İŞLETME ARAŞTIRMALARI DERGİSİ
JOURNAL OF BUSINESS RESEARCH-TURK
2025, 17(4), 3311-3326
https://doi.org/10.20491/isarder.2025.2153

İşgörenlerin Siber Güvenlik Farkındalıklarının Ölçülmesi: Van İli Örneği

Measurement of Employees' Cybersecurity Awareness: The Case of Van Province

Recep ALMALI [a] **Celal KIZILDERE** [b]

[a] Van Yüzüncü Yıl Üniversitesi, Sosyal Bilimler Enstitüsü, Van, Türkiye. recepalmalı@gmail.com
[b] Van Yüzüncü Yıl Üniversitesi, Erciş İşletme Fakültesi, Van, Türkiye. celalkzldere@gmail.com

MAKALE BİLGİSİ

Anahtar Kelimeler:
İşgören
Bilgi Teknolojileri
Bilgi Güvenliği
Siber Güvenlik

Gönderilme Tarihi 8 Mart 2025
Revizyon Tarihi 7 Aralık 2025
Kabul Tarihi 10 Aralık 2025

Makale Kategorisi:
Araştırma Makalesi

ÖZET

Amaç – Çalışmanın temel amacı, Van ilinde çalışan bireylerin siber güvenlik farkındalık düzeylerini ölçmek ve bu farkındalık düzeylerinin demografik faktörlerle (yaş, cinsiyet, eğitim seviyesi, sektör) olan farklılıklarını analiz etmektir. Çünkü dijital dönüşümün hızla arttığı günümüzde, siber güvenlik farkındalığının önemi bireyler ve kurumlar için giderek artmaktadır. Araştırma, siber güvenlik stratejilerinin geliştirilmesinde ve çalışanların eğitim ihtiyaçlarının belirlenmesinde yol gösterici olmayı hedeflemektedir.

Yöntem – Araştırmada kullanılan veriler, Van ilinde aktif olarak çalışan 451 bireyle anket yöntemi kullanılarakelde edilmiştir.Daha sonra toplanan bu veriler, SPSS ve AMOS istatistiksel programları aracılığı ile analize tabi tutulmuştur.

Bulgular – Elde edilen bulgular, demografik faktörlerin genel farkındalık düzeyini doğrudan etkilemediğini, ancak cinsiyet ve yaş gibi alt boyutlarda farklılıklar yarattığını göstermiştir. Çalışma, eğitim seviyesinin farkındalık üzerinde etkili olduğunu ve sürekli eğitim ile bireysel farkındalık artırma çabalarının önemli olduğunu ortaya koymaktadır. Sektör faktörünün de farkındalık üzerinde belirgin bir etkisi olmadığı, ancak sektörlere özgü tehditlere yönelik eğitim programlarının faydalı olacağı görülmüştür.

Tartışma – Bu çalışma, siber güvenlik farkındalığının artırılmasında demografik faktörlerin tek başına belirleyici olmadığını, ancak eğitimin sürekli ve sektöre özgü özelleştirilmesinin daha etkili sonuçlar doğuracağına dikkat çekmektedir. Ayrıca, farkındalık eğitimlerinin düzenli olarak güncellenmesi ve bireylerin ihtiyaçlarına göre şekillendirilmesi gerektiği görülmektedir. Araştırmabulgularının, kurumların siber güvenlik stratejilerini geliştirmelerine ve çalışanlarının eğitim ihtiyaçlarını belirlemelerine yardımcı olacak önemli bir yol haritası sunmaya katkı sağlayacağıdüşünülmektedir.

ARTICLE INFO

Keywords:
Employee
Information Technology
Information Security
Cybersecurity

Received 8 March 2025
Revised 7 December 2025
Accepted 10 December 2025

Article Classification:
Research Article

ABSTRACT

Purpose – The primary aim of this study is to measure the cyber security awareness levels of employees in Van province and examine the relationship between these awareness levels and demographic factors (age, gender, education level, sector). In today's rapidly advancing digital transformation, the importance of cyber security awareness is increasing for both individuals and institutions. This research aims to serve as a guide in developing cyber security strategies and identifying the training needs of employees.

Design/methodology/approach – The data used in this study were obtained through a survey conducted with 451 actively working individuals in Van province. The collected data were then analyzed using SPSS and AMOS statistical software.

Results – The findings indicate that demographic factors do not directly effect overall awareness levels, but variables such as gender and age created differences in subdimensions. The study reveals that education level significantly influences awareness and high lights the importance of continuous education in enhancingin dividual awareness. It was also observed that the sector factor does not have a significant impact on awareness; however, sector-specifictraining programs addressing specific threat scould be beneficial.

Discussion – This study emphasizes that demographic factors alone are not decisive in increasing cybe rsecurity awareness. However, continuous and sector-specific education proves to be more effective. Additionally, cyber security awareness training should be regularly updated and tailored to the needs of individuals. Theres earch findings are expected to contribute to the development of cyber security strategies in institutions and assist in identifying the training needs of employees, providing a significant roadmap for this purpose.

*Bu çalışma, Almalı'nın yüksek lisans tezinden üretilmiştir.

ETİK ONAY: : Çalışmanın etik onay izni Van Yüzüncü Yıl Üniversitesi Sosyal Bilimler Enstitüsü Etik Komisyonu tarafından 23.05.2024 tarihli 2024/10-12 sayılı karar ile alınmıştır.

Önerilen Atıf/ Suggested Citation
Almalı, R., Kızıldere, C. (2025). İşgörenlerin Siber Güvenlik Farkındalıklarının Ölçülmesi: Van İli Örneği, İşletme Araştırmaları Dergisi, 17 (4), 3311-3326.

1. Giriş

Dijitalleşme, iş dünyasında köklü değişiklikler yaratan ve bilgi teknolojilerinin giderek daha merkezi bir rol oynadığı bir süreci tanımlar. (Schwab, 2016: 11-17) tarafından ifade edildiği gibi, dördüncü sanayi devrimiyle birlikte dijital dönüşüm, hem iş dünyasında büyük fırsatlar yaratmakta hem de beraberinde önemli bilgi güvenliği riskleri getirmektedir. Bu dönüşüm, bilgi güvenliği ve siber güvenliği, işletmelerin sürdürülebilirliğini ve veri güvenliğini sağlamak adına kritik stratejik konular haline getirmiştir (Enısa, 2023: 13-16). Ancak, dijitalleşmenin hızla ilerlemesine rağmen, literatürde siber güvenlik farkındalığına ilişkin bazı önemli boşluklar bulunmaktadır.

Özellikle, literatürde siber güvenlik farkındalığının yalnızca genel düzeyde ölçülmesi ve demografik faktörlerin etkilerinin incelenmesi üzerinde yoğunlaşılmıştır. Ancak, sektörler arası farkların ve kültürel etmenlerin siber güvenlik farkındalığına olan etkisi konusunda daha fazla araştırmaya ihtiyaç duyulmaktadır. Ayrıca, bireylerin siber güvenlik farkındalık seviyelerinin pratikte nasıl uygulandığına dair daha derinlemesine çalışmalar eksiktir. Çoğu çalışma, farkındalık düzeyini artırmak için eğitim programları önerirken, eğitim yöntemlerinin etkinliği ve sektöre özgü ihtiyaçlar üzerine yeterince odaklanmamaktadır.

Bunun yanı sıra, bireylerin siber güvenlik konusundaki psikolojik motivasyonları ve bu motivasyonların farkındalık seviyelerine nasıl etki ettiği üzerine de sınırlı sayıda çalışma bulunmaktadır. Eğitim stratejileri ve kurumsal farkındalık programlarının bireysel davranışlar üzerindeki etkisinin daha ayrıntılı bir şekilde araştırılması gereklidir. Ayrıca, literatürde siber güvenlik farkındalığının zaman içinde nasıl değiştiği, eğitim ve bilinçlendirme programlarının etkinliğinin sürdürülebilirliği gibi konularda daha fazla uzun vadeli araştırmalara ihtiyaç olduğu görülmektedir.

Bu çalışma, Van ilinde çalışan bireylerin siber güvenlik farkındalık düzeylerini demografik faktörlerle ilişkilendirerek, literatürdeki bu boşlukları doldurmayı amaçlamaktadır. Bu bağlamda, sektörel farklar, eğitim yöntemlerinin etkinliği gibi konularda daha fazla bilgi edinilmesi hedeflenmektedir.

