İSTANBUL
İL MİLLÎ EĞİTİM MÜDÜRLÜĞÜ
İSTANBUL EĞİTİM DERGİSİ
ISTANBUL EDUCATION JOURNAL (ISTJ)

İstanbul Eğitim Dergisi, 2025
Sayı.2 Sayfa.83-104
Araştırma Makalesi
doi.org/10.71270/istanbulegitim.istj.1660280

Öğretmenlerin Oltalama Saldırılarına Karşı Farkındalık Düzeyleri

Neslihan Genç[1]*, Murat Yücel[2]

[1*]Sorumlu yazar, Millî Eğitim Bakanlığı, Dilek Sabancı Ticaret Mesleki ve Teknik Anadolu Lisesi, İstanbul, Türkiye
neslihankgenc@gmail.com 0009-0002-8254-4783
[2]Gazi Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü, Ankara, Türkiye 0000-0002-0349-4013

Makale Geliş Tarihi: 18/03/2025 *Makale Kabul Tarihi:16/06/2025*

Öz

Siber güvenliğin önem kazandığı dijital dünyada oltalama saldırıları, hassas bilgileri ele geçirmek ve sistemlere erişim sağlamak için kullanılan en yaygın siber tehditlerden biridir. Sosyal mühendislik teknikleriyle gerçekleştirilen bu saldırılar, günümüzde sadece bireyleri değil, küçük işletmelerden çok uluslu şirketlere, yerel yönetimlerden kritik devlet altyapılarına kadar tüm ekonomik ve sosyal katmanları hedef almaktadır. Bu araştırma, Millî Eğitim Bakanlığı'na bağlı resmî okullardaki farklı kademelerde (anaokulu, ilkokul, ortaokul, lise) görev yapan öğretmenlerin oltalama saldırılarına karşı farkındalık düzeylerini belirlemek amacıyla betimsel tarama modeline dayalı olarak gerçekleştirilmiş nicel bir çalışmadır. Bu bağlamda kartopu örnekleme ile seçilen öğretmenlerin günlük mesleki faaliyetleri sırasında alabilecekleri gerçekçi oltalama e-postaları tasarlanmış ve e-postalar kullanılarak bu tür saldırılara karşı farkındalık düzeyleri ve verdikleri tepkiler analiz edilmiştir. Araştırma bulgularına göre öğretmenlerin teknik branşlarda dâhi oltalama saldırılarına karşı farkındalık düzeylerinin yeterli olmadığı ortaya çıkmıştır. Bu sonuçlar, öğretmenlerin siber tehditlere karşı savunmasız olduğu ve kapsamlı eğitim programlarına ihtiyaç duyulduğunu göstermektedir. Bu durumda, ilgili eğitim programlarının tüm öğretmenleri kapsaması; eğitim içeriklerinin interaktif simülasyonlar ve oltalama senaryolarıyla zenginleştirilerek öğretmenlere pratik deneyim kazandırması önerilebilir. Ayrıca, dijital okuryazarlık derslerinin öğretmenlerin mesleki gelişim programlarına entegre edilmesi ve bu kapsamda güvenli internet kullanımı, güçlü şifre oluşturma, veri koruma ve oltalama saldırılarını tanıma gibi konuların kapsamlı bir şekilde ele alınması, siber güvenlik farkındalığının artırılmasına önemli katkılar sağlayabilir.

