ARAŞTIRMA

Geliş Tarihi: 07 Mayıs 2025
Kabul Tarihi: 01 Aralık 2025

ÖĞRETMENLERİN BRANŞ BAZINDA SİBER GÜVENLİK FARKINDALIK DÜZEYLERİNİN BELİRLENMESİ

Determining Teachers' Cybersecurity Awareness Levels by Subject Area

DOI: 10.58307/kaytek.1694363

Dr. Öğretim Üyesi Mustafa COŞAR* / Murat ERDOĞAN

Özet

Bilişim Teknolojileri (BT) ve dijitalleşme, bireysel yaşamları dönüştürmenin ötesinde Kamu Yönetimi süreçlerini ve Dijital Devlet dönüşümünü hızlandırmaktadır. Bu dönüşümde eğitim sektörü, öğrenci ve personel bilgileri gibi büyük ölçekli hassas verileri yönetmesi nedeniyle siber güvenliğin kritik bir bileşeni haline gelmiştir. Dolayısıyla öğretmenlerin siber güvenlik farkındalık düzeyi, yalnızca bireysel bir korunma meselesi değil; kamusal bilgi güvenliği, dijital risk yönetimi ve hizmet kalitesinin sürdürülebilirliği açısından stratejik bir gerekliliktir. Bu çalışmada, Çorum ilindeki Milli Eğitim okullarında görev yapan farklı branşlardaki öğretmenlerin kişisel siber güvenlik farkındalık düzeylerinin belirlenmesi ve bu kapsamda politika yapıcılara yönelik öneriler geliştirilmesi amaçlanmıştır. Toplam 96 katılımcıdan elde edilen veriler öğretmenlerin BT kullanım düzeyleri ve güvenlik davranışlarını değerlendirmek üzere analiz edilmiştir. Branşlar arası farkları incelemek amacıyla Tek Yönlü Varyans Analizi uygulanmıştır. Analiz sonucunda farkındalık düzeylerinin genel olarak üst-orta seviyede olduğu; BT branşı öğretmenlerinin en yüksek farkındalığa sahip olduğu (%84,75), onları Sosyal Bilimler (%76,80) ve Fen Bilimleri (%73,52) branşlarının izlediği belirlenmiştir. Elde edilen bulgular kamu çalışanlarının dijital yetkinlikleri ve MEB'in güvenlik politikaları bağlamında tartışılmış; eğitim kurumlarında siber güvenlik farkındalığının artırılmasına yönelik uygulamaya dönük öneriler sunulmuştur.

Anahtar Kelimeler: *Dijitalleşme, Siber dünya, Siber güvenlik, Bilgi güvenliği, Farkındalık düzeyi*

Abstract

Information Technologies (IT) and digitalization are accelerating the transformation of Public Administration processes and the Digital State beyond their impact on individual lifestyles. Within this transformation, the education sector—one of the most critical components of public service—manages large volumes of sensitive data, including student and personnel records. Therefore, the cyber security awareness of teachers as public employees is not only an individual protection requirement but also a strategic necessity for ensuring public information security, digital risk management, and the continuity of service quality. As the first line of defense against increasing cyber threats, cyber security awareness also places upon teachers the responsibility of serving as digital role models for students and society. This study aims to measure the personal cyber security awareness levels of teachers from different branches working in the public schools of Çorum Province and to provide policy-oriented recommendations that may contribute to national cyber security strategies. Data collected from 96 participants were analyzed in detail, including teachers' IT usage habits and information security behaviors. Additionally, a One-Way Analysis of Variance was conducted to examine differences between branches. The results indicate that teachers' overall cyber security awareness levels are at an upper-intermediate level; the IT branch demonstrates the highest awareness (84.75%), followed by the Social Sciences (76.80%) and Science (73.52%) branches. These findings are discussed in relation to the digital competencies of public-sector employees and the cyber security policies of the MEB, and several specific policy recommendations are presented for decision-makers.

Keywords: *Digitalization, Cyber world, Cyber security, Information security, Awareness level*

Dr. Öğretim Üyesi Mustafa COŞAR, Hitit Üniversitesi, Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi, mustafacosar@gmail.com, ORCID: 0000-0001-6482-4592
Murat ERDOĞAN, Hitit Üniversitesi, Lisansüstü Eğitim Enstitüsü, Adli Bilimler A.B.D. Yüksek Lisans Öğrencisi, muraterdogan41@gmail.com ORCID: 0009-0009-9259-6289

GİRİŞ

Bilişim Teknolojilerinin (BT) hızla gelişmesi ile birlikte zaman ve mekân gibi geleneksel engeller ortadan kalkmakta; bireyler, kurumlar ve devletler faaliyetlerini dijital ortamlara taşımaktadırlar. Özellikle bilgisayar, tablet ve telefon gibi elektronik cihazların küçülerek daha taşınabilir, bağlantı özelliklerinin artması ve daha akıllı hale gelmesi, bu dijitalleşme sürecini kamu hizmetleri de dahil olmak üzere hızlandırmaktadır. Datareport internet sitesinde yayınlanan rapora göre, Ocak 2023 itibarıyla dünya genelinde internet kullanıcı sayısının 5,16 milyara, aktif sosyal medya kullanıcı sayısının ise 4,76 milyara ulaştığı raporlanmaktadır (Kemp, 2023).

Siber dünyanın dijital yaşam koşulları, insanların iletişim kurmalarını, sosyalleşmelerini ve eğitimden iş yaşamına kadar pek çok faaliyetlerini dönüştürmektedir (Ünlü, 2018; Baz, 2018; Ryan vd., 2017). Bu yaygınlaşma, kamu yönetiminin de Dijital Devlet modeline geçişini zorunlu kılmıştır. Dijital Devlet yaklaşımı, vatandaşlara sunulan hizmetlerin güvenli, şeffaf ve kesintisiz dijital platformlar üzerinden yürütülmesini hedefler. Bu dönüşüm, kamu kurumlarını ve kamu çalışanlarını büyük hacimli hassas veriyi yönetme ve koruma yükümlülüğü ile karşı karşıya bırakmaktadır. OECD'nin Dijital Devlet Politikası Çerçevesi (OECD, 2020) ve OECD Skills Outlook raporları (OECD, 2019), kamu çalışanlarının dijital becerilerinin ve siber güvenlik farkındalığının dijital kamu hizmetlerinin sürdürülebilirliği için kritik öneme sahip olduğunu vurgulamaktadır. Birleşmiş Milletler'in E-Devlet Raporu (United Nations, 2022) da kamu hizmetlerinin dijitalleşmesiyle birlikte kamu personelinin dijital yetkinliklerinin stratejik bir gereklilik haline geldiğini belirtmektedir. Dünya Bankası'nın "Digital Government Transformation: User-Centric Public Services" raporu (World Bank, 2020) ise dijital devlet dönüşümünde kullanıcı odaklı hizmet tasarımının ve dijital kamu çalışanlarının yetkinliklerinin merkezi bir unsur olduğunu ifade ederek bu yaklaşımı pekiştirmektedir.

Dijitalleşmenin yaygınlaşması, faydalı kullanımın yanı sıra zararlı ve tehlikeli kullanım biçimlerini de artırmaktadır. Özellikle kamu kurumlarına ve bireylere yönelik siber tehditlerin son yıllarda hızla yükseldiği hem ulusal hem de uluslararası raporlarda açıkça görülmektedir. ENISA'nın 2021 ve 2023 Tehdit Manzarası raporları, fidye yazılımları, kimlik avı, DDoS saldırıları ve tedarik zinciri zafiyetlerinin küresel ölçekte dramatik biçimde arttığını ortaya koymaktadır (ENISA, 2021; ENISA, 2023). BT sektöründen TrendMicro'nun 2023 Siber Risk Raporu da bu bulguları desteklemekte; 2023'ün ilk yarısında kaydedilen 605 bin siber tehdidin en çok devlet kurumları (145,9 bin) ve eğitim

sektörünü (101,4 bin) hedef aldığını göstermektedir. Raporda, Türkiye'nin fidye saldırılarında 14.209 olay ile ilk sırada yer alması, kamu güvenliği ve ulusal siber güvenlik stratejileri açısından dikkat edilmesi gereken önemli bir risk düzeyine işaret etmektedir.

BT kullanıcılarının siber güvenliğini tehdit eden başlıca riskler; sistem açıkları, kullanıcı ihmalleri ve kullanım hatalarıdır. Tekerek (2008)'e göre siber tehditler, bireylerin yeterli bilince, bilgiye, eğitime ve farkındalığa sahip olmadan teknoloji kullanması ya da kötü niyetli faaliyetler sonucu ortaya çıkmaktadır. Bu nedenle kamusal bilgi güvenliğini sağlamanın ilk adımı, kamu personelinin farkındalığının artırılması ve düzenli eğitimlerle desteklenmesidir.

