilcisi" görevlendirilmesi, akademik personel ile bilgi işlem birimleri arasındaki iletişimi güçlendirebilir. Düzenli farkındalık anketleri ile gelişimin izlenmesi ve bu verilerin kalite süreçlerine entegre edilmesi de kurumsal öğrenmeyi destekleyecektir. Siber güvenliğin yalnızca teknik bir konu değil, kurumsal bir kültür unsuru olduğu vurgulanmalı ve bu farkındalık çeşitli etkinliklerle görünür kılınmalıdır [23].

Bu araştırma, tek bir devlet üniversitesi örneklemiyle sınırlıdır. Katılımcıların yaş dağılımı ve birim çeşitliliği, elde edilen bulguların genellenebilirliğini sınırlandırmaktadır. Gelecek çalışmalarda farklı üniversiteleri kapsayan daha geniş örneklemlerle veri toplanması, yaş, akademik kıdem ve dijital alışkanlıklar arasındaki etkileşimlerin daha ayrıntılı incelenmesine katkı sağlayacaktır. Ayrıca nitel veri toplama yöntemlerinin (örneğin odak grup görüşmeleri) kullanılması, siber güvenlik farkındalığının bilişsel ve davranışsal boyutlarının daha derinlemesine anlaşılmasına olanak tanıyacaktır.

Yazar Katkıları: Kavramsallaştırma, H.Ş. ve S.Ö.; metodoloji, S.Ö.; yazılım, H.Ş. ve S.Ö.; doğrulama, H.Ş.; biçimsel analiz, H.Ş.; soruşturma, H.Ş.; kaynaklar, S.Ö.; veri iyileştirme, Ö.F.E.; yazı- orijinal taslak hazırlama, Ö.F.E, H.Ş. ve S.Ö.; yazma- gözden geçirme ve düzenleme, H.Ş. ve Ö.F.E.; görselleştirme, H.Ş. ve S.Ö. Tüm yazarlar makalenin yayınlanan versiyonunu okudu ve kabul etti.

Finansman: Bu araştırma dışarıdan fon almadı.

Çıkar çatışmaları: Bu çalışma, Bursa Teknik Üniversitesi, Etik Kurulu tarafından etik açıdan onaylanmıştır. Bunun dışında yazarlar, çalışmayla ilgili herhangi bir ticari veya finansal çıkar çatışması bulunmadığını beyan eder.

Kaynakça

- [1] T. Posa and J. Grossklags, "Work experience as a factor in cyber-security risk awareness: A survey study with university students," *J. Cybersecurity and Privacy*, vol. 8, no. 2, pp. 490–515, 2022.
- [2] J. Smith, "The role of cloud computing in big data analytics and artificial intelligence," *J. Cloud Comput.*, vol. 10, no. 3, pp. 45–47, 2020.
- [3] Türkiye İstatistik Kurumu (TÜİK), "Veri Portalı," [Online]. Available: <https://data.tuik.gov.tr>, Accessed: Aug. 29, 2023.
- [4] M. Köprülü, "Üniversite öğretim elemanlarının kişisel siber güvenlik farkındalık durumlarının belirlenmesi: Yıldız Teknik Üniversitesi örneği," M.S. thesis, Eğitim Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, Türkiye, 2023.
- [5] W. Stallings, *Cybersecurity: Principles and Practice*, 2nd ed. London: Pearson Education, 2017.
- [6] Y. Kaya, *Bilgisayar Mühendisliği Temelleri*. Ankara, Türkiye: Seçkin Yayıncılık, 2008.
- [7] A. Gorainoff, *Ransomware: Everything You Need to Know About Ransomware*. Independently Published, 2020.
- [8] J. Erickson, *Hacking: The Art of Exploitation*. San Francisco, CA: No Starch Press, 2003.
- [9] C. Hadnagy, *Social Engineering: The Art of Human Hacking*. Hoboken, NJ: Wiley, 2010.
- [10] P. A. Henry, *Denial of Service Attacks: Real Threats and Practical Solutions*. Syngress, 2006.
- [11] D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Hoboken, NJ: Wiley, 2011.
- [12] G. M. Hoglund and G. McGraw, *Exploiting Software: How to Break Code*. Boston, MA: Addison-Wesley, 2004.
- [13] J. Steinberg, *Cybersecurity for Dummies*. Hoboken, NJ: Wiley, 2019.
- [14] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Hoboken, NJ: Wiley, 2002.
- [15] S. Masum, "Çalışanların siber güvenlik farkındalıklarının araştırılması," M.S. thesis, Fen Bilimleri Enstitüsü, İstanbul Üniversitesi, İstanbul, Türkiye, 2022.
- [16] F. Aslay, "Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi," *Int. J. Multidiscip. Stud. Innov. Technol.*, vol. 1, no. 1, pp. 24–28, 2017.
- [17] C. Almaz, M. Sevi, and İ. Tuğal, "Üniversitelerdeki siber güvenlik sorunları ve farkındalık eğitimleri," *Bilişim Teknolojileri Dergisi*, vol. 14, no. 3, pp. 229–238, 2021.
- [18] O. Erol, Y. L. Şahin, E. Yılmaz, and H. İ. Haseski, "Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması," *Int. J. Human Sciences*, vol. 12, no. 2, pp. 75–91, 2015.
- [19] S. Kılıç, "Cronbach'ın alfa güvenirlik katsayısı," *J. Mood Disorders*, vol. 6, no. 1, pp. 47–48, 2016.
- [20] S. Tüfekçi Aslım and G. Saraçoğlu, "Öğretmen adaylarının e-öğrenme stilleri ile dijital okuryazarlık arasındaki ilişki," *Trakya Eğitim Dergisi*, vol. 13, no. 3, pp. 1404–1426, 2023.

-
- [21] J. Yerby, A. Koohang, and J. Paliszkiewicz, "Social media privacy concerns and risk beliefs," *Online J. Appl. Knowl. Manage.*, vol. 7, no. 1, pp. 1–13, 2019.
- [22] L. Hadlington, "Employees attitudes towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom," *Int. J. Cyber Criminol.*, vol. 12, no. 1, pp. 269–281, 2018.
- [23] T. Zengin, U. Didinir, G. Bayar, and H. Şahin, "AR-GE merkezi proje yönetim sisteminde dijital dönüşüm," *Academic Perspective Procedia*, pp. 1–10, 2022.