Anahtar kelimeler: *Dijital dünya, siber güvenlik, siber tehdit, oltalama saldırıları, öğretmen farkındalığı.*

Atıf bilgisi: Genç, N. ve Yücel, M. (2025). Öğretmenlerin oltalama saldırılarına karşı farkındalık düzeyleri. *İstanbul Eğitim Dergisi,* (2), 83-104. https://doi.org/10.71270/istanbulegitim.istj.1660280

İntihal: *Bu makalenin benzerlik oranı intihal.net ile kontrol edilmiş olup incelemesi en az iki hakem tarafından çift taraflı kör hakemlik ilkesi ile gerçekleştirilmiştir.*

Istanbul Education Journal, 2025
Issue.2 Page.83-104
Research Article
doi.org/10.71270/istanbulegitim.istj.1660280

Teachers' Awareness Levels of Phishing Attacks

Neslihan Genc[1]*, Murat Yucel[2]

[1*]Corresponding author, Ministry of National Education, Dilek Sabancı Vocational and Technical Anatolian High School of Commerce, Istanbul, Türkiye neslihankgenc@gmail.com 0009-0002-8254-4783

[2]Gazi University, Department of Electrical and Electronics Engineering, Ankara, Türkiye 0000-0002-0349-4013

Date of Submission: 18/03/2025 *Date of Acceptance:16/06/2025*

Abstract

In today's digital world, where cybersecurity has become increasingly important, phishing attacks are one of the most common cyber threats used to obtain sensitive information and gain access to systems. These attacks, which are carried out using social engineering techniques, now target not only individuals but also all economic and social strata, from small businesses to multinational companies and local governments to critical state infrastructure. This research is a quantitative study based on a descriptive survey model, conducted to determine the awareness levels of teachers working at different levels (kindergarten, primary, secondary, high school) in official schools affiliated with the Ministry of National Education regarding phishing attacks. In this context, realistic phishing emails that teachers selected through snowball sampling might receive during their daily professional activities were designed, and their awareness levels and responses to such attacks were analysed using these emails. According to the research findings, it was revealed that even teachers in technical fields haven't had sufficient awareness of phishing attacks. These results show that teachers are vulnerable to cyber threats and that comprehensive training programmes are needed. In this case, it may be recommended that the relevant training programmes cover all teachers and that the training content be enriched with interactive simulations and phishing scenarios to provide teachers with practical experience. Additionally, integrating digital literacy courses into teachers' professional development programmes and comprehensively addressing topics such as safe internet use, strong password creation, data protection, and phishing attack recognition within this scope can significantly contribute to increasing cybersecurity awareness.

Keywords: *Digital world, cybersecurity, cyber threat, phishing attacks, phishing attacks, teacher awareness.*

Cite as: Genc, N., & Yucel, M. (2025). Teachers' awareness levels of phishing attacks. *Istanbul Education Journal,* (2), 83-104. https://doi.org/10.71270/istanbulegitim.istj.1660280

Giriş

Amerika Birleşik Devletleri Patent Ofisi Müdürü Charles H. Duell, 1899 yılında *"Artık yeni hiçbir şey yok. İcat edilebilecek her şey icat edildi."* dediğinde, insanlık teknolojik yeniliklerin sınırına ulaştığını düşünüyordu (Vikisöz, 2022). Ancak, bu tarihten sonra bilgisayar, internet ve dijital teknolojiler gibi birçok devrim niteliğinde icat geliştirilmiş ve modern yaşamı köklü bir şekilde dönüştürmüştür. Bilgisayarın icadı, bilginin dijitalleşmesini sağlayarak, sonraki teknolojik ilerlemelerin temelini oluşturmuştur. İnternetin keşfi ile birlikte bilgiye küresel ölçekte istenilen zamanda ve istenilen yerden ulaşmak mümkün hâle gelmiş, bu da bireylerin ve kurumların dijital bağımlılığını artırmıştır.

Dijitalleşmenin hızla ilerlemesiyle birlikte, siber güvenlik, bireyler ve kurumlar için kritik bir konu hâline gelmiştir. Oltalama saldırıları, siber tehditler arasında en yaygın olanlardan biri olup, özellikle insan unsurunu hedef alarak gerçekleştirilmektedir. Verizon'un 2023 Veri İhlali Araştırmaları Raporu'na göre, tüm siber ihlallerin %74'ü insan hatasından kaynaklanmaktadır ve saldırganların sisteme erişmek için en yaygın kullandıkları üç yöntem; çalıntı kimlik bilgileri, oltalama saldırıları ve sistem güvenlik açıklarının istismarıdır (Verizon, 2023). Benzer şekilde, Dünya Ekonomik Forumu'nun 2022 yılı raporunda, gerçekleşen siber güvenlik ihlallerinin %95'inin insan hatasından kaynaklandığı vurgulanmıştır (World Economic Forum [WEF], 2022).