Öğretmenler, bir yandan MEB dijital sistemleri üzerinden hassas öğrenci verilerini yöneten kamu görevlileri, diğer yandan öğrencilere güvenli internet davranışlarını öğreten dijital rol modellerdir. Ancak dünya genelindeki araştırmalar, öğretmenlerin siber güvenlik konusunda öğrencileri yeterince hazırlayamadığını göstermektedir. ABD Ulusal Bilgi Güvenliği Raporu da öğretmenlerin öğrencilere temel internet kullanım becerilerini sınırlı düzeyde öğrettiklerini belirtmektedir (Tekerek ve Tekerek, 2013). Bu durum, öğretmenlerin farkındalık ve dijital yetkinlik düzeylerinin önemini ortaya koymaktadır.

Literatürde toplumun farklı kesimlerinin siber güvenlik farkındalıklarını ölçen araştırmalar bulunsa da (Avcı ve Oruç, 2020; Uzun ve Coşar, 2022; Aksoğan ve Atıcı, 2023; Canoğulları, 2021), branş bazında derinlemesine karşılaştırma yapılması ve bu bulguların kamu yönetimi politikaları çerçevesinde tartışılması eksiktir. Örneğin, Canoğulları (2021) araştırmasında öğretmenlerin genel bilgi güvenliği farkındalık düzeylerini orta düzeyin hemen üzerinde bulmuştur. Türkiye Cumhuriyeti'nin BT alanında gelişmiş bir toplum inşa etme hedefinde, öncelikle bu dönüşümün merkezinde yer alan öğretmenlerin siber güvenlik farkındalığının doğru ve güncel bir şekilde belirlenmesi zorunludur.

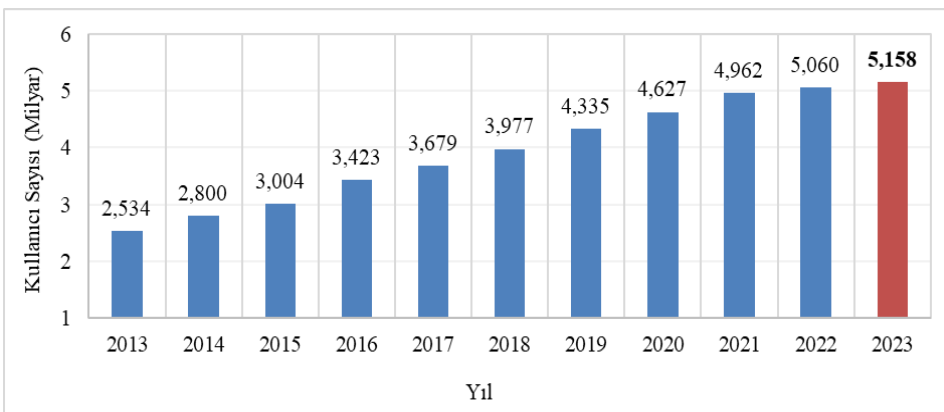
Bu çalışma, söz konusu boşluğu doldurmayı hedefleyerek öğretmenlerin siber güvenlik farkındalık düzeylerini belirlemeyi amaçlamaktadır. Elde edilen bulgularla öğretmenlerin BT kullanımı, e-posta, sosyal medya ve diğer dijital uygulamalara ilişkin tutumları değerlendirilmiş; sonuçlar Ulusal Siber Güvenlik Stratejisi ve MEB'in dijital güvenlik politikaları kapsamında ele alınarak kamu yönetimi ve teknoloji yönetişimi alanına katkı sunulmuştur.

KAVRAMSAL ÇERÇEVE

Siber Güvenlik ve Dijitalleşmenin Etkisi

Siber dünya her geçen gün büyüdükçe dijital yaşamın bileşenleri de çok çeşitli uygulamalar üretmektedir. İnternet, servis sağlayıcılar, sunucular ve bağlantı türleri; hız, kapasite ve erişim yöntemleri açısından gelişerek dijital yaşamı desteklemektedir. Siber dünya; bağlantı altyapıları, donanımlar, yazılımlar, kullanıcılar ve uygulamalar gibi bileşenlerden oluşmakta olup her biri kendine özgü mimari ve işleyişe sahiptir (Coşar, 2022). Bu nedenle, her bileşenin sürdürülebilir şekilde çalışması için belirlenen kurallar ve kullanım politikaları bulunmakta, güvenlik bu politikaların en kritik unsurlarından biri olmaktadır.

BT'nin son 20 yıldaki gelişimi, dijital yaşamın büyük ölçüde ağlar ve internet üzerinden sunulduğunu göstermektedir. Dijital dünyanın bir bileşeni olan insanlar da kullanıcı kimliğiyle bu ekosistemde yer almaktadır. Şekil 1'de, internet kullanıcılarının 2013'te 2,53 milyardan 2023 başında 5,16 milyara yükselerek iki katından fazla arttığı görülmektedir.

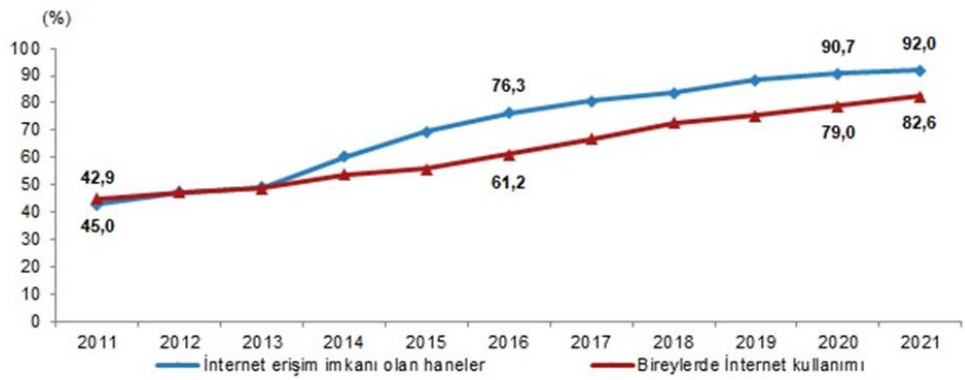


Şekil 1. 2013-2023 Yılları Arası İnternet Kullanıcı Sayıları (Kemp, 2023)

Grafikte ayrıca, internet kullanıcılarının son bir yılda yaklaşık 100 milyon arttığını ve bunun %2'lik bir büyümeyle sonuçlandığını gösterilmektedir. On yıllık bir perspektif ile bakıldığında internet kullanıcı sayısının her yıl düzenli bir artış sergileyerek ilerlediği görülmektedir. Bunun yanında, sosyal medya uygulamaları kullanıcılarının son on yıllık dönemde internet kullanıcılarından daha hızlı artış gösterdiği kaydedilmiştir. Aynı raporda, 2023 yılı itibariyle sosyal medya kullanıcısı sayısının 4,76 milyar olduğu belirtilmektedir. Bu

sayının 2013'de 1,72 milyar iken on yıllık bir zamanda 2,7 kattan daha fazla arttığı hesaplanabilir. Bu veriler ışığında, sosyal medya kullanıcı sayısının son bir yılda yaklaşık 140 milyona ulaştığı görülmektedir.

TÜİK'in yayınlamış olduğu 2021 yılı Hanehalkı BT Kullanım Araştırması raporunda internete erişim olanağı olan hane oranı 2021 yılında %92,0 olmuştur. Bu oranın bir önceki yıl değeri ise %90,72'dir. Aynı araştırmada, bireysel internet kullanımı oranı 2020 yılında %79'ken 2021 yılında %82,6 çıkmıştır (TÜİK, 2022). Şekil 2'de özetlenmeye çalışılan araştırma sonuçlarına göre internet kullanımının bireylerde ve hanelerde her yıl belirli oranlarda arttığı görülmektedir.