2. Literatür Araştırması

Siber güvenlik farkındalığı, dijitalleşmenin hız kazanmasıyla birlikte bireylerin ve kurumların korunmasında kritik bir faktör haline gelmiştir. Son yıllarda artan siber saldırılar, bu farkındalığı daha önemli hale getirmiştir. Literatürde siber güvenlik farkındalığının farklı demografik gruplar üzerindeki etkisi, siber tehditlerin ekonomik boyutu ve farkındalık artırma stratejileri üzerine pek çok çalışma yapılmıştır.

Kruger ve Kearney (2012), çalışanların bilgi güvenliği farkındalık seviyelerini değerlendirmek için geliştirdikleri Information Security Awareness (ISA) Modeli ile farkındalık seviyelerini ölçmenin kurumsal güvenlik stratejilerinin başarısına doğrudan katkıda bulunduğunu vurgulamışlardır. Bu model, farkındalık düzeylerini belirlemeye yönelik anket ve test kombinasyonları içermekte ve sonuçlar, farklı sektörlerdeki çalışanların bilgi güvenliği farkındalığının çeşitli düzeylerde olduğunu göstermektedir.

İlk kapsamlı çalışmalardan biri, (Kınay, Sözcü, Taşkın ve İpek 2014), tarafından yapılan ve İstanbul'da bir özel üniversitede öğrencilerin bilgi güvenliği farkındalık seviyelerini değerlendiren çalışmadır. Bu çalışmada geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği, farkındalık düzeylerini "yüksek", "orta" ve "düşük" olarak sınıflandırmış ve her seviyeye uygun öneriler sunmuştur.

Tayvan Milli Eğitim Bakanlığı (2015), tarafından yürütülen İnternet Güvenliğinde Öğretmen Farkındalığı (TAIS) projesi, öğretmenlerin çevrimiçi güvenlik konusundaki bilgi düzeylerini artırmayı amaçlamıştır. Proje kapsamında seminerler, atölye çalışmaları ve konferanslar düzenlenmiş, ancak projenin son aşamasında hedeflenen kitleye tam olarak ulaşılamamıştır.

STM ve Fortinet (2016), raporlarına göre Türkiye fidye yazılım (ransomware) saldırılarında Avrupa'da ilk sırada yer almakta ve online bankacılık saldırılarından en fazla etkilenen ülkelerden biri olarak dikkat çekmektedir.

Fulya Aslay (2017), Türkiye'nin fidye yazılım (ransomware) ve zararlı yazılım (malware) tehditlerinde Avrupa'da üst sıralarda yer aldığını belirtmiştir. Çalışma, özellikle Türkiye'de bu tehditlere karşı farkındalığın artırılması gerektiğini vurgulamaktadır.

Aloul (2017), körfez ülkelerindeki üniversite öğrencileri üzerinde yaptığı araştırmada, sosyal mühendislik saldırıları (phishing) ve kötü niyetli yazılımlar hakkında öğrencilerin farkındalık düzeylerinin düşük olduğunu ortaya koymuştur. Eğitim programlarının dijital güvenlik farkındalığı üzerindeki olumlu etkisini vurgulamıştır.

Puhakainen ve Siponen (2020), bilgi güvenliği farkındalığını artırmanın en etkili yollarından birinin bireyselleştirilmiş eğitim programları olduğunu savunmuşlardır. Çalışma, eğitimde kullanılan hikâye anlatımı ve oyunlaştırma yöntemlerinin farkındalık düzeyini artırmada başarılı sonuçlar verdiğini göstermektedir.

CybersecurityVentures (2021) verilerine göre, siber suçların küresel maliyeti, 2015 yılında 3 trilyon dolar iken, bu maliyetin 2025 yılında 10,5 trilyon dolara ulaşması beklenmektedir.

Cengiz Gündüz Alp (2021), Türkiye'deki üniversitelerin bilgi işlem birimlerinde çalışanların dijital güvenlik farkındalıklarını incelemiş ve kadın çalışanların farkındalık düzeyinin erkeklere kıyasla daha yüksek olduğunu; ayrıca, 51-60 yaş grubundaki çalışanların diğer yaş gruplarına göre daha yüksek farkındalık seviyesine sahip olduğunu tespit etmiştir.

Check Point Research (2022) raporunda, dünya genelinde haftalık siber saldırıların 2021'e göre %38 oranında arttığı ve özellikle finans, eğitim ve sağlık sektörlerinin hedef alındığı belirtilmiştir.

Jeong ve arkadaşları (2022), ulusal kültürel faktörlerin kamu ve özel sektörlerdeki siber güvenlik stratejilerini şekillendirdiğini ve bu faktörlerin siber güvenlik yatırımlarında belirleyici olduğunu göstermiştir.

Kumar ve arkadaşları (2023), yapay zekâ tabanlı güvenlik sistemlerinin daha güvenilir ve şeffaf hale getirilmesi için açıklanabilir yapay zekâ kullanımının gerekliliğini vurgulamıştır. Bu çalışma, yapay zekâ uygulamalarında güvenlik ve şeffaflık sağlanmasının önemine dikkat çekmektedir.

3. Yöntem

3.1. Araştırmanın Modeli

Bu araştırma, tarama modellerinden biri olan tekil tarama modeli kullanılarak gerçekleştirilmiştir. Tekil tarama modeli, mevcut durumu olduğu gibi açıklamaya yönelik bir yaklaşımdır ve olayların sebeplerine odaklanmak yerine mevcut özelliklerini ve aralarındaki bağlantıları incelemeye öncelik verir (Karasar, 2012). Araştırmanın odağındaki olay, kişi ya da nesne, doğal koşulları içinde olduğu gibi incelenir; herhangi bir müdahale veya değişiklik yapılmaz. Bu model, değişkenlerin türlerini veya miktarlarını ayrı ayrı belirlemeyi amaçlayan betimsel bir araştırma modelidir.

Bu çalışmada tekil tarama modeli, Van ilinde çalışan bireylerin siber güvenlik farkındalık düzeylerini ölçmek amacıyla kullanılmıştır. Araştırmanın temel amacı, çalışanların siber güvenlik farkındalık düzeylerini belirlemek ve bu farkındalık düzeyinin demografik faktörlere göre değişiklik gösterip göstermediğini incelemektir. Bu bağlamda, araştırma verileri anket yöntemi ile toplanmış ve elde edilen veriler istatistiksel analizlere tabi tutulmuştur.Araştırma için Van Yüzüncü Yıl Üniversitesi Sosyal Bilimler Enstitüsü Etik Kurulu'nun 23.05.2024 tarih ve 2024/10-12 sayılı kararı ile Etik Kurul izni alınmıştır.

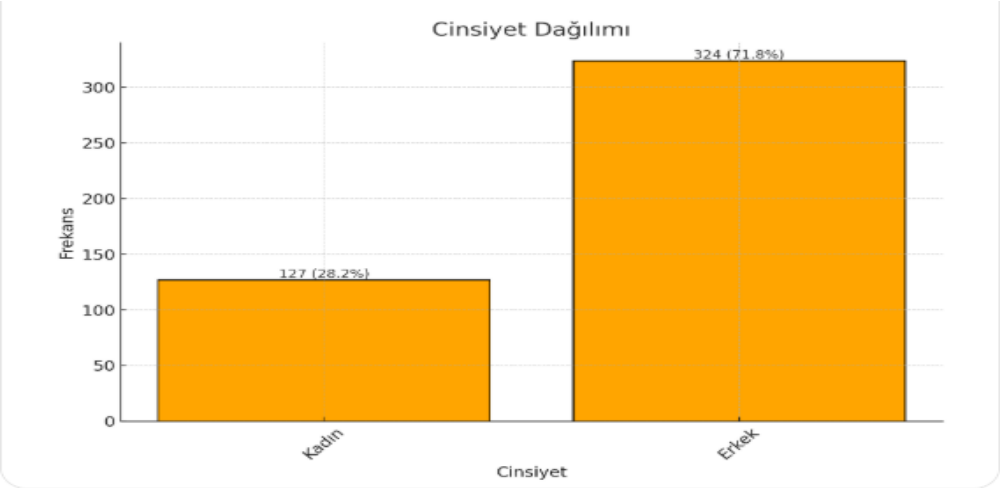
3.2. Evren ve Örneklem

Araştırmanın evreni, Van ilinde ikamet eden ve aktif iş hayatında bulunan bireylerden oluşmaktadır. Araştırmanın örneklemi, rastgele örnekleme yöntemi ile seçilen 451 katılımcıdanteşekkül etmektedir. Örneklem seçiminde, katılımcıların Van ilinde yaşaması ve aktif olarak bir işte çalışıyor olması temel kriter olarak belirlenmiştir. Araştırmaya katılanlara şu iki soru yöneltilmiştir:

Van ilinde mi yaşıyorsunuz?