Vade'nin 2023 yılı üçüncü çeyrek raporuna göre, oltalama saldırıları dünya genelinde %173 oranında artış göstermiştir. Rapora göre, ağustos ayında 207,3 milyon, eylül ayında 172,6 milyon ve temmuz ayında 113,4 milyon oltalama e-postası gönderilmiştir (Vade Secure, 2023). Bu durum, oltalama saldırılarının ne denli büyük bir tehdit oluşturduğunu ve saldırganların giderek daha fazla hedefe yöneldiğini göstermektedir.

Oltalama saldırıları, özellikle bireylerin ve kurumların karşı karşıya kaldığı en yaygın siber tehditlerdendir. Bu saldırılar, kullanıcıları güvenilir görünen sahte mesajlarla kandırarak kişisel bilgilerini ifşa etmelerini sağlar. Phishing olarak da bilinen bu saldırılar, şifreler, gizli veriler veya sistemlere erişim gibi kritik bilgileri elde etmeye yöneliktir. Günümüzde oltalama, birçok birey ve kuruluşu etkileyen, sürekli büyüyen bir siber suç türüdür (Ribeiro vd., 2024). Saldırılar genellikle, tanıdık bir kişi veya kuruluş gibi davranarak veya cazip teklifler sunarak hedefin dikkatini çeker. Sonuçlar, özellikle kurumsal hesaplar ele geçirildiğinde veya kredi kartı dolandırıcılığı gibi finansal kayıplar yaşandığında yıkıcı olabilir (Phishing.org, 2024; Rader ve Rahman, 2013).

Oltalama terimi, ilk kez Ocak 1996'da internet kayıtlarına geçmiş olup, bu saldırılar başlangıçta America Online (AOL) kullanıcılarını hedef alarak hesap bilgilerini ele geçirmeye yönelik sosyal mühendislik teknikleriyle gerçekleştirilmiştir (Phishing.org, 2024). 1996 yılından itibaren oltalama saldırıları giderek daha sofistike hâle gelmiş ve farklı yöntemlerle yaygınlaşmıştır. 2014 yılında yaşanan büyük ölçekli finansal kayıplar, bu saldırıların küresel ölçekte ciddi bir tehdit olarak kabul edilmesine neden olmuş, 2016'dan itibaren internet ve sosyal medyanın daha da yaygınlaşması, oltalama saldırılarının hızlı bir şekilde artmasına yol açarak siber tehdit ortamında kalıcı bir yükseliş trendine girmesine neden olmuştur (Goel ve Jain, 2018).

Oltalama saldırıları süreci genellikle keşif, hazırlık, dağıtım, eylem ve sömürü aşamalarından oluşur. Saldırgan, önce hedefi belirleyip bilgi toplar, sahte internet siteleri ve e-postalar hazırlar, bunları hedeflere gönderir ve kurbanın bilgilerini toplar (Abroshan vd., 2021; Korkmaz vd., 2021; Mohammad vd., 2015). Oltalama saldırıları farklı formlarda gerçekleşir. E-posta oltalaması, sesli oltalama, mızrak oltalama, balina avı, SMS oltalama ve sosyal medya oltalaması gibi çeşitleri bulunur (LivingSecurity, 2024). Bu saldırıların hepsi, kullanıcıları kandırarak hassas bilgilerini ele geçirmeyi amaçlar ve çeşitli sosyal mühendislik tekniklerini kullanır.