Şekil 2. İnternet Erişim Olanağı Olan Haneler ve Bireylerin İnternet Kullanımı (TÜİK, 2022)

BT'nin iş ve özel yaşamda yaygınlaşması, bilgi güvenliği ve siber güvenlik risklerini de artırmaktadır. Eminağaoğlu ve Gökşen (2009), bilgi güvenliğini siber dünyadaki kişisel verilerin kaydı, iletimi ve paylaşımı süreçlerini içeren bir kavram olarak tanımlamaktadır. Risklerin tespiti, önlem alımı ve saldırılara karşı tepki geliştirme bilgi güvenliğinin temel adımlarıdır. Dijital verilerin hızla artması kötü niyetli kişilerin yetkisiz erişim girişimlerini teşvik etmekte; BT'deki hızlı değişim ise yeni güvenlik problemlerini beraberinde getirmektedir (Aldridge, Medina ve Ralphs, 2010). Check Point'in 2023 raporunda, yılın ilk yarısında 48 fidye yazılımının 2.200'den fazla mağdura ulaştığı ve ikinci çeyrekte haftalık saldırılarda %8 artış olduğu belirtilmiştir (Check Point, 2023).

Siber tehdit; dijital varlıklara, verilere, donanıma, yazılıma veya altyapıya izinsiz ve yetkisiz erişimdir. Aslay (2017), bu saldırıların planlı ve koordineli yürütüldüğünü vurgular. Açıklar ve zafiyetler genellikle kullanıcı ihmali, donanım-yazılım eksikleri veya uygulamalardaki bilinçli/bilinçsiz hatalardan kaynaklanmaktadır. Bu açıkları tespit eden saldırganlar oltalama, sızma,

dinleme ve sahte içerik oluşturma gibi birçok yöntemle tehdit oluşturabilmektedir.

Aydın ve Yükçü (2020), siber tehditlerin yalnızca kişisel verileri değil, devletlerin ve işletmelerin kritik kaynaklarını da hedef aldığını vurgulamaktadır. Günümüzde iletişim, enerji, sağlık, ulaştırma gibi kritik altyapılara yönelik saldırılar artmakta; askeri ve sivil kurumlara yönelik istihbarat amaçlı veri sızdırma girişimleri de yaygınlaşmaktadır. Güvenli bir dijital ortam için siber dünya bileşenlerinin gizlilik, bütünlük ve erişilebilirlik ilkeleriyle korunması gerekmektedir.

Dijital Devlet, Kamu Yönetiminde Bilgi Güvenliği ve Siber Risk Yönetimi

Dijitalleşme süreci yalnızca teknolojik bir dönüşüm değil, aynı zamanda kamu yönetiminde yapısal bir yeniden yapılanmayı da beraberinde getirmektedir. OECD'nin Dijital Devlet Politikası Çerçevesi (OECD, 2020), dijital devletin temel boyutlarını kullanıcı odaklılık, güvenilir veri yönetimi, dijital güvenlik ve kamu çalışanlarının dijital yetkinlikleri olarak tanımlamaktadır. OECD Skills Outlook (2019) raporu ise kamu çalışanlarının dijital ve siber güvenlik becerilerinin, dijital kamu hizmetlerinin sürdürülebilirliği için kritik olduğunu vurgulamaktadır. Birleşmiş Milletler E-Devlet Gelişmişlik Endeksi (United Nations, 2022) de kamu kurumlarının dijital kapasitesinin yalnızca teknik altyapıya değil, aynı zamanda kamu çalışanlarının bilgi güvenliği farkındalığına dayandığını belirtmektedir. Bu çerçeve, öğretmenler gibi kritik kamu personelinin siber güvenlik farkındalığının dijital devletin güvenliği ve kamu hizmeti kalitesi açısından stratejik önem taşıdığını göstermektedir.

Dijitalleşmenin hızlanmasıyla birlikte, kamu yönetimi kurumları da "Dijital Devlet" (E-Devlet) modeline geçişi zorunlu kılmaktadır. Dijital Devlet, kamu hizmetlerini etkin, şeffaf ve çevrimiçi olarak sunmayı hedeflerken, bu dönüşüm süreci beraberinde kamu sektöründe bilgi güvenliği risklerini de artırmaktadır. Kamu kurumları tarafından toplanan ve işlenen vatandaşlara ait hassas kişisel veriler, kritik kamu hizmetlerinin sürekliliği ve ulusal güvenlik açısından korunması gereken varlıklardır.

Kamusal Bilgi Güvenliği kavramı, kamu çalışanlarının, erişim yetkisi verilen her türlü veriyi görevlerini icra ederken gizlilik, bütünlük ve erişilebilirlik prensiplerine uygun olarak koruma sorumluluğunu ifade eder. Öğretmenler, MEB bünyesinde görev yapan kamu personeli olarak, öğrencilerin kişisel verileri, notları ve sağlık bilgileri gibi son derece hassas verileri yönetmekte ve bu nedenle bilgi güvenliği zincirinin kritik bir halkasını oluşturmaktadır. Bilgi güvenliği zincirindeki en zayıf halkanın genellikle teknoloji değil, insan faktörü

olduğu unutulmamalıdır.

Kamu Yönetiminde Siber Risk Yönetimi bağlamında, kurumların siber saldırılarla başa çıkma ve hizmet sürekliliğini sağlama stratejileri giderek daha kritik hale gelmektedir. Bu alandaki yeni teknolojiler ve yaklaşımlar, riskleri minimize etmeyi ve dijital güvenliği sistematik biçimde güçlendirmeyi hedefler. Örneğin, merkeziyetsiz, şeffaf ve değiştirilemez veri yapısı sunan Blok Zinciri teknolojisi; kamu sektöründe e-seçimler, tapu kayıtları ve kimlik yönetimi gibi alanlarda güvenilirliği artırma potansiyeline sahiptir (Coşar, 2025; Söylemez, Ay ve Ay, 2022). Yerel yönetimlerde Akıllı Kentlerden Blok Zinciri Kentlere geçiş ise dijital dönüşümün ve güvenliğin yerel düzeyde nasıl ele alınması gerektiğini göstermektedir (Söylemez ve Söylemez, 2024).

Bu teknolojilere ek olarak, yapay zekâ tabanlı tehdit tespit sistemleri büyük ölçekli verileri gerçek zamanlı analiz ederek anomali algılama, saldırı örüntülerini öğrenme ve otomatik risk sınıflandırması gibi önemli yetenekler sunmaktadır (Coşar, 2024). Bu sayede kurumların siber olay müdahale kapasitesi ve saldırı önleme süreçleri önemli ölçüde güçlenmektedir. Bununla birlikte, teknoloji tabanlı çözümler sistem ve altyapı güvenliğini artırsa da, kullanıcı düzeyindeki farkındalık kamu güvenliğini tehdit eden riskleri önlemede hâlâ ilk ve en önemli adım olmaya devam etmektedir.

Öğretmenlerin Kamusal Sorumluluğu ve Dijital Rol Model Olması

Öğretmenlerin siber güvenlik farkındalığı, yalnızca kendi kişisel ve mesleki güvenlikleri için değil, aynı zamanda taşıdıkları kamusal sorumluluk nedeniyle de büyük önem taşır. Bu roller şu şekilde açıklanabilir:

Kamusal Görev: Öğretmenler, kamu hizmetini dijital ortamda sunarken hassas veriyi korumak zorundadır. Bir öğretmenin siber ihmali sonucu oluşan veri ihlali, tüm kurumsal sistemi ve binlerce öğrenci/veli verisini tehlikeye atarak kamu zararına yol açabilir.

Dijital Rol Model: Öğretmenler, öğrencilere dijital vatandaşlık ve güvenli internet kullanımı becerilerini kazandırmada kilit rol oynar (Tekerek ve Tekerek, 2013). Öğretmenlerin düşük siber güvenlik farkındalığı, öğrencilere aktardıkları bilginin kalitesini düşürür ve geleceğin dijital vatandaşlarının güvensiz alışkanlıklar edinmesine neden olabilir. Dolayısıyla, öğretmenlerin farkındalık düzeyi, ulusal siber güvenlik stratejisinin uzun vadeli başarısını doğrudan etkilemektedir.

Bu bağlamda, bu çalışma, kamu yönetimi perspektifiyle öğretmenlerin siber güvenlik farkındalık düzeylerini branşlar bazında inceleyerek, kamu çalışanlarının dijital yetkinlikleri ve MEB politikaları için yol gösterici veriler

sunmayı hedeflemektedir.