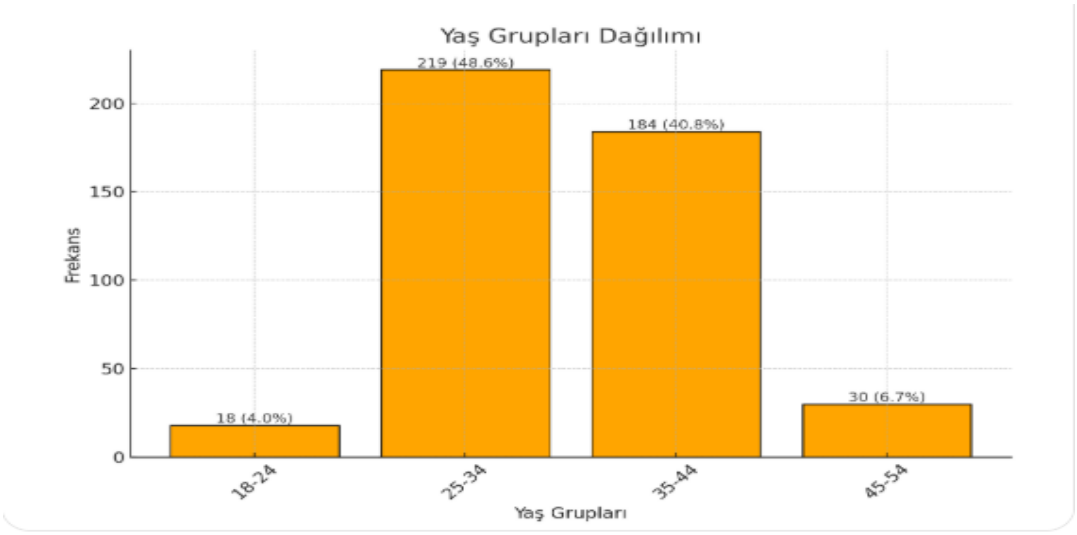
Van ilinde yaşıyorsanız, aktif bir işte çalışıyor musunuz?

Bu sorulara "Hayır" cevabı veren katılımcılar, kapsam dışında bırakılmıştır. Anket sonuçları, katılımcıların demografik özelliklerine göre aşağıdaki tablolarda gösterilmiştir.



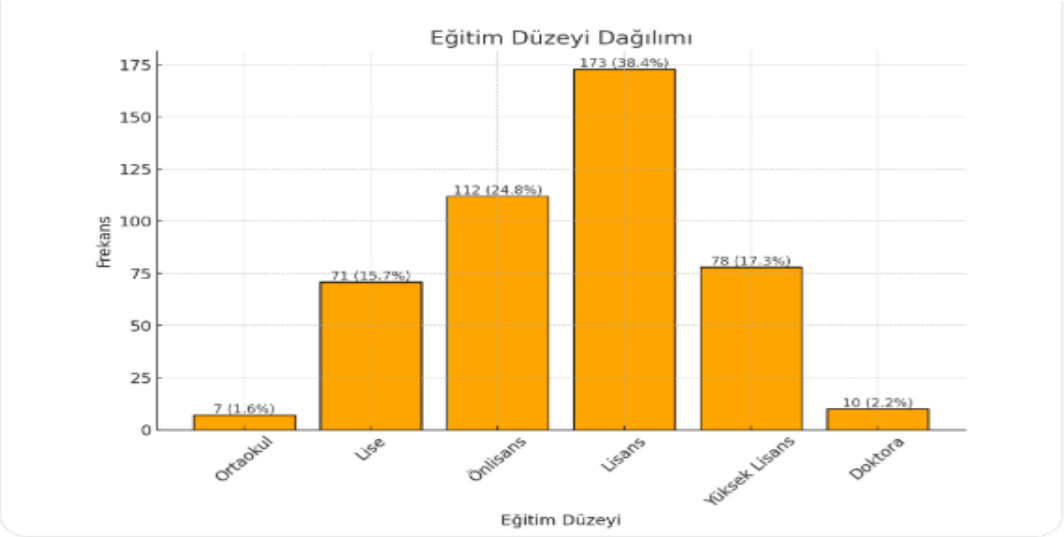
Şekil 1. Araştırmanın katılımcılarına ait cinsiyet dağılımı

Şekil 1'de gösterildiği gibi anket çalışmasına katılan ve Van ilinde ikamet edip aktif olarak çalışma hayatında bulunan 451 katılımcının %71,8'i (n=324) erkek, %28,2'si (n=127) kadındır.



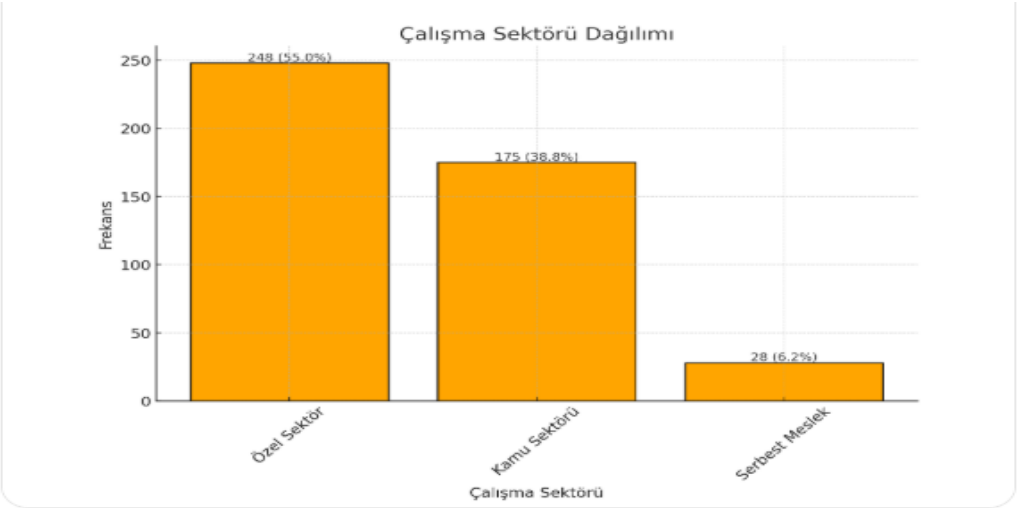
Şekil 2. Araştırmanın katılımcılarına ait yaş dağılımı

Şekil 2'de gösterildiği gibi katılımcıların yaş dağılımına bakıldığında, %48,6'sının (n=219) 25-34 yaş aralığında olduğu görülmektedir. Aynı şekilde %40,8'i (n=184) 35-44 yaş aralığında, %6,7'si (n=30) 45-54 yaş aralığında, %4,0'ı (n=18) ise 18-24 yaş aralığında yer almaktadır.



Şekil 3. Araştırmanın katılımcılarına ait eğitim düzeyi dağılımı

Şekil 3'te gösterildiği gibi katılımcıların eğitim düzeyi incelendiğinde, %1,6'sının (n=7) ortaokul, %15,7'sinin (n=71) lise, %24,8'inin (n=112) ön lisans, %38,4'ünün (n=173) lisans, %17,3'ünün (n=78) yüksek lisans ve%2,2'sinin (n=10) doktora mezunu olduğu belirlenmiştir.



Şekil 4. Araştırmanın katılımcılarına ait çalışılan sektör dağılımı

Şekil 4'te gösterildiği gibi katılımcıların çalıştıkları sektörlere göre dağılımı incelendiğinde, %55,0'ının (n=248) özel sektörde, %38,8'inin (n=175) kamu sektöründe ve%6,2'sinin (n=28) serbest meslek kategorisinde olduğu belirlenmiştir.