Oltalama saldırıları, finansal kayıpların ötesinde geniş çaplı ekonomik etkiler yaratır. Kişisel verilerin çalınması, finansal zararlar, itibar kaybı ve iş sürekliliğinin bozulması gibi olumsuz sonuçlara yol açar. Proofpoint'un raporuna göre, 2023 yılında organizasyonların %71'i en az bir başarılı oltalama saldırısına uğramıştır (Proofprint, 2024). Oltalama saldırılarının küresel çapta hızla yaygınlaşması, insanların hata yapma eğilimleri ve bilinç eksikliğiyle doğrudan ilişkilidir. Kurumlar için ciddi riskler oluşturan bu saldırılar, iç güvenlik önlemlerini aşarak siber savunma duvarlarını etkisiz hâle getirebilir. Teknik güvenlik önlemleri tek başına yeterli olmadığından, çalışanların siber güvenlik farkındalığını artırmak kritik önem taşımaktadır (Aldawood ve Skinner, 2019). Kurumlar, oltalama saldırılarını önlemek için farkındalık eğitimleri ve simülasyon testleri uygulamakta, özellikle özel sektör bu saldırılara karşı direnç oluşturmak için periyodik eğitimler düzenlemektedir (KnowBe4, 2023). 5681 organizasyonda, 12,5 milyon kullanıcı üzerinde yapılan bir çalışmada, kullanıcıların %33,1'inin şüpheli bağlantılara tıklama eğiliminde olduğu tespit edilmiş; ancak 90 günlük ve 12 aylık farkındalık eğitimleri sonrasında bu oranların önemli ölçüde azaldığı görülmüştür (KnowBe4, 2023). Bu durum, oltalama saldırılarıyla mücadelede teknik önlemlerin yanı sıra eğitim ve farkındalığın da büyük bir rol oynadığını ortaya koymaktadır.

Türkiye'de kamu kurum ve kuruluşlarında çalışanların bilgi güvenliği farkındalıklarının düşük olduğu çeşitli araştırmalarla ortaya konmuştur (Çakır ve Taşer, 2023; Kahriman, 2022). Eğitim sektöründe de benzer bir durum söz konusudur (Canoğulları, 2021; Sapanca ve Kanbul, 2022; Ateş ve Küçük, 2023). Öğretmenlerin bilgi güvenliği konusunda yeterli farkındalığa sahip olmamaları, eğitim ortamlarında çeşitli güvenlik açıklarına ve zafiyetlere yol açabilmekte; bu nedenle farkındalık düzeylerini artırmaya yönelik kapsamlı ve sürdürülebilir eğitim programlarının uygulanması gerekmektedir (Ateş ve Küçük, 2023).

Oltalama saldırılarına yönelik farkındalık, farklı bireylerin siber güvenlik davranışlarını anlama ve önleyici stratejiler geliştirme açısından önemli bir araştırma alanı hâline gelmiştir. Literatürde, farklı sektörlerde çalışan bireylerin bu tür saldırılara verdikleri tepkiler incelenmiş; simülasyonlar, eğitim müdahaleleri ve davranışsal modeller üzerinden çeşitli yaklaşımlar test edilmiştir. Örneğin, Mohebzada ve arkadaşları (2012) 10.000 üniversite çalışanı ve öğrencisi üzerinde yaptıkları simülasyonlarda, katılımcıların oltalama e-postalarını tanıma konusunda ciddi zorluklar yaşadığını ortaya koymuştur. Benzer şekilde, Kuzey Kentucky Üniversitesi'nde öğrencilerle yapılan bir çalışma, güvenlik eğitimlerinin kötü amaçlı bağlantılara tıklama oranlarını azalttığını, ancak bu etkinin eğitim yöntemine bağlı olarak değiştiğini göstermiştir (Carella vd., 2017). Malezya'da yürütülen bir çalışmada (Mustafa vd., 2019), meslek öğrencilerinin oltalama farkındalığını artırmak için tasarladıkları bir modelin etkinliğini test etmiştir. Çalışmada, öğrencilere ön test ve son test uygulanarak eğitim müdahalesinin bilgi düzeylerini anlamlı ölçüde artırdığı gösterilmiştir.