Tablo 1. Örneklemin Demografik Özellikleri

Demografik Özellik			**Katılımcı Sayısı**
1	Cinsiyet	Kadın	45
		Erkek	51
		Toplam	**96**
2	Yaş Aralığı	25-35 yaş arası	41
		35-50 yaş arası	46
		50 yaş ve üzeri	9
		Toplam	**96**
3	Mesleki Tecrübe	1-10 sene arası	23
		10-25 sene arası	61
		25 sene ve üstü	12
		Toplam	**96**
4	Mesleki Alan	Bilişim Teknolojileri	32
		Sosyal Bilimler	32
		Fen Bilimleri	32
		Toplam	**96**

YÖNTEM

Araştırma Grubu

Araştırmaya, Çorum ili genelinde MEB'e bağlı okullarda görev yapan, farklı branşlardan 96 öğretmen katılmıştır. Araştırmanın temel amacına uygun olarak, katılımcıların seçimi amaçlı örnekleme yöntemlerinden heterojenite (çeşitlilik) örneklemesi alt türü ve kolay ulaşılabilir örnekleme birlikte kullanılarak yapılmıştır. Bu yaklaşım, branşlar arası karşılaştırma yapabilmek için örneklemin; 32 BT, 32 Fen Bilimleri branşları (Matematik, Fen bilgisi, Biyoloji) ve 32 Sosyal Bilimler branşları (Türk Dili ve Edebiyatı, Tarih, Din Kültürü) öğretmenlerinden oluşturularak dengeleme ilkesi gözetilmesini sağlamıştır. Bu örnekleme yönteminin tercih edilmesi, genellenebilirlik açısından kısıtlılık yaratmakla birlikte, çalışmanın temel hipotezini (branşlar arası farkın varlığı) test etme amacına hizmet etmiştir. Anket uygulamasına katılanlar hakkında belirlenen bilgiler Tablo 1'de özetlenmiştir.

Katılımcıların demografik özelliklerine göre dağılımı şu şekildedir: 51'i Erkek ve 45'i kadın öğretmendir. Yaş dağılımı bakımından 25-35 yaş aralığında 41, 35-50 yaş aralığında 46 ve 50 yaş üzeri 9 öğretmenden meydana gelmektedir.

Veri Toplama Araçları

Araştırma kapsamında veri toplamak için iki kısımdan oluşan bir anket formu kullanılmıştır. İlk kısım, katılımcıyı tanımlayan demografik özellikleri (branş, yaş, çalışma yılı, cinsiyet, BİT kullanma becerileri) içermektedir. İkinci bölümde ise Erol, Şahin, Yılmaz ve Haseski (2015) tarafından geliştirilen Kişisel Siber Güvenliği Sağlama Ölçeği (KSGSÖ) kullanılarak farkındalık düzeyi ölçülmüştür.

Kullanılan KSGSÖ, toplamda 25 maddeden oluşmakta ve bilgi güvenliği ile siber güvenlik alanını kapsamaktadır. Ölçek, kapsam olarak birleşerek 5 alt faktörden oluşmaktadır: 10 maddelik Kişisel Gizliliği Koruma, 4 maddelik Güvenilmeyenden Kaçınma, 5 maddelik Önlem Alma, 2 maddelik Ödeme Bilgilerini Koruma ve 4 maddelik İz Bırakmama. Tablo 2'de Ölçek Faktörlerinin Kapsadığı Madde Sayıları ve Numaraları sunulmuştur. Ölçeğin güvenilirlik analizi için 30 katılımcı ile yapılan ön uygulamada Cronbach Alpha değeri $\alpha = 0.79$ olarak bulunmuştur. Bu değer, ölçeğin araştırma grubunda yüksek derecede iç tutarlılığa sahip olduğunu göstermektedir (George ve Mallery, 2019).

Tablo 2. Ölçek Faktörlerinin Kapsadığı Madde Sayıları ve Numaraları

Faktör	Madde Sayısı	Faktör Adı	İçerdiği Maddeler
1	10	Kişisel Gizliliği Koruma	M5,M7,M12,M13,M17,M18,M19,M20,M24,M25
2	4	Güvenilmeyenden Kaçınma	M9, M10, M11, M22
3	5	Önlem Alma	M1,M2,M3,M4,M6
4	2	Ödeme Bilgilerini Koruma	M15,M16
5	4	İz Bırakma	M8,M14,M21,M23

KSGSÖ'nin uygulanması, pandemi koşulları göz önüne alınarak web tabanlı bir anket sunum aracı olan Google Formlar üzerinden gerçekleştirilmiştir. Anket, Çorum ilindeki 250'yi aşkın öğretmene ulaştırılmış ve 103 geri dönüş alınmıştır.

Elde edilen veriler bilgisayar ortamına aktarılmıştır. Alınan 103 yanıttan 7 tanesi eksik veya hatalı veri içerdiği için elenmiştir. Bu eleme süreci; Ölçek maddelerinin %20'sinden fazlasının boş bırakılması, tüm maddelere aynı yanıtın verilmesi ve demografik bilgilerin tam olmaması kriterleri temel alınarak yapılmıştır. Sonuç olarak analizler 96 katılımcı üzerinden yürütülmüştür.

Veri analizi için Microsoft Excel ve SPSS v21 programı kullanılmıştır. İlk aşamada, örneklemin genel özelliklerini ve farkındalık düzeylerini tanımlamak amacıyla yüzde, ortalama ve frekans dağılımı gibi temel istatistiki işlemler kullanılmıştır.

İkinci aşamada, makalenin temel amacına uygun olarak, öğretmenlerin branşları arasındaki siber güvenlik farkındalık düzeylerinin istatistiksel açıdan anlamlı bir fark gösterip göstermediğini belirlemek amacıyla One-Way ANOVA yapılmıştır. Analiz sonuçları F değeri ve p değeri ile birlikte %95 güven aralığında raporlanmıştır.

Sınırlılıklar

Bu çalışmanın başlıca sınırlılıkları aşağıda özetlenmiştir:

Örneklem Büyüklüğü ve Temsil Gücü: Araştırma yalnızca Çorum ilinde yürütülmüş olup toplam 96 katılımcıdan elde edilen verilerle sınırlıdır. Bu durum, bulguların Türkiye genelindeki öğretmenlere genellenebilirliğini sınırlamaktadır.

Örneklem Seçim Yöntemi: Katılımcıların belirlenmesinde tesadüfi olmayan, uygun/kolay ulaşılabilir örnekleme yöntemi kullanılmıştır. Bu örnekleme yaklaşımı, temsil yeteneğini azaltan bir özelliğe sahiptir.

Veri Toplama Yöntemi: Anketlerin Google Formlar aracılığıyla çevrim içi olarak uygulanması, yanıt vermeyen bireylerin özelliklerine ilişkin bilgi edinilmesini engellemiştir. Bu durum, örneklemin gerçek temsil gücü hakkında kesin çıkarımlar yapmayı güçleştirmektedir.

Bulgular

Bu bölümde, katılımcılardan toplanan verilerin istatistiksel analiz sonuçları sunulmaktadır.

Tanımlayıcı Bulgular

Katılımcıların yaklaşık %68'i mesleki ve günlük işlerinin büyük bir kısmını bilgisayar ortamında gerçekleştirdiklerini, %32'si ise yalnızca temel düzeyde bilgisayar kullanımına sahip olduklarını belirtmiştir. Siber güvenlik farkındalığına ilişkin bazı temel tanımlayıcı bulgular şöyledir:

- Erkek katılımcıların farkındalık düzeyi %79,59; kadın katılımcıların farkındalık düzeyi %72,47 olarak hesaplanmıştır.
- 25-35 yaş arası öğretmenlerde farkındalık %80,79; 35-50 yaş arası öğretmenlerde %78,84; 50 yaş ve üzeri öğretmenlerde ise %75,42 olarak bulunmuştur.

Bu bulgular, öğretmenlerin genel olarak orta-üst düzeyde siber güvenlik farkındalığına sahip olduklarını göstermektedir.

Branşlar Arası Farkındalık ve İstatistiksel Analiz Sonuçları

Farklı branşlarda görev yapan öğretmenlerin siber güvenlik farkındalık düzeyleri arasında anlamlı bir fark olup olmadığını belirlemek amacıyla One-Way ANOVA uygulanmıştır.

Tablo 3. Branş Bazında Tanımlayıcı İstatistiki Değerler

Branş	Ortalama Farkındalık Skoru	Standart Sapma	N
BT	84.75	11,02	32
Sosyal Bilimler	76.80	11,14	32
Fen Bilimleri	73,52	12,66	32

Tablo 3'teki tanımlayıcı bulgular incelendiğinde, BT öğretmenlerinin farkındalık düzeylerinin diğer iki branşa göre belirgin şekilde daha yüksek olduğu, Sosyal Bilimler ve Fen Bilimleri öğretmenlerinin ise birbirine yakın ortalama değerlere sahip olduğu görülmektedir.