3.3. Veri toplama araçları

Bu araştırmada, nicel araştırma yöntemlerinden biri olan anket tekniği kullanılarak veriler toplanmıştır. Arpaci, I., & Sevinç, K. (2022).tarafından geliştirilen Siber Güvenlik Ölçeği temel alınarak hazırlanan anket formu, Google Forms aracılığıyla çevrimiçi olarak uygulanmış ve katılımcılara elektronik ortamda ulaştırılmıştır. Çevrimiçi katılımın yanı sıra, belirli katılımcılarla yüz yüze görüşmeler de gerçekleştirilmiştir.

Anket formu, iki bölümden oluşmaktadır:

Birinci bölüm, katılımcıların demografik özelliklerini belirlemeye yönelik 4 sorudan oluşmaktadır (cinsiyet, yaş, eğitim durumu, çalışılan sektör).

İkinci bölüm, katılımcıların siber güvenlik farkındalık düzeylerini ölçmek amacıyla hazırlanmış 24 ifadeden oluşmaktadır. Katılımcılar, bu ifadeleri 5'li Likert ölçeği (1: Kesinlikle Katılmıyorum, 5: Kesinlikle Katılıyorum) üzerinden değerlendirmiştir. Anket sonuçları, daha sonra istatistiksel analizlere tabi tutulmuş ve bulgular araştırmanın amaçları doğrultusunda yorumlanmıştır.

3.4. Araştırmanın Hipotezleri

H1: Cinsiyet değişkeni açısından katılımcıların siber güvenlik farkındalık düzeylerinde anlamlı farklılık vardır.

H2: Yaş değişkeni açısından katılımcıların siber güvenlik farkındalık düzeylerinde anlamlı farklılık vardır.

H3: Eğitim düzeyi açısından katılımcıların siber güvenlik farkındalık düzeylerinde anlamlı farklılık vardır.

H4: Çalışılan sektör açısında, katılımcıların siber güvenlik farkındalık düzeylerinde anlamlı farklılık vardır.

3.5. Siber Güvenlik Ölçeği

Araştırmada kullanılan veri toplama aracı, Arpacı ve Sevinç (2022) tarafından geliştirilen Siber Güvenlik Ölçeği (SGÖ) olmuştur. Bu ölçek, 5'li Likert tipi bir değerlendirme aracıdır ve katılımcıların siber güvenlik farkındalık düzeylerini ölçmek için geliştirilmiştir. Ölçek, Gizlilik, Kontrol/Sahiplik, Bütünlük, Gerçeklik, Erişilebilirlik ve Fayda olmak üzere 6 farklı faktörden oluşan toplam 24 maddeyi kapsamaktadır.

Katılımcılar, ölçek maddelerini "Kesinlikle Katılıyorum" (5) ile "Kesinlikle Katılmıyorum" (1) arasında derecelendirmiştir. Puanlama sırasında:

17 madde doğrudan (1'den 5'e doğru) puanlanırken,

7 ters madde ise ters puanlama yöntemiyle (5'ten 1'e doğru) değerlendirilmiştir.

3.6. Verilerin Analizi

Bu çalışmada elde edilen veriler, SPSS 30.0 ve AMOS 24.0 istatistik programları kullanılarak analiz edilmiştir. Betimleyici istatistikler, katılımcıların genel eğilimlerini ve veri dağılımlarını incelemek amacıyla kullanılmıştır.

Araştırmanın analiz sürecinde aşağıdaki istatistiksel yöntemler uygulanmıştır:

Cronbach Alpha Güvenilirlik Testi: Kullanılan ölçeğin iç tutarlılığını ve güvenilirliğini değerlendirmek için uygulanmıştır.

Doğrulayıcı Faktör Analizi (DFA): Ölçeğin yapı geçerliliğini test etmek ve faktör yapısının doğruluğunu belirlemek amacıyla AMOS programı ile gerçekleştirilmiştir.

Korelasyon Analizi: Değişkenler arasındaki ilişkileri belirlemek ve bu ilişkilerin yönü ile gücünü değerlendirmek amacıyla kullanılmıştır.

Bağımsız Gruplar t-Testi: Katılımcıların demografik özelliklerine göre gruplar arasında anlamlı fark olup olmadığını değerlendirmek için uygulanmıştır.

Tek Yönlü Varyans Analizi (ANOVA): Farklı gruplar arasında anlamlı farkların olup olmadığını belirlemek amacıyla kullanılmıştır.

Tüm analizler, verilerin güvenilirliğini ve geçerliliğini artırmak ve elde edilen bulguların daha tutarlı bir şekilde yorumlanmasını sağlamak için dikkatle yürütülmüştür.

Tablo 1. Güvenirlik Analizi Sonucu

Cronbach AlfaKat sayısı	Standartlaştırılmış Maddeler Cronbach Alfa Kat sayısı	İfade sayısı
0,790	0,802	24

Tablo 1'de görüldüğü gibi, Cronbach Alpha değeri 0.70'in üzerinde hesaplanmıştır. Bu sonuç, ölçeğin genel ve boyut bazında yüksek düzeyde güvenilirliğe sahip olduğunu göstermektedir. Cronbach Alpha katsayısı, bir ölçeğin maddelerinin aynı yapıyı ölçüp ölçmediğini değerlendiren ve iç tutarlılığı ortaya koyan önemli bir göstergedir. Katsayı değeri 0.70'in üzerinde olan ölçekler, genellikle güvenilir olarak kabul edilir (Nunnally, 1978; aktaran, Liu, 2003). Bu durumda, elde edilen sonuçlar, ölçek maddelerinin tutarlı ve güvenilir sonuçlar verdiğini göstermektedir.

Tablo 2. Ortalama, Çarpıklık ve Basıklık Değerleri (N=451)

	Min.	Max.	Ort.	S.S.	Çar.	Bas.
1-Siber ortamda paylaştığım kişisel bilgiler konusunda temkinliyimdir.	1	5	4,06	0,942	-1,167	1,397
2-Gerçek hayatta üçüncü şahıslarla paylaşmak istemediğim bilgi ve belgeleri siber ortamda da paylaşmam.	1	5	4,16	0,897	-1,318	2,034
3-Siber ortamda paylaştığım verilerin sadece gerekli kişilerce görüntülenmesini sağlarım.	1	5	3,98	1,018	-1,257	1,324
4-Hesaplarıma ait şifrelerin güvenliği konusunda dikkatliyim.	1	5	4,24	0,880	-1,532	2,997
5-Şifremi oluştururken sembol, rakam ya da büyük küçük harflerden oluşan tahmini zor bir şifre seçerim.	1	5	4,30	0,870	-1,580	2,813
6-E-posta şifremin güvenliği için telefon doğrulaması hizmetini kullanırım.	1	5	4,19	0,973	-1,382	1,488
7-Cevabını hatırlayacağım bir güvenlik sorusu seçmeye özen gösteririm.	1	5	4,21	0,912	-1,571	2,787
8-Kredi kartı bilgilerimin kaydedilmemiş olmasına dikkat ederim.	1	5	4,23	0,989	-1,445	1,699
9-Siber ortamda veri saklamak güvenli değildir.	1	5	3,91	0,968	-0,845	0,574
10-Siber ortamda sakladığım bilgi ve belgeler kaybolabilir ya da silinebilir.	1	5	3,82	0,997	-0,900	0,617
11-Siber ortamda veri paylaşımı yapmak herhangi bir risk içermez.	1	5	3,92	1,071	-0,959	0,435
12-Siber ortamda saklanan bilgi ve belgelere üçüncü şahısların erişme olasılığı vardır.	1	5	3,96	1,031	-1,269	1,422
13-Tanımadığım kişilerden gelen e-postalardaki linkleri ve eklentileri açarım.	1	5	4,00	1,151	-1,169	0,536
14-Girdiğim web sitesinin güvenlik sertifikası olmadığı yönünde bildirim gelse de kullanmaya devam ederim.	1	5	3,64	1,154	-0,543	-0,624
15-E-postama gelen istenmeyen (spam) postaları açtığım olmuştur.	1	5	3,47	1,258	-0,225	-1,287
16-E-postama gelen müşteri edinme/oltalama amaçlı postaları açtığım olmuştur.	1	5	3,65	1,146	-0,552	-0,609
17-Belirsiz kaynaklardan gelen bağlantıları (linkleri) ve dosyaları açtığım olmuştur.	1	5	3,64	1,161	-0,535	-0,783
18-Cihazımda güncel bir anti virüs programı var.	1	5	3,31	1,244	-0,401	-0,976
19-Cihazımı düzenli olarak anti virüs programı ile taratırım.	1	5	3,27	1,274	-0,315	-1,056
20-Cihazıma Kurulu gelen güvenlik duvarı açık.	1	5	3,29	1,179	-0,379	-0,803
21-İnternetten indirdiğim dosyaları cihazımda yüklü anti virüs programı olmasa da açarım.	1	5	3,33	1,189	-0,183	-1,029
22-Siber ortamda sosyal medya uygulamalarını bilgi paylaşımı için kullanırım.	1	5	3,10	1,153	-0,292	-0,928
23-Günlük hayatta karşılaştığım problemleri çözmek için siber ortamı yaygın olarak kullanırım.	1	5	3,22	1,170	-0,301	-0,876
24-Siber ortamda sunulan hizmetlerden bilgi yönetimi (bilgiyi elde etmek, saklamak, paylaşmak ve kullanmak) için faydalanırım.	1	5	3,58	1,069	-0,738	-0,012