Sağlık sektöründe yapılan uzun vadeli bir araştırma, tekrarlanan oltalama simülasyonlarının çalışanların direncini artırdığını (Gordon vd., 2019; Rizzoni vd., 2022), ancak tıklama oranlarının hâla %14 gibi yüksek bir seviyede kaldığını vurgulamıştır (Gordon vd., 2019). Bu bulgular, kritik altyapıya sahip kurumlarda siber güvenlik eğitimlerinin sürekliliğinin önemini ortaya koymaktadır. İtalya'da bir şirkette yapılan çalışmada ise aciliyet vurgusu içeren e-postaların çalışanları daha savunmasız hâle getirdiği, demografik değişkenlerin ise sınırlı bir etkiye sahip olduğu belirlenmiştir (De Bona ve Paci, 2020).

Türkiye'deki araştırmalar, kamu kurumlarında çalışanların oltalama saldırılarına karşı düşük farkındalık düzeyine işaret etmektedir. Arslan (2021), 33000 çalışan üzerinde yapılan bir simülasyon çalışmasında, personelin sahte e-postaları tespit etme başarısının düşük olduğunu ve özellikle taşra birimlerindeki çalışanların daha yüksek risk altında bulunduğunu tespit etmiştir. Aslan (2022) ise sistematik

tatbikatlar ve düzenli eğitimlerin siber güvenlik farkındalığını artırdığını, ancak bu etkinin sürdürülebilir olması için kurumsal politikaların gerekliliğini vurgulamıştır.

Yeoh ve arkadaşları (2021) simüle oltalama saldırıları ile anlık geri bildirimli eğitim entegrasyonunu test etmiş, bu yaklaşımın şüpheli e-posta bildirimlerini artırdığını ve tıklama davranışını istatistiksel olarak anlamlı düzeyde azalttığını ortaya koymuştur. Operant koşullandırma temelli model, davranışsal geri bildirim mekanizmalarının siber güvenlik eğitimlerinde kritik rolünü kanıtlamıştır. Benzer şekilde, Tayland'da bir finans kuruluşunda yapılan çalışmada, üç aşamalı bir eğitim programının çalışan farkındalığını önemli ölçüde artırdığı ve kadın çalışanların erkeklere kıyasla daha yüksek performans sergilediği belirlenmiştir (Daengsi vd., 2021). Kişiselleştirilmiş saldırıların etkisini ele alan Hillman, Harel ve Toch (2023), İsrail'deki bir finans kuruluşunda 5000 çalışanla yaptıkları üç aşamalı simülasyonda, kişiselleştirilmiş e-postaların genel mesajlara göre istatistiksel olarak anlamlı daha yüksek tıklanma oranına ulaştığını göstermiştir. Çalışma, kurumların kişiye özgü sosyal mühendislik senaryolarına odaklanan eğitim modelleri geliştirmesi gerektiğini vurgulamaktadır.

Mevcut literatür incelendiğinde, eğitim sektöründeki öğretmenlerin bilgi güvenliği ve siber güvenlik farkındalıklarının genel olarak araştırıldığı; ancak oltalama saldırılarına karşı farkındalıklarını ölçen kapsamlı çalışmaların oldukça sınırlı olduğu görülmektedir (Ateş ve Küçük, 2023; Canoğulları, 2021; Mohebzada vd., 2019; Olsen ve Tokerud, 2020; Ravichandran vd., 2025; Sapanca ve Kanbul, 2022). Bu durum, yalnızca öğretmenlerin kişisel bilgi güvenliklerini değil, aynı zamanda öğrencilerin dijital güvenliğini de riske atabilir. Öğretmenlerin bu konuda yeterli farkındalığa sahip olmamaları, siber tehditlerin eğitim ortamlarında yayılma tehlikesini artırabilir, hem bireysel hem de kurumsal güvenlik açısından önemli bir açık oluşturabilir.