Tablo 4. Öğretmenlerin Farkındalık Düzeyleri İçin Tek Yönlü ANOVA Sonuçları

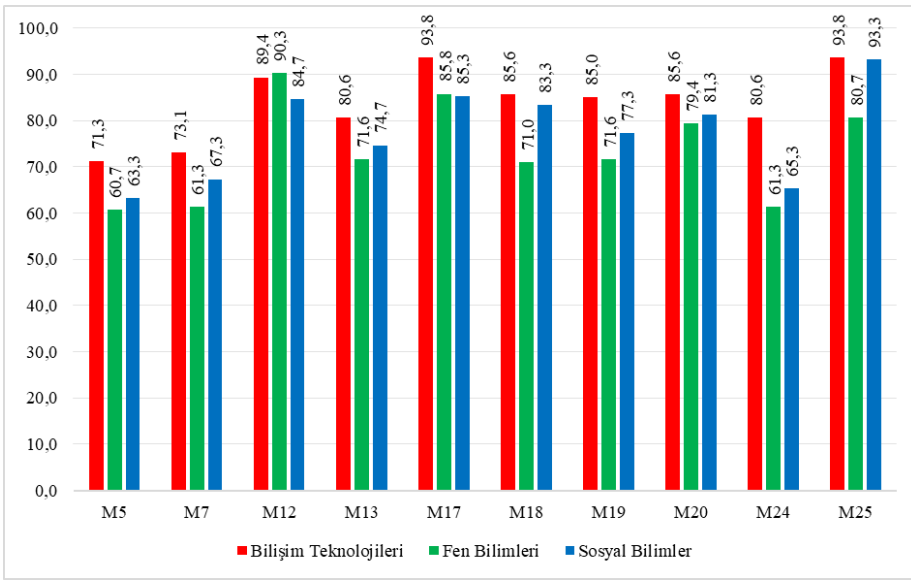
	Kareler Toplamı (KT)	Serbestlik Derecesi (sd)	Ortalama Kare (OK)	F	p
Gruplar Arası	1505,00	2	752,50	5,56	0,013
Gruplar İçi	12583,71	93	135,31	-	-
Toplam	14088,71	95			

Tablo 4'te verilen ANOVA sonuçlarına göre, branşlar arasında farkındalık puanları açısından istatistiksel olarak anlamlı bir fark bulunmuştur ($F[2, 93] = 5.56$, $p = .013 < .05$). Bu sonuç, öğretmenlerin siber güvenlik farkındalık düzeylerinin branş değişkenine göre anlamlı biçimde farklılaştığını ortaya koymaktadır. Farkın hangi branşlardan kaynaklandığını belirlemek amacıyla yapılan Tukey HSD Post Hoc testi, $p<.05$ anlamlılık düzeyine göre, BT öğretmenlerinin farkındalık düzeylerinin Sosyal Bilimler ve Fen Bilimleri öğretmenlerinden anlamlı derecede daha yüksek olduğunu göstermiştir. Sosyal Bilimler ve Fen Bilimleri branşları arasında ise anlamlı bir fark bulunmamıştır.

Bu bulgu, mesleki uzmanlık alanının siber güvenlik farkındalığı üzerinde etkili bir değişken olduğunu ve öğretmenlere yönelik siber güvenlik eğitim programlarının branş bazında belirlenmesi gerektiğini desteklemektedir.

Kişisel Gizliliği Koruma

KSGSÖ'ndeki alt faktörlerden bir diğeri, Kişisel Gizliliği Koruma Faktörü (KGKF)' dür. Bu faktör kapsamında tüm katılımcılardan alınan veriler analiz edilerek Şekil 3'teki grafik elde edilmiştir. Bu grafik 3 farklı branş türündeki öğretmenleri farkındalık oranlarını ayrı ayrı ele alarak yansıtmaktadır.

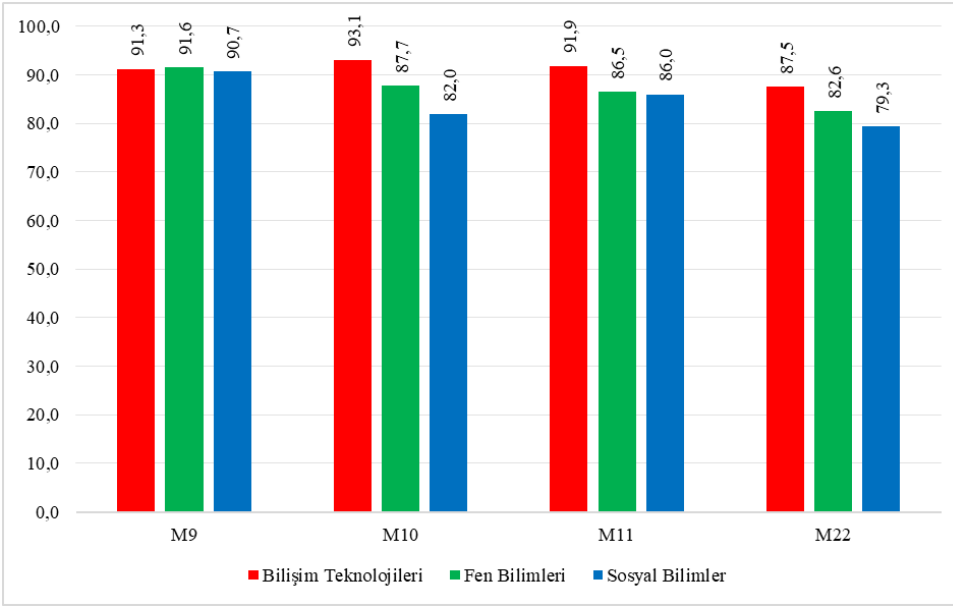


Şekil 3. Üç Farklı Branş Bazında KGKF Grafiği

Şekil 3 incelendiğinde, BT öğretmenlerinin kişisel gizliliği koruma konusunda diğer branşlara göre çoğu maddede daha yüksek farkındalık düzeyine sahip olduğu görülmektedir. Bu sonuç, BT öğretmenlerinin kişisel gizliliği koruma konusunda alan bilgisi ve tecrübesi ile doğru orantılı bir şekilde ilişkilendirilebilir. Diğer yandan, Sosyal Bilimler öğretmenleri ise web ve sosyal medya ortamlarında kişisel bilgi paylaşımında Fen Bilimleri öğretmenlerine kıyasla daha dikkatli görünmektedir. Bununla birlikte, M12 ve M17 maddelerinde Fen Bilimleri öğretmenlerinin Sosyal Bilimlere göre daha yüksek puan aldığı ve tanımadıkları kişilerden gelen e-posta veya bağlantı isteklerine karşı daha duyarlı oldukları anlaşılmaktadır.

Güvenilmeyenden Kaçınma

Güvenilmeyenden Kaçınma faktörü, KSGSÖ'nün tehdit ve risklere karşı korunmayı ölçen alt boyutlarından biridir. Analiz sonuçları Şekil 4'te sunulmuştur. M22 dışındaki tüm maddelerde tüm branşlarda farkındalığın %80'in üzerinde olduğu belirlenmiştir. "Güvenmediğim sitelerden dosya indirmem" şeklindeki M22 maddesinde ise Sosyal Bilimler öğretmenleri %79,3 ile diğer branşlara kıyasla biraz daha düşük bir değerlendirme göstermiştir.



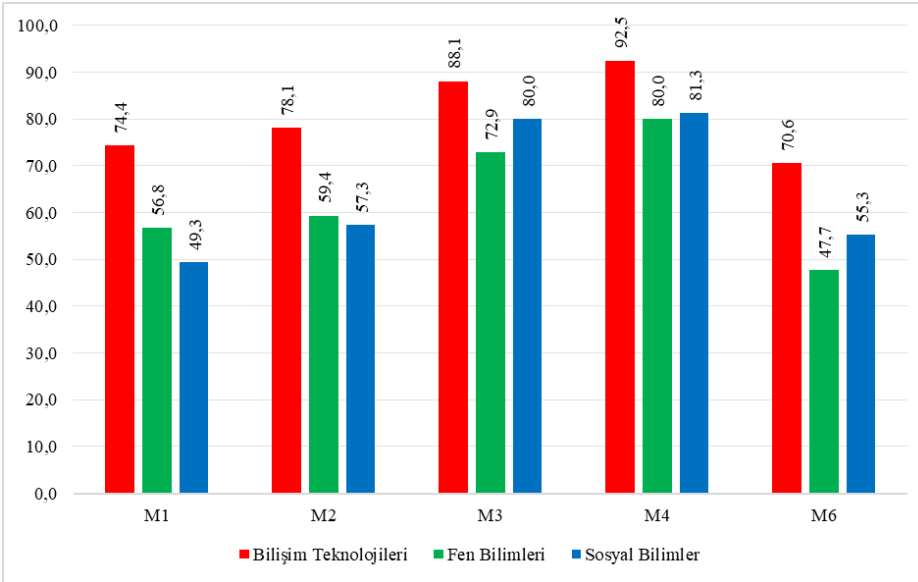
Şekil 4. Üç Farklı Branş Türünde Güvenilmeyenden Kaçınma Faktörü Grafiği

Anketin bu alt faktörünün M10, M11 ve M22 maddelerine verilen yanıtlara bakıldığında, BT öğretmenlerinin tüm gruplar içinde en yüksek farkındalık düzeyine sahip olduğu görülmektedir. Ayrıca Fen Bilimleri öğretmenleri, Sosyal Bilimler öğretmenlerine kıyasla siber ortamlarda daha dikkatli davranmakta; güvenmedikleri sitelere bağlanmama ve gelen talepleri sorgulama konusunda daha temkinli görünmektedir. M9 maddesinde ise tüm branşlarda farkındalık düzeyinin oldukça yüksek olduğu, öğretmenlerin %90'ın üzerinde bilinçli davrandıkları belirlenmiştir.