Tablo 2'de, araştırma verilerinin normalliğini değerlendirmek amacıyla çarpıklık (skewness) ve basıklık (kurtosis) değerleri incelenmiştir. Literatürde, verilerin normal dağılım gösterdiğini kabul etmek için bu değerlerin belirli sınırlar içinde olması gerektiği belirtilmektedir.

Tabachnick ve Fidell (2015), çarpıklık ve basıklık değerlerinin −1.5 ile +1.5 aralığında olması gerektiğini ifade ederken,

George ve Mallery (2002) bu sınırları −2 ile +2,

Kalaycı (2015) ise daha geniş bir aralık olan −3 ile +3 olarak kabul etmektedir.

Araştırmada elde edilen çarpıklık ve basıklık değerlerinin bu sınırlar içinde olması, verilerin normallik varsayımını karşıladığını göstermektedir. Ayrıca, Merkezi Limit Teoremi'ne göre, sosyal bilimlerde örneklem büyüklüğü 400'den büyük (N > 400) olduğunda, normallik varsayımının sağlandığı kabul edilmektedir. Bu bağlamda, araştırmanın 451 kişilik örneklemi, normallik varsayımını destekleyen yeterli bir büyüklüğe sahiptir (Karasar, 2012: 102-103).

Sonuç olarak, verilerin normallik varsayımını karşıladığı kabul edilerek, araştırmanın sonraki aşamalarında t-testi, ANOVA ve korelasyon analizleri normallik varsayımı doğrultusunda gerçekleştirilmiştir.

Tablo 3. Doğrulayıcı Faktör Analizi

Madde	Yol	Faktörler	β0	β1	S.E.	C.R.	P
Giz1	<---	Gizlilik	0,573	1			
Giz2	<---	Gizlilik	0,785	1,303	0,13	10,06	***
Giz3	<---	Gizlilik	0,59	1,112	0,123	9,018	***
Kont5	<---	Kontrol/sahiplik	0,537	1			
Kont4	<---	Kontrol/sahiplik	0,688	1,181	0,114	10,339	***
Kont3	<---	Kontrol/sahiplik	0,64	1,172	0,118	9,907	***
Kont2	<---	Kontrol/sahiplik	0,839	1,375	0,121	11,386	***
But4	<---	Bütünlük	0,453	1			
But3	<---	Bütünlük	0,165	0,377	0,139	2,706	0,007
But2	<---	Bütünlük	0,698	1,49	0,231	6,456	***
But1	<---	Bütünlük	0,568	1,178	0,182	6,463	***
Kont1	<---	Kontrol/sahiplik	0,792	1,312	0,118	11,121	***
Ger5	<---	Gerçeklik	0,757	1			
Ger4	<---	Gerçeklik	0,794	1,034	0,065	15,798	***
Ger3	<---	Gerçeklik	0,753	1,078	0,071	15,075	***
Ger2	<---	Gerçeklik	0,588	0,775	0,066	11,748	***
Ger1	<---	Gerçeklik	0,578	0,76	0,066	11,545	***
Er1	<---	Erişilebilirlik	0,798	1			
Er2	<---	Erişilebilirlik	0,944	1,21	0,099	12,216	***
Er3	<---	Erişilebilirlik	0,381	0,452	0,057	7,898	***
Er4	<---	Erişilebilirlik	0,169	0,202	0,059	3,432	***
Fay1	<---	Fayda	0,6	1			
Fay2	<---	Fayda	0,717	1,215	0,141	8,606	***
Fay3	<---	Fayda	0,621	0,96	0,112	8,577	***

β0(Standardize değerler)

β1(Standardize olmayan değerler)

Tablo 3'te doğrulayıcı Faktör Analizi (DFA) sonuçları, modelin genel olarak kabul edilebilir bir uyum düzeyine sahip olduğunu göstermektedir. Analiz sonuçlarında Ki-kare / Serbestlik Derecesi Oranı 2,136 olarak hesaplanmıştır. Bu değer, modelin gözlemlenen veri ile kuramsal model arasındaki uyumunun iyi olduğunu ifade etmektedir.

Modelin genel uyumunu değerlendiren Yaklaşımın Ortalama Kök Hata Kareleri (RMSEA) değeri 0,050 bulunmuştur. Bu değer, modelin popülasyon düzeyinde mükemmel uyum kriterini karşıladığını göstermektedir. Ayrıca, Uyum İyiliği İndeksi (GFI) 0,915 ve Karşılaştırmalı Uyum İndeksi (CFI) 0,918 olarak hesaplanmıştır. Bu değerler, modelin genel uyumunun kabul edilebilir düzeyde olduğunu ve kuramsal model ile gözlemlenen veri arasında yeterli bir uyum sağladığını ortaya koymaktadır.

Modelde yer alan faktörlerin, ilgili maddelerle olan ilişkileri incelendiğinde, maddelerin büyük çoğunluğunun faktör yüklerinin 0,5'in üzerinde olduğu gözlemlenmiştir. Faktör yükleri, maddelerin ilgili faktörleri ne kadar iyi temsil ettiğini göstermektedir ve genellikle 0,5 ve üzerindeki değerler yeterli kabul edilmektedir. Bununla birlikte, Bütünlük faktörüne ait But3 maddesi (0,165) ve Erişilebilirlik faktörüne ait Er4 maddesi (0,169) düşük faktör yüklerine sahiptir. Bu durum, bu maddelerin ilgili faktörleri temsil etme gücünün sınırlı olduğunu göstermektedir. Ancak, bu maddelerin modelin genel uyum istatistiklerini olumsuz etkilemediği ve teorik bağlamda anlamlı olduğu göz önüne alınarak analizde tutulmasına karar verilmiştir.

Analiz sürecinde, modifikasyon indeksleri incelenmiş, ancak teorik çerçevenin korunması amacıyla herhangi bir modifikasyon yapılmamıştır. Modelin mevcut haliyle genel uyum istatistiklerinin yeterli düzeyde olması, modifikasyona gerek olmadığını desteklemektedir.

Genel olarak, DFA sonuçları modelin geçerli ve güvenilir bir yapı sunduğunu göstermektedir. Modelin genel uyum istatistikleri ve faktör yükleri değerlendirildiğinde, elde edilen sonuçlar araştırma modelinin kuramsal çerçeveye uygun bir şekilde çalıştığını ortaya koymaktadır. Sonuçlar, modelin araştırma bağlamında uygun bir temel sunduğunu ve analizler için yeterli kabul edildiğini göstermektedir.

Tablo 4. Korelasyon Analizi

	Gizlilik	Kontrol/Sahiplik	Bütünlük	Gerçeklik	Erişilebilirlik	Fayda
Gizlilik	1					
Kontrol/Sahiplik	0,516**	1				
Bütünlük	0,295**	0,312**	1			
Gerçeklik	0,295**	0,289**	0,098*	1		
Erişilebilirlik	0,165**	0,305**	0,081	0,278**	1	
Fayda	0,059	0,040	0,120*	-0,191**	0,010	1

Tablo 4'te sunulan korelasyon analizi sonuçlarına göre, değişkenler arasında anlamlı ilişkiler tespit edilmiştir. Gizlilik ile diğer değişkenler arasında pozitif ve anlamlı ilişkiler görülmüştür. Özellikle gizlilik ile kontrol/sahiplik arasındaki ilişki ($r = 0.516$, $p < 0.001$) pozitif ve güçlüdür. Gizlilik ile bütünlük ($r = 0.295$, $p < 0.001$) ve gerçeklik ($r = 0.295$, $p < 0.001$) arasında orta düzeyde pozitif ilişkiler bulunurken, erişilebilirlik ile gizlilik ($r = 0.165$, $p < 0.001$) zayıf bir ilişki göstermektedir. Gizlilik ile fayda ($r = 0.059$, $p = 0.213$) arasındaki ilişki ise istatistiksel olarak anlamlı değildir.