Bu araştırma, Türkiye'deki öğretmenlerin oltalama saldırılarına karşı farkındalıklarını belirlemeyi ve bu farkındalığın artırılmasına yönelik stratejiler geliştirmeyi amaçlamaktadır. Siber tehditlerin eğitim sektöründeki yaygınlığı giderek artmakta ve bu durum yalnızca öğretmenleri değil, öğrencileri de risk altına sokmaktadır. Öğretmenlerin siber güvenlik farkındalığının artırılması, öğrencilerin dijital güvenliğinin sağlanması açısından kritik bir öneme sahiptir. Elde edilecek bulguların, eğitim sektöründe uygulanabilir siber güvenlik politikalarının geliştirilmesine katkı sağlaması ve öğretmenlerin dijital tehditlere karşı daha dirençli hâle gelmesini desteklemesi beklenmektedir.

Araştırma, öğretmenlerin siber güvenlik farkındalıklarını ölçmek ve analiz etmek amacıyla, uygun bir senaryoya dayalı simüle edilmiş oltalama e-postaları kullanılarak gerçekleştirilmiştir. Bu simülasyon, öğretmenlerin oltalama tehditlerini tanıyabilme ve bu tehditlere karşı uygun yanıtlar verebilme becerilerini değerlendirmek için tasarlanmıştır. Katılımcılara gönderilecek sahte e-postalar aracılığıyla, öğretmenlerin siber saldırılara karşı nasıl tepki verdikleri ve hangi savunma stratejilerini benimsedikleri analiz edilecektir. Böylece, eğitim kurumlarının siber güvenlik önlemlerini güçlendirmek için etkili öneriler geliştirilmesine katkı sağlanacaktır. Bu çalışma, eğitim sektöründeki siber tehditlere karşı direnci artırmayı, öğretmenlerin bilinç düzeyini yükseltmeyi ve siber güvenlik eğitimleri ile politikalarının geliştirilmesine yönelik temel bir referans kaynağı oluşturmayı hedeflemektedir.

Araştırmada, *"Öğretmenlerin siber güvenlik ve özellikle oltalama saldırıları konusundaki farkındalıkları ne düzeydedir?"* sorusuna yanıt aranmıştır. Ayrıca, araştırmada ele alınan alt problemler şu şekildedir:

1.Öğretmenler, simüle edilmiş oltalama e-postalarını tanıma konusunda ne kadar yeteneklidir?

2.Farklı senaryolar altında öğretmenlerin siber tehditlere karşı tepkileri nasıl değişmektedir?

3.Siber güvenlik farkındalığının artırılması için öğretmenlere hangi tür eğitimlerin verilmesi gerekmektedir?

4.Öğretmenlerin siber güvenlik konusundaki bilgi ve becerilerini geliştirmek için hangi stratejik adımlar atılmalıdır?

Yöntem

Bu bölümde, araştırmanın yöntemi, çalışma grubu, veri toplama süreci ve analiz yöntemleri açıklanmaktadır.

Araştırmanın Modeli

Bu araştırma, öğretmenlerin siber güvenlik farkındalığını değerlendirmek amacıyla betimsel tarama modeline dayalı olarak gerçekleştirilmiş nicel bir çalışmadır. Araştırma kapsamında öğretmenlere gerçekçi ancak zararsız oltalama e-postaları gönderilmiş ve katılımcıların bu e-postaları açma, içindeki bağlantılara tıklama gibi davranışları sayısal verilere dönüştürülerek analiz edilmiştir. Elde edilen nicel veriler doğrultusunda, öğretmenlerin oltalama saldırılarına karşı farkındalıkları belirlenmiştir.