Önlem Alma

KSGSÖ'nün üçüncü alt faktörü olan Önlem Alma, siber tehdit ve saldırılara karşı temel koruyucu adımları içermektedir. Bu adımlar; güncel yazılım

kullanımı, bağlantı güvenliğinin kontrolü, güvenlik yazılımlarının kullanılması ve temel güvenlik ayarlarının yapılması gibi uygulamalardan oluşmaktadır. Katılımcı yanıtlarının analiz edildiği Şekil 5'e göre, üç branşta da M3 ve M4 maddeleri dışında diğer maddelerde farkındalık düzeylerinin görece düşük olduğu görülmektedir.

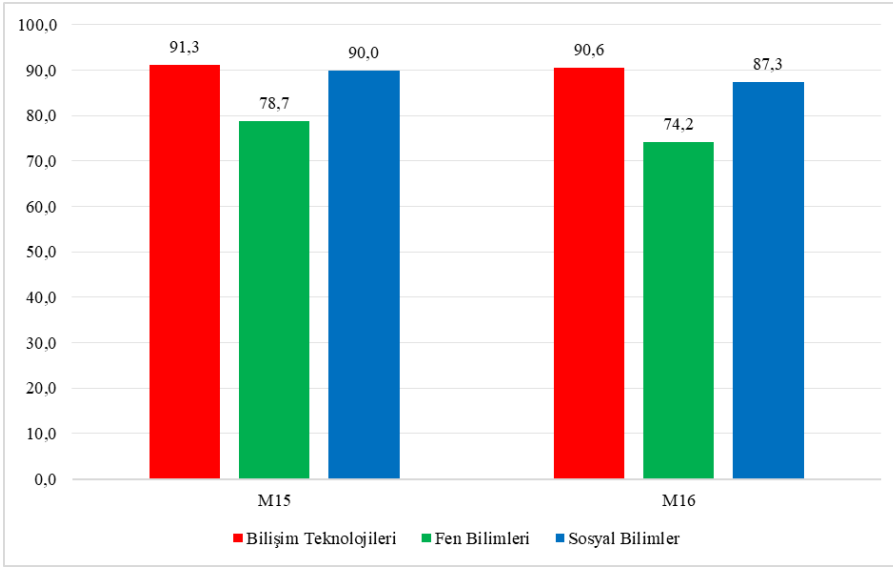


Şekil 5. Üç Farklı Branş Türünde Önlem Alma Faktörü Grafiği

Şekil 5 incelendiğinde, parola oluşturma ve güvenlik yazılımı kullanımı dışındaki önlemlere ilişkin farkındalık düzeylerinin tüm branşlarda genellikle %70'in altında kaldığı görülmektedir. Buna karşın BT öğretmenleri, tüm maddelerde diğer branşlara göre daha yüksek önlem alma tutumuna sahiptir. Maddeler bazında değerlendirildiğinde, M1 ve M2'de Fen Bilimleri öğretmenleri ikinci sırada yer alırken; M3, M4 ve M6'da Sosyal Bilimler öğretmenlerinin ikinci sıraya çıktığı anlaşılmaktadır.

Ödeme Bilgilerini Koruma

KSGSÖ'nün dördüncü alt faktörü olan Ödeme Bilgilerini Koruma, maddi kayıpların en sık yaşandığı alanı kapsamaktadır. Katılımcı cevaplarının analizine dayanan Şekil 6, bu faktöre ilişkin bulguları göstermektedir. İki maddeden oluşan bu faktörde, özellikle Fen Bilimleri öğretmenlerinin diğer iki branşa kıyasla daha düşük farkındalık düzeyine sahip olduğu görülmektedir.

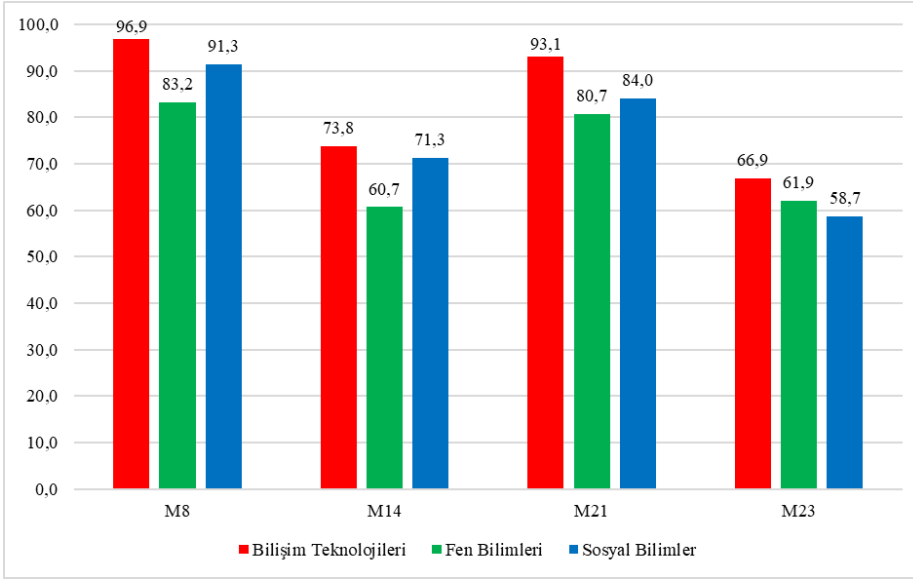


Şekil 6. Üç Farklı Branşa Göre Ödeme Bilgilerini Koruma Grafiği

Ödeme Bilgilerini Koruma grafiği, kullanıcıların çevrim içi ödeme işlemleri sırasında donanım ve yazılım güvenliğini ne ölçüde kontrol ettiklerini göstermektedir. Ölçek sonuçları, BT öğretmenlerinin ödeme sürecindeki güvenlik önlemlerine diğer iki branşa göre daha yüksek farkındalıkla yaklaştığını ortaya koymaktadır. Bununla birlikte, Sosyal Bilimler öğretmenlerinin Fen Bilimleri öğretmenlerine kıyasla bu konuda daha dikkatli davrandıkları da görülmektedir.

İz Bırakmama

KSGSÖ'nün son alt faktörü olan İz Bırakmama, internet kullanımından sonra sistemde kalan log kayıtları, tarayıcı gezinti izleri ve oturum bilgileri gibi dijital kalıntıların temizlenmesine yönelik farkındalığı ölçmektedir. Ayrıca parolaların belirli aralıklarla güncellenmesi de bu faktörün önemli bir bileşenidir. Katılımcıların bu alt faktöre ilişkin yanıtları analiz edilerek elde edilen bulgular Şekil 7'de sunulmuştur.