Kontrol/Sahiplik ile erişilebilirlik (r = 0.305, p < 0.001) ve bütünlük (r = 0.312, p < 0.001) arasında orta düzeyde pozitif ilişkiler gözlenmiştir. Benzer şekilde, gerçeklik ile kontrol/sahiplik (r = 0.289, p < 0.001) pozitif ve anlamlıdır. Ancak, kontrol/sahiplik ile fayda (r = 0.040, p = 0.393) arasında anlamlı bir ilişki bulunmamıştır.

Gerçeklik ile erişilebilirlik (r = 0.278, p < 0.001) orta düzeyde pozitif, gerçeklik ile fayda (r = −0.191, p < 0.001) negatif ve anlamlı bir ilişki göstermiştir. Bu, gerçeklik algısının artmasının fayda algısını azaltabileceğini düşündürmektedir. Bütünlük ile gerçeklik (r = 0.098, p = 0.038) ve fayda (r = 0.120, p = 0.011) zayıf ancak anlamlı ilişkilere sahiptir. Erişilebilirlik ile bütünlük (r = 0.081, p = 0.085) arasında anlamlı bir ilişki tespit edilmemiştir.

Genel olarak, gizlilik, kontrol/sahiplik, bütünlük ve gerçeklik değişkenlerinin birbiriyle anlamlı ilişkiler içinde olduğu görülmektedir. Ancak, fayda değişkeninin diğer değişkenlerle olan ilişkileri zayıf veya istatistiksel olarak anlamsızdır. Bu durum, fayda algısının araştırma bağlamında farklı faktörlerden etkilenebileceğini göstermektedir.

4. Bulgular

Siber Güvenliğin Cinsiyete Göre Farkındalık Seviyesinin Ölçülmesi

Çalışanların siber güvenlik farkındalık düzeylerinin cinsiyete göre farklılaşıp farklılaşmadığını incelemek amacıyla bağımsız örneklem t-testi yapılmış ve sonuçlar aşağıdaki tabloda gösterilmiştir:

Tablo 5. Cinsiyete Göre Genel Siber Güvenlik Farkındalığı T-Testi Sonuçları

Cinsiyet	**N**	**Ort.**	**S.S.**	**t**	**P**
Kadın	127	3.7920	0.34100	0.775	0.439
Erkek	324	3.7607	0.48186		

Tablo 5'te sunulan bağımsız gruplar t-testi sonuçlarına göre, cinsiyetin genel siber güvenlik farkındalığı üzerinde istatistiksel olarak anlamlı bir etkisi bulunmamıştır (t = 0.775, p = 0.439). Kadın katılımcıların ortalama puanları (Ort. = 3.79, S.S. = 0.34), erkek katılımcıların ortalama puanlarından (Ort. = 3.76, S.S. = 0.48) biraz daha yüksek olmasına rağmen bu fark istatistiksel olarak anlamlı değildir.

Bu sonuç, cinsiyetin siber güvenlik farkındalığı üzerinde belirgin bir etkisi olmadığını göstermektedir. Kadınlar ile erkekler arasında farkındalık düzeyleri benzer olup, cinsiyet değişkeni siber güvenlik farkındalığını anlamlı şekilde etkileyen bir faktör olarak değerlendirilememektedir.

Tablo 6. Cinsiyete Göre Alt Boyutlar T-Testi Sonuçları

	Cinsiyet	**N**	**Ort.**	**S.S.**	**t**	**P**
Gizlilik	Kadın	127	4.1339	0.65769	-1.268	0.205
	Erkek	324	4.0350	0.77598		
Kontrol/Sahiplik	Kadın	127	4.2094	0.59674	-0.481	0.631
	Erkek	324	4.2451	0.74606		
Bütünlük	Kadın	127	3.8858	0.58989	-0.320	0.749
	Erkek	324	3.9074	0.66386		
Gerçeklik	Kadın	127	3.8173	0.69466	2.347	0.020
	Erkek	324	3.6253	0.96834		
Erişilebilirlik	Kadın	127	3.2913	0.73582	-0.157	0.875
	Erkek	324	3.304	0.85556		
Fayda	Kadın	127	3.2546	0.78843	-0.685	0.494
	Erkek	324	3.3179	0.91772		

Tablo 6'da sunulan bağımsız gruplar t-testi sonuçlarına göre, cinsiyetin siber güvenlik farkındalığının alt boyutlarının çoğu üzerinde anlamlı bir etkisi bulunmamış, ancak Gerçeklik boyutunda istatistiksel olarak

anlamlı bir fark tespit edilmiştir (t = 2.347, p = 0.020). Kadın katılımcıların Gerçeklik farkındalığına ilişkin ortalama puanları (Ort. = 3.82, S.S. = 0.69), erkek katılımcıların ortalama puanlarından (Ort. = 3.63, S.S. = 0.97) anlamlı derecede daha yüksektir. Bu sonuç, kadınların çevrimiçi ortamda gerçeklik farkındalığına ilişkin algılarının erkeklere kıyasla daha yüksek olduğunu göstermektedir.

Diğer alt boyutlar olan Gizlilik, Kontrol/Sahiplik, Bütünlük, Erişilebilirlik ve Fayda değişkenleri açısından kadın ve erkek katılımcılar arasında istatistiksel olarak anlamlı bir fark tespit edilmemiştir (p > 0.05). Bu durum, cinsiyetin siber güvenlik farkındalığı üzerindeki etkisinin sınırlı olduğunu ve yalnızca Gerçeklik boyutunda anlamlı bir farklılık yarattığını ortaya koymaktadır.

Sonuç olarak, H1: Cinsiyet, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir.hipotezi desteklenmemektedir.

Siber Güvenliğin Yaşa Göre Farkındalık Seviyesinin Ölçülmesi

Araştırmaya katılan çalışanların yaş değişkeninin ANOVA testi sonuçları analiz edilmiştir.

Tablo 7. Yaş gruplarına Göre Genel ANOVA sonuçları

	Kareler Top.	S.d	Kareler Ort.	F	P
Gruplar arası	1,086	3	0,362	1,826	0,142
Gruplar içi	88,650	447	0,198		
Toplam	89,737	450			

Tablo 7'de sunulan tek yönlü ANOVA analizi sonuçlarına göre, yaş grupları arasında genel siber güvenlik farkındalığı skorları açısından istatistiksel olarak anlamlı bir fark bulunmamıştır (F = 1.826, p = 0.142). Gruplar arasındaki varyasyon toplamı 1.086, ortalama kare değeri ise 0.362 olarak hesaplanmıştır. Gruplar içindeki varyasyon toplamı 88.650, ortalama kare değeri ise 0.198'dir.p değeri (p = 0.142) 0.05'ten büyük olduğu için, yaş grupları arasında genel farkındalık düzeyleri açısından anlamlı bir fark olmadığı sonucuna varılmıştır. Bu bulgu, yaş değişkeninin genel siber güvenlik farkındalığı üzerinde belirgin bir etkisi olmadığını ve farklı yaş gruplarının farkındalık düzeylerinin büyük ölçüde benzer olduğunu göstermektedir.