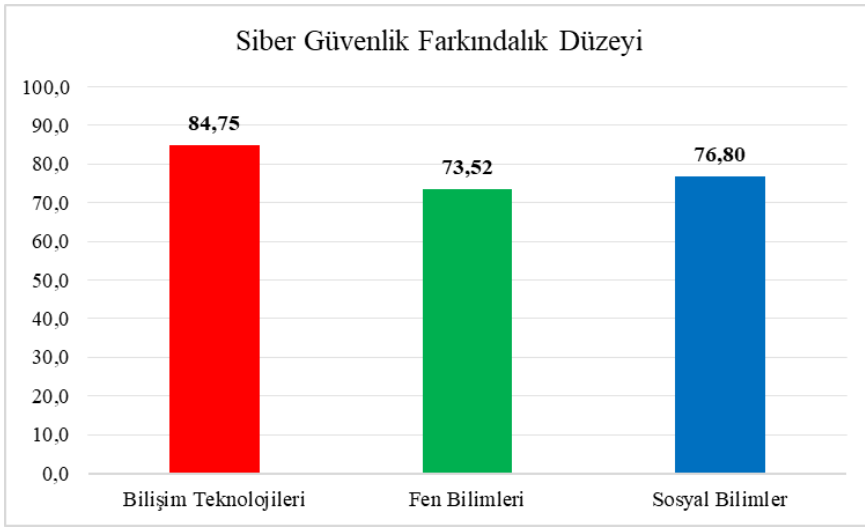


Şekil 7. İz Bırakmama Alt Faktörü Grafiği

Şekil 7'de yer alan grafik incelendiğinde, iz bırakmamaya yönelik farkındalığın BT öğretmenlerinde tüm maddelerde oldukça yüksek olduğu ve diğer branşlara göre açık ara ilk sırada yer aldığı görülmektedir. Sosyal Bilimler öğretmenleri ise M8, M14 ve M21 maddelerinde Fen Bilimleri öğretmenlerinden daha yüksek farkındalık düzeyi göstermişlerdir. Buna karşılık, "İnternette kullandığım parolaları değiştiririm" olan M23 maddesinde Fen Bilimleri öğretmenleri ikinci sıraya yükselmiştir. Ancak bu maddede her üç branşın da düşük bir farkındalık göstermesi kullanıcıların periyodik parola değiştirme alışkanlığını yeterince benimsemediğini vurgulamaktadır.

Siber Güvelik Farkındalık Düzeyi

Ölçeği oluşturan alt faktörler ve maddeleri birlikte değerlendirildiğinde, branşlara göre genel siber güvenlik farkındalığı dağılımı Şekil 8'de gösterilmiştir. Analiz sonuçlarına göre BT öğretmenleri %84,75 ile en yüksek farkındalık düzeyine sahipken bunu, %76,80 ile Sosyal Bilimler ve %73,52 ile Fen Bilimleri öğretmenleri izlemiştir.



Şekil 8. Branş Bazında Siber Güvenlik Farkındalık Düzeyi

Şekil 8'deki ortalamalar incelendiğinde, BT öğretmenlerinin siber güvenlik farkındalık düzeyinin Sosyal Bilimler branşına kıyasla 7,95 puan, Fen Bilimleri branşına kıyasla ise 10,23 puan daha yüksek olduğu görülmektedir. Bu farkın, BT öğretmenlerinin mesleki uzmanlıkları gereği dijital sistemler, siber tehditler ve koruyucu güvenlik mekanizmaları konusunda daha geniş bilgi ve deneyime sahip olmalarından kaynaklandığı değerlendirilmektedir.

SONUÇ VE ÖNERİLER

Bu araştırmada, Çorum ilinde görev yapan üç farklı branştaki öğretmenlerin Kişisel Siber Güvenlik Farkındalık düzeyleri incelenmiştir. Uygulanan KSGSÖ'nün ön testinde Cronbach Alpha güvenirlik katsayısı 0.79 olarak hesaplanmış ve ölçeğin yeterli iç tutarlılığa sahip olduğu belirlenmiştir. Bu doğrulama sonrasında ana veri toplama süreci gerçekleştirilmiştir.

Araştırma bulguları, öğretmenlerin genel olarak orta-üst düzeyde siber güvenlik farkındalığına sahip olduklarını göstermektedir. Branşlara göre yapılan analizde, BT öğretmenlerinin farkındalık düzeyinin (%84,75) diğer branşlara göre anlamlı biçimde daha yüksek olduğu görülmüştür. Sosyal Bilimler öğretmenlerinin farkındalık düzeyi %76,80, Fen Bilimleri öğretmenlerinin farkındalık düzeyi ise %73,52 olarak bulunmuştur. Cinsiyet değişkenine göre erkek öğretmenlerin farkındalık düzeyi %79,59, kadın öğretmenlerin farkındalık düzeyi ise %72,47'dir. Yaş değişkeni incelendiğinde, farkındalık düzeyinin yaş ilerledikçe sınırlı ölçüde azaldığı görülmektedir. Bu sonuçlar, BT öğretmenlerinin mesleki uzmanlıkları nedeniyle dijital sistemler,

tehditler ve koruma yöntemlerine dair daha yüksek bilgi ve deneyime sahip oldukları varsayımıyla uyumludur.

Siber tehditlerin dünya genelinde artış göstermesi, temel düzeyde güvenlik farkındalığının önemini daha da artırmaktadır. Nitekim uluslararası raporlar, 2030 yılına kadar siber saldırıların ekonomik etkisinin 90 trilyon dolara ulaşabileceğini öngörmektedir (Aslay, 2017). Bu nedenle öğretmenlerin bilgi güvenliği farkındalığı, yalnızca bireysel güvenlik açısından değil, eğitim kurumlarının veri bütünlüğünün korunması açısından da kritik öneme sahiptir. MEB tarafından yürütülen hizmet içi eğitimler ve bilgilendirme faaliyetlerinin bu düzeyde farkındalık oluşmasında etkili olduğu değerlendirilmektedir.

Araştırma bulgularına dayanarak öğretmenlere ve genel dijital kullanıcı profiline yönelik aşağıdaki öneriler sunulmaktadır:

- Dijital sistemlere erişim sırasında daha güçlü parolalar tasarlanmalı ve periyodik olarak değiştirilmelidir.
- Dijital sistemlerin kullanımları sırasında üreticilerin tayin ettikleri varsayılan ayarlar yerine kişiselleştirilmiş ve gelişmiş ayarlar tercih edilmelidir.
- Dijital sistemlere erişimlerin sürekli kontrol altında tutularak yetkisiz ve izinsiz erişimlerin önüne geçilmelidir. Bunun için trafik analizi ve işlem (log) kayıtlarının incelenmesi faydalıdır.
- Umuma açık alanlarda ortak kullanılan BT'ye erişim dikkatli yapılmalı, kullanım bittikten sonra geriye dönük izler ve kayıtlar temizlenmelidir.
- Dijital sistemlerin periyodik olarak yedekleri alınarak anlık kayıpların önüne geçilmelidir.
- Dijital ortamlarda yayılan bilgilerin doğruluğu ve güncelliği güvenilir kaynaklardan teyit edilmeden bilgi ve fikir sahibi olunmamalı ve paylaşılmamalıdır.
- Kişisel özel ve hassas bilgileri izinsiz ve yetkisiz bir şekilde erişimi ve paylaşımı yapılmamalıdır.
- Dijital sistemlerde kurulu yazılımların ve donanımların güncel tutulmasına, çeşitli güvenlik yazılımları ile taramalarının yapılmasına özen gösterilmelidir.
- Dijital ortamların erişim ve denetim ayarlarının düşük seviyelerden üst seviyelere çekilmesi sağlanmalıdır.

- Dijital sistemlere erişimler sırasında çok katmanlı kimlik doğrulama (Parola, SMS, Biometrik vb.) mekanizmaları geliştirilmelidir.
- Toplumun tüm kesimlerinin bilgi güvenliği ve siber güvenlik hakkında farkındalık düzeyinin geliştirilmesine yönelik çalışmaların yapılması
- Siber tehdit ve saldırılara maruz kalındığında BT konusunda bilgili ve profesyonel kişilere danışarak yardım alınmalıdır.
- Siber tehdit ve saldırılar hakkında güvenilir ve otorite kaynaklardan bildirilen duyuru ve raporlar takip edilerek güncel bilgi sahibi olunmalıdır.

Günümüzde çocukların teknoloji ile tanışma yaşının giderek düşmesi, dijital güvenliğin önemini daha da artırmaktadır. Bilgi teknolojilerinin yoğun kullanıldığı bu dönemde, Türkiye'nin gelişmiş ülkelerle rekabet edebilmesi için eğitim sistemine BT okuryazarlığı, siber güvenlik, veri analitiği ve yapay zekâ gibi konularda kapsamlı derslerin eklenmesi büyük önem taşımaktadır. Bu doğrultuda öğretmenlerin bu alanlarda bilinçlendirilmesi ve gerekli becerilerle donatılması, geleceğin güvenli ve bilinçli nesillerinin yetişmesine önemli katkılar sağlayacaktır.

KAYNAKÇA

Aksoğan, M. & Atıcı, B. (2023). Akademisyenlerin Dijital Veri Güvenliği Farkındalıkları Üzerine Bir Araştırma: Malatya Örneği. Gümüşhane Üniversitesi Sosyal Bilimler Dergisi, Cilt:14, Sayı:2, ss.429-439.

Aldridge, J., Medina, J. & Ralphs, R. (2010). The Problem of Proliferation: Guidelines for Improving the Security of Qualitative Data in a Digital Age, Research Ethics, Volume:6, Issue:1, pp.3-9. https://doi.org/10.1177/174701611000600102.

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

Avcı, Ü. & Oruç, O. (2020). Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi. İnönü Üniversitesi Eğitim Fakültesi Dergisi, Cilt:21 Sayı:1, ss:284-303, https://doi.org/10.17679/inuefd.526390

Aydın, Ö. & Yükçü, S. (2020). Siber Saldırı Önlemede Blokzinciri Teknolojisinin Fayda Maliyet Açısından Değerlendirilmesi. MANAS Sosyal Araştırmalar Dergisi, Cilt: 9, Sayı:4, ss.2519-2530

Baz, F. Ç. (2018). Sosyal Medya Bağımlılığı: Üniversite Öğrencileri Üzerine Çalışma, OPUS Uluslararası Toplum Araştırmaları Dergisi, Cilt:9, Sayı:16, ss.276-295, https://doi.org/10.26466/opus.470118

Canoğulları, E. (2021). Öğretmenlerin Bilgi Güvenliği Konusundaki Farkındalıklarının İncelenmesi, Kalem Uluslararası Eğitim ve İnsan Bilimleri Dergisi, Cilt:11, Sayı:2, ss.651-679, https://doi.org/10.23863/kalem.2021.219

Check Point. (2023). Surge in Cybercrime: Check Point 2023 Mid-Year Security Report. İnternet, Erişim Tarihi: 23 Ağustos 2023, Erişim Adresi: https://blog.checkpoint.com/security/check-point-software-2023-mid-year-security-report-old-meets-new-as-usb-devices-and-artificial-intelligence-are-exploited-by-cybercriminals/

Coşar, M. (2022). Siber Dünyanın Karanlık Yüzü: Deepweb ve Darknet. Journal of Management Theory and Practices Research, Cilt:3, Sayı:1, ss:58-71.

Coşar, M. (2024). Kurumsal Bilgi Güvenliği Yönetiminde Yapay Zekâ Destekli Risk Analizi. Denetişim, Sayı 31, ss.144-155. https://doi.org/10.58348/denetisim.1519578

Coşar, M., (2025). Blockchain Technology in Digital Public Applications. inbook. Digital Transformation in Public Administration. Ed(s): Leblebici, D.N., Yıldırım, K.E., Gemici, E., Nova Science Publishers, ISBN:979-8-89530-250-7. https://doi.org/10.52305/kqdb2586

Eminağaoğlu, M. & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir? Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt:11, Sayı:4.

ENISA. (2021). ENISA Threat Landscape 2021. İnternet, Erişim Tarihi: 21 Kasım 2025, Erişim Adresi: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA. (2025). ENISA Threat Landscape 2023. İnternet, Erişim Tarihi: 21 Kasım 2025, Erişim Adresi: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği Geliştirme Çalışması. International Journal of Human Sciences, Volume:12, No:2, pp:75-91, https://doi.org/10.14687/ijhs.v12i2.3185

George, D. & Mallery, P. (2019). IBM SPSS Statistics 26 Step by Step: A Simple Guide and Reference. 16th Edition, Routledge. ISBN:9780429056765 https://doi.org/10.4324/9780429056765

Kemp, S. (2023). Digital 2023: Global Overview Report. İnternet. Erişim Tarihi: 10 Haziran 2023, Erişim Adresi: https://datareportal.com/reports/digital-2023-global-overview-report

OECD. (2016). Skills for a digital world. OECD Publishing. OECD Digital Economy Papers, 2 June 2016. https://doi.org/10.1787/5jlwz83z3wnw-en

OECD. (2019). OECD Skills Outlook 2019: Thriving in a digital world. OECD Publishing. https://doi.org/10.1787/df80bc12-enOECD Skills Outlook, 9 May 2019

OECD. (2020). The OECD Digital Government Policy Framework: Six dimensions of a digital government. OECD Public Governance Policy Papers. 7 October 2020. https://doi.org/10.1787/f64fed2a-en

OECD. (2021). Digital education outlook 2021: Pushing the frontiers with AI, blockchain and robots. OECD Digital Education Outlook. 8 June 2021. https://doi.org/10.1787/589b283f-en

Ryan, T., Allen, K-A., Gray, D.L. & McInerney, D.M. (2017). How Social Are Social Media? A Review of Online Social Behaviour and Connectedness, Journal of Relationships Research, Volume:8, e8, pp.1-8, https://doi.org/10.1017/jrr.2017.13

Söylemez, A., Ay, H.M., Ay, N.G. (2022). Dijital Toplumda E-Seçim ve Blok Zinciri Uygulamaları. Ed. Arslan I., Akçaçı, T., Bozgeyik. Küreselleşme Çağında Kalkınma ve Yeni Ekonomi, Orion Kitabevi, ISBN: 978-625-7294-82-9, 2022 Ankara.

Söylemez, A., Söylemez, D. İ. (2024, July). The Role of Blockchain Technology in Public Admınistration. 10. International European Congress on Advanced Studies in Basic Sciences, 26-28 July 2024 Amsterdam, Netherlands.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi, KSÜ Doğa Bilimleri Dergisi, Cilt:11,Sayı:1,ss.132-137.
https://dergipark.org.tr/en/pub/ksudobil/issue/35406/393310

Tekerek, M. & Tekerek, A. (2013). Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. Turkish Journal of Education, Cilt:2, Sayı:3, ss.61-70, https://doi.org/10.19128/turje.181065

Trendmicro. (2023). Stepping Ahead of Risk - Trend Micro 2023 Midyear Cyber Security Threat Report. İnternet, Erişim Tarihi: 12 Ağustos 2023, Erişim Adresi: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/stepping-ahead-of-risk-trend-micro-2023-midyear-cybersecurity-threat-report

TUİK. (2022). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2021. Erişim Adresi: https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437, Erişim Tarihi: 15 Mayıs 2023.

United Nations. (2022). United Nations E-Government Survey 2022: The future of digital government. United Nations Department of Economic and Social Affairs. İnternet, Erişim Tarihi: 21 Kasım 2025, Erişim Adresi: https://publicadministration.desa.un.org/publications/un-e-government-survey-2022

Uzun, E. & Coşar, M. (2022). Lise Çağındaki Öğrencilerin Sosyal Medya Ortamları Hakkında Bilgi Güvenliği Farkındalık Düzeyleri, Hitit Ekonomi ve Politika Dergisi, Cilt:2, Sayı:1, ss.50-61.

Ünlü, F. (2018). Orta Yaş Üstü Bireylerde Sosyal Medya Bağımlılığı ve Sosyal İzolasyon, PESA Uluslararası Sosyal Araştırmalar Dergisi, Cilt:4, Sayı:1, ss.161-172, https://doi.org/10.25272/j.2149-8385.2018.4.1.13

World Bank. (2020). Digital Government – User-Centric Public Services. World Bank Publications. Erişim Tarihi: 21 Kasım 2025, Erişim Adresi: https://documents.worldbank.org/curated/en/562371467117654718/pdf/105318-WP-PUBLIC-Digital-Government-2020.pdf

Etik Beyanı: Yazarlar bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu beyan ederler. Aksi bir durumun tespiti halinde Kamu Yönetimi ve Teknoloji Dergisi'nin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarlarına aittir.

Yazar Katkıları: Dr. Öğretim Üyesi Mustafa COŞAR ve Murat ERDOĞAN çalışmanın tamamında birlikte katkı sunmuşlardır.

Çıkar Beyanı: Yazarlar ve herhangi bir kurum/ kuruluş arasında çıkar çatışması yoktur.

Teşekkür: Yayın sürecinde katkısı olan hakemlere teşekkür ederiz.

Ethics Statement: The authors declare that the ethical rules are followed in all preparation processes of this study. In the event of a contrary situation, the Journal of Public Administration and Technology has noresponsibility and all responsibility belongs to the authors of the study.

Author Contributions: Dr. Öğretim Üyesi Mustafa COŞAR ve Murat ERDOĞAN have contributed together to all parts and stages of the study.

Conflict of Interest: There is no conflict of interest among the authors and any institution.

Acknowledgement: We would like to thank the referees who contributed to the publication process.