Tablo 8. Yaş grupları Alt Boyutlara göre ANOVA sonuçları

		Kareler Top.	S.d	Kareler Ort.	F	P
Gizlilik	Gruplar arası	5,153	3	1,718	3,137	0,025
	Gruplar içi	244,733	447	0,548		
	Toplam	249,887	450			
Kontrol/Sahiplik	Gruplar arası	3,073	3	1,024	2,066	0,104
	Gruplar içi	221,693	447	0,496		
	Toplam	224,766	450			
Bütünlük	Gruplar arası	2,005	3	0,668	1,621	0,184
	Gruplar içi	184,230	447	0,412		
	Toplam	186,234	450			
Gerçeklik	Gruplar arası	2,479	3	0,826	1,013	0,387
	Gruplar içi	364,559	447	0,816		
	Toplam	367,038	450			
Erişilebilirlik	Gruplar arası	2,545	3	0,848	1,255	0,289
	Gruplar içi	302,120	447	0,676		
	Toplam	304,665	450			
Fayda	Gruplar arası	1,013	3	0,338	0,432	0,731
	Gruplar içi	349,711	447	0,782		
	Toplam	350,723	450			

Tablo 8'de sunulan tek yönlü ANOVA analizi sonuçlarına göre, yaş gruplarının siber güvenlik farkındalığının alt boyutları üzerindeki etkisi incelenmiştir. Analiz sonucunda yalnızca Gizlilik boyutunda yaş grupları arasında istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (F = 3.137, p = 0.025). Bu bulgu, yaşın gizlilik farkındalığı üzerinde etkili bir değişken olabileceğini göstermektedir.

Diğer alt boyutlar olan Kontrol/Sahiplik, Bütünlük, Gerçeklik, Erişilebilirlik ve Fayda açısından yaş grupları arasında anlamlı bir fark bulunmamıştır ($p > 0.05$). Bu durum, yaş değişkeninin genel siber güvenlik farkındalığı üzerindeki etkisinin sınırlı olduğunu, ancak belirli bir boyutta (Gizlilik) farklılık yaratabileceğini ortaya koymaktadır.

Post-hoc testi sonuçlarına göre, Gizlilik boyutunda yaş grupları arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($p > 0.05$). ANOVA analizinde anlamlılık tespit edilmesine rağmen, post-hoc test sonuçları farklılıkların belirgin olmadığını göstermektedir. Bu durum, farkların gruplar arasında homojen dağılabileceğini veya farkların küçük olduğunu işaret edebilir.

Elde edilen bu bulgulara göre, "H2: Yaş, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir." hipotezi desteklenmemektedir.

Siber Güvenliğin Eğitim durumuna Göre Farkındalık Seviyesinin Ölçülmesi

Tablo 9. Eğitim Durumuna göre genel ANOVA sonuçları

	Kareler Top.	S.d	Kareler Top.	F	P
Gruplar arası	2,294	5	0,459	2,335	0,041
Gruplar içi	87,442	445	0,196		
Toplam	89,737	450			

Tablo 9'da sunulan ANOVA analizi sonuçlarına göre, eğitim düzeyi grupları arasında genel siber güvenlik farkındalığı açısından istatistiksel olarak anlamlı bir fark olduğu belirlenmiştir ($F = 2.335$, $p = 0.041$). Gruplar arası varyans (2.294) ile gruplar içi varyans (87.442) arasındaki oran, eğitim düzeyinin genel farkındalık üzerinde anlamlı bir etkisi olduğunu göstermektedir.

Post-hoc testi sonuçlarına göre, anlamlı fark yalnızca Ortaokul ve Ön lisans grupları arasında tespit edilmiştir ($p = 0.038$). Diğer eğitim düzeyleri arasında ise istatistiksel olarak anlamlı bir fark bulunmamıştır ($p > 0.05$).

Bu bulgular, eğitim düzeyinin siber güvenlik farkındalığını etkileyen sınırlı bir değişken olduğunu, farkındalık düzeylerinin özellikle belirli gruplar arasında farklılık gösterdiğini ortaya koymaktadır.

Tablo 10. Eğitim durumu Alt Boyutlara göre ANOVA sonuçları

		Kareler Top.	S.d	Kareler Ort.	F	P
Gizlilik	Gruplar arası	11,302	5	2,260	4,216	0,001
	Gruplar içi	238,585	445	0,536		
	Toplam	249,887	450			
Kontrol/Sahiplik	Gruplar arası	6,018	5	1,204	2,448	0,033
	Gruplar içi	218,749	445	0,492		
	Toplam	224,766	450			
Bütünlük	Gruplar arası	2,746	5	0,549	1,332	0,249
	Gruplar içi	183,488	445	0,412		
	Toplam	186,234	450			
Gerçeklik	Gruplar arası	4,202	5	0,840	1,031	0,399
	Gruplar içi	362,836	445	0,815		
	Toplam	367,038	450			
Erişilebilirlik	Gruplar arası	4,419	5	0,884	1,310	0,259
	Gruplar içi	300,246	445	0,675		
	Toplam	304,665	450			
Fayda	Gruplar arası	14,046	5	2,809	3,713	0,003
	Gruplar içi	336,677	445	0,757		
	Toplam	350,723	450			

Tablo 10'da sunulan analiz sonuçlarına göre, eğitim düzeyinin siber güvenlik farkındalığı üzerinde kısmi olarak anlamlı bir etkisi olduğu belirlenmiştir. ANOVA sonuçlarına göre, Gizlilik, Kontrol/Sahiplik ve Fayda boyutlarında eğitim düzeyine göre anlamlı farklar tespit edilmiştir ($p < 0.05$). Ancak, Bütünlük, Gerçeklik ve Erişilebilirlik boyutlarında gruplar arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($p > 0.05$).

Post-hoc testi sonuçları, bu farkların detaylarını ortaya koymuştur. Gizlilik boyutunda, Ortaokul düzeyindeki katılımcıların farkındalık puanlarının Lise, Önlisans, Lisans ve Yüksek Lisans düzeylerine kıyasla anlamlı derecede daha düşük olduğu görülmüştür. Fayda boyutunda, Lise düzeyindeki katılımcıların puanlarının Lisans, Yüksek Lisans ve Doktora düzeylerine göre daha düşük olduğu tespit edilmiştir.

Kontrol/Sahiplik boyutunda ANOVA sonucu anlamlılık tespit edilmesine rağmen, post-hoc test sonuçları gruplar arasında belirgin bir fark göstermemiştir.

Sonuç olarak, eğitim düzeyi siber güvenlik farkındalığı üzerinde özellikle Gizlilik ve Fayda boyutlarında etkili bir değişken olarak görülmüştür. Diğer boyutlarda ise anlamlı bir fark bulunmamaktadır. Bu durum, eğitim düzeyinin belirli boyutlarda farkındalığı etkileyen, ancak genel olarak sınırlı bir etkisi olduğunu göstermektedir.

Elde edilen bu sonuçlara göre, "H3: Eğitim düzeyi, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir." hipotezi desteklenmemektedir.

Siber Güvenliğin Çalışılan Sektöre Göre Farkındalık Seviyesinin Ölçülmesi

Tablo 11. Çalışılan Sektöre Göre genel ANOVA sonuçları

	Kareler Top.	S.d	Kareler Ort.	F	P
Gruplar arası	0,283	2	0,142	0,709	0,492
Gruplar içi	89,453	448	0,200		
Toplam	89,737	450			

Tablo 11'de sunulan ANOVA analizi sonuçlarına göre, çalışılan sektör grupları arasında genel siber güvenlik farkındalığı açısından istatistiksel olarak anlamlı bir fark bulunmamıştır ($F = 0.709$, $p = 0.492$). p-değeri ($p = 0.492$) 0.05 anlamlılık düzeyinden büyük olduğu için, sektör grupları arasında farkındalık düzeyleri açısından anlamlı bir farklılık olmadığı sonucuna ulaşılmıştır.

Bu bulgu, çalışılan sektörün siber güvenlik farkındalığı üzerinde etkili bir değişken olmadığını ve gruplar arasında fark yaratmadığını göstermektedir.

Tablo 12. Çalışılan Sektöre göre Alt boyutlar ANOVA sonuçları

		Kareler Top.	S.d	Kareler Ort.	F	P
Gizlilik	Gruplar arası	0,292	2	0,146	0,262	0,770
	Gruplar içi	249,595	448	0,557		
	Toplam	249,887	450			
Kontrol/Sahiplik	Gruplar arası	2,145	2	1,072	2,158	0,117
	Gruplar içi	222,622	448	0,497		
	Toplam	224,766	450			
Bütünlük	Gruplar arası	1,702	2	0,851	2,066	0,128
	Gruplar içi	184,533	448	0,412		
	Toplam	186,234	450			
Gerçeklik	Gruplar arası	2,994	2	1,497	1,842	0,160
	Gruplar içi	364,044	448	0,813		
	Toplam	367,038	450			
Erişilebilirlik	Gruplar arası	2,442	2	1,221	1,810	0,165
	Gruplar içi	302,223	448	0,675		
	Toplam	304,665	450			
Fayda	Gruplar arası	1,020	2	0,510	0,653	0,521
	Gruplar içi	349,704	448	0,781		
	Toplam	350,723	450			

Tablo 12'de sunulan analiz sonuçlarına göre, çalışılan sektörün siber güvenlik farkındalığı üzerinde anlamlı bir etkisi bulunmamıştır ($p > 0.05$). Gizlilik, Kontrol/Sahiplik, Bütünlük, Gerçeklik, Erişilebilirlik ve Fayda boyutlarında sektörler arasında istatistiksel olarak anlamlı bir farklılık tespit edilmemiştir.

Bu bulgular, çalışılan sektörün siber güvenlik farkındalığını etkileyen bir değişken olmadığını göstermektedir. Dolayısıyla, "H4: Çalışılan sektör, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir." hipotezi desteklenmemektedir.

5. Sonuç ve Tartışma

Dijital çağda bireylerin ve kurumların bilgi güvenliğini sağlamada siber güvenlik farkındalığı kritik öneme sahiptir. Bu çalışmada, cinsiyet, yaş, eğitim seviyesi ve çalışılan sektör gibi demografik faktörlerin siber güvenlik farkındalığı üzerindeki etkileri incelenmiş ve farkındalığı artırmaya yönelik öneriler geliştirilmiştir.

Araştırma sonuçları, demografik faktörlerin genel farkındalık düzeyinde belirleyici olmadığını, ancak alt boyutlarda bazı farklılıklar yarattığını göstermektedir. Cinsiyet açısından, kadın ve erkek katılımcılar arasında genel fark bulunmamakla birlikte, gerçeklik boyutunda kadınların farkındalık düzeyinin erkeklere göre daha yüksek olduğu tespit edilmiştir. Bu sonucun Cengiz Gündüz Alp (2021), çalışması ile uyumlu olduğu görülmüştür. Yaş değişkeninin genel farkındalık düzeyi üzerinde anlamlı bir etkisi bulunmamış, ancak eğitim materyallerinin farklı yaş gruplarının öğrenme stillerine göre düzenlenmesinin faydalı olacağı görülmüştür. Aloul (2017), çalışmasında olduğu gibi bu çalışmada da eğitim seviyesi açısından farkındalığın formal eğitimle sınırlı olmadığı, sürekli eğitim ve bireysel farkındalık artırma çabalarının önem taşıdığı belirlenmiştir. Yine literatürdeki Kruger ve Kearney'in (2012) ile Jeong ve vd. (2022) çalışmalarında olduğu gibi çalışılan sektör faktörünün de farkındalık üzerinde belirgin bir etkisi olmadığı, ancak sektörlere özgü tehditlere yönelik eğitim programlarının faydalı olabileceği ifade edilmiştir.

Bu bulgular doğrultusunda aşağıdaki öneriler geliştirilmiştir:

Cinsiyete özel eğitim programları: Gerçeklik boyutundaki farkındalık düzeyi dikkate alınarak, kadınların bu alandaki duyarlılığı korunmalı ve erkek çalışanların bu boyuttaki farkındalıkları artırılmalıdır.

Genel farkındalık programları: Yaş, eğitim ve sektör ayrımı yapmaksızın tüm çalışanları kapsayacak şekilde kolay erişilebilir ve anlaşılır eğitimler tasarlanmalıdır.

Süreklilik ve güncelleme: Farkındalık eğitimleri düzenli aralıklarla tekrarlanmalı ve güncel tehditlere uygun olarak yenilenmelidir.

Sektörel risklere yönelik eğitimler: Özellikle hassas veriyle çalışan sektörler için risk odaklı modüller geliştirilmelidir.

Araştırmanın bulguları, genel siber güvenlik farkındalığının demografik faktörlerden bağımsız olarak artırılabileceğini göstermektedir. Ancak eğitimlerin sürekli güncellenmesi ve bireylerin ihtiyaçlarına göre özelleştirilmesi, daha etkili sonuçlar sağlayacaktır.

Araştırma sonuçları ve sınırlılıkları dikkate alınarak gelecekte yapılacak olası araştırmalar için bazı önerilerde bulunulmaktadır. Kendilerini daima yenilemek durumunda olan işletmeler ile kendilerini sürekli olarak geliştirmek zorunda olan işgörenlerin algı ve davranışları sürekli olarak değişebilmektedir. Dolayısıyla işgörenlerinsiber güvanlik farkındalık düzeylerinin belirli periyotlarda ölçülmesi faydalı olacaktır. Bu araştırma Van İli ile sınırlandırılmıştır. İleride yapılacağı öngörülenaraştırmalar farklı il ve farklı sektörlerde değişik veri toplama ve analiz yöntemleri ile gerçekleştirilebilir.

Kaynaklar

Aloul, F. (2017). Socialengineeringawarenessamonguniversitystudents. *International Journal of Cybersecurity*, 5(2), 22-29.

Arpaci, I., &Sevinç, K. (2022). Development of thecybersecurityscale (CS-S): Evidence of validityandreliability. Information Development, 38(2), 218-226. doi:10.1177/0266666921997512.

Aslay, F. (2017). *Türkiye'de Siber Güvenlik Tehditleri ve Farkındalık Çalışmaları*. STM ve Fortinet Raporları.

Check Point Research. (2022). *Cyber Attack Trends: 2022 Annual Report*.

CybersecurityVentures. (2021). *2021 Cybersecurity Market Report*.

ENISA. (2023). *ThreatLandscape Report 2023*. EuropeanUnionAgencyforCybersecurity.

George, D. Mallery, P. (2002) *SPSS for Windows Step by Step: A Simple Guide and Reference, 11.0 Update.* 4th Edition, Boston: Allyn& Bacon.

Gündüz Alp, C. (2021). *Türkiye'de Üniversitelerde Dijital Veri Güvenliği Farkındalığı*. İstanbul: Bilgi Üniversitesi Yayınları.

Jeong, H., Kim, S., & Park, J. (2022). *CulturalFactors in CybersecurityInvestmentDecisions*. *Journal of CybersecurityStudies*, 15(4), 25-42.

Jeong, J., Grobler, M., & C., M. A. P. (2022). Simplifyingcybersecuritymaturitymodelsthroughnationalculture: A fuzzylogicapproach. *Proceedings of theAnnual Hawaii International Conference on SystemSciences*, https://doi.org/10.24251/hicss.2022.662

Kalaycı, Ş. (2016). *SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri.* Ankara:

Karasar, N. (2012). *Bilimsel Araştırma Yöntemi.* Ankara: Nobel Yayınları.

Kınay, H., Sözcü, Ö. F., Taşkın, E., ve İpek, Ġ. (2014). Bilgi güvenliği farkındalığı ölçeğinin ilk bulguları. *8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu'nda sunulan bildiri.*

Kruger, H. A., &Kearney, W. D. (2012). A prototypeforassessinginformationsecurityawareness. *Computers& Security*, 25(4), 289-296.

Kumar, R., Lin, D., & Zhao, Y. (2023). *ExplainableArtificialIntelligence in CyberThreatHunting*. *Computers& Security*, 45, 85-98.

Liu (2003). Developing a Scaletomeasuretheınteractivity of websites, Journal of AdvertisingResearch, June, 207–217.

Nunnally, J.C (1978), Psychometrictheory ,NewYork: McGraw Hill.

PonemonInstitute. (2023). *Cost of a Data Breach Report*. IBM Security.

Puhakainen, P., &Siponen, M. (2020). Improvingemployees' cybersecurityawarenessthroughstorytellingandgamification. *Journal of Information Systems Security*, 12(4), 145-159.

Schwab, Klaus. (2016). Dördüncü Sanayi Devrimi. (Çeviren: Zülfü Dicleli). İstanbul: Optimist Yayınları.

STM ve Fortinet (2016). Türkiye'de fidye yazılım ve bankacılık saldırıları. *STM Siber Güvenlik Raporu 2016*.

Tabachnick, B. G. &Fidell, L. S. (2015). *Çok Değişkenli İstatistiklerin Kullanımı.* (Çev. Ed. Mustafa Baloğlu). Ankara: Nobel Akademik Yayıncılık.

Tayvan Milli Eğitim Bakanlığı (2015). Internet SafetyAwarenessforTeachers (TAIS) Project. *Ministry of Education Report*, Taipei.

Whitman, M. E., &Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.