Çalışma Grubu

Araştırma grubunu, Türkiye Millî Eğitim Bakanlığı'na bağlı farklı kademelerde (anaokulu, ilkokul, ortaokul, lise) görev yapan öğretmenler oluşturmaktadır. Örneklem seçiminde, olasılıklı olmayan örneklem yöntemlerinden kartopu örnekleme yöntemi kullanılmıştır. Kartopu örneklemesi, ulaşılması zor popülasyonlara erişimi kolaylaştıran bir yöntem olup, özellikle belirli bir meslek grubu içinde yayılım sağlamak için tercih edilmiştir (Abreu, 2023). Bu yöntem, ulaşılması zor gruplara erişim sağlamak açısından avantaj sağlasa da, elde edilen bulguların genellenebilirliği açısından bazı sınırlılıklar barındırmaktadır.

Öğretmenlere ulaşmak için araştırmacının bağlı olduğu eğitim kurumundaki öğretmenlerden başlanarak, bu öğretmenler aracılığıyla sosyal medya ağları ve mesleki bağlantılar kullanılmıştır. Gönüllü katılım esasına dayalı olarak genişleyen öğretmen grubu sayesinde araştırmaya farklı illerden, özellikle İstanbul ağırlıklı olmak üzere toplam 230 öğretmen davet edilmiştir. Ancak, 33 (%14,35) öğretmen araştırmaya katılmayı reddetmiş ve çalışma 197 (%85,65) katılımcı ile gerçekleştirilmiştir.

Veri Toplama Araçları

Araştırma için veri toplama süreci Google Forms aracılığıyla yürütülmüştür. Katılımcılar, araştırma hakkında bilgilendirildikten sonra *"Bilgilendirilmiş Gönüllü Olur Formu"*nu onaylayarak çalışmaya dâhil edilmiştir. Katılımcıların görev yaptığı okul kademesi, branşı ve araştırmada kullanılacak e-posta adresleri toplanmıştır. Araştırma etik kurallar çerçevesinde gerçekleştirilmiştir.

Veri Toplama Süreci

Araştırma 13-15 Mayıs 2024 tarihleri arasında gerçekleştirilmiştir. Veri toplama süreci kapsamında, öğretmenlerin mesleki yaşamlarında karşılaşabilecekleri içeriklere benzer şekilde oltalama e-postaları hazırlanmıştır. E-posta metinleri, Millî Eğitim Bakanlığı'nın MEBBİS (Millî Eğitim Bakanlığı Bilişim Sistemleri) sistemi üzerinden duyurulan hizmet içi eğitim kursları temel alınarak düzenlenmiş ve öğretmenlerin dikkatini çekebilecek özgün başlıklar ve açıklamalarla yapılandırılmıştır. E-posta içerikleri, katılımcıların görev yaptıkları okul kademesi ve branş bilgilerine göre kişiselleştirilmiş ve içinde yer alan bağlantı, sahte bir başvuru sayfasına yönlendirme yapacak şekilde yapılandırılmıştır. Gerçek kurs bilgileri temel alınarak hazırlanan bu sahte e-postalar aracılığıyla öğretmenlerin farkındalıkları ölçülmüştür. Öğretmenlerin mesleklerine ve branşlarına uygun olarak tasarlanan oltalama e-postaları, toplanan e-posta adreslerine gönderilmiş

ve bu e-postaların takibi *Mailsuite* isimli uygulama ile yapılmıştır. *Mailsuite* ile gönderilen oltalama e-postalarının açılıp açılmadığı, kaç kez açıldığı, bağlantıya tıklanıp tıklanmadığı, tıklanma sayısı gibi sayısal veriler elde edilmiştir. Ancak yazılımın, e-postanın gelen kutusuna mı yoksa spam klasörüne mi düştüğünü belirleyememesi ve günlük sınırlı sayıda e-posta gönderimine izin vermesi, veri toplama sürecinde sınırlılık oluşturmuştur. E-posta içeriklerinin mobil cihazlarda farklı görünümler sergilemesi de analizlerde dikkate alınmıştır.

Gönderilen 197 oltalama e-postasından 196'sı katılımcılara ulaşmış ve bu e-postalardan 138'i (%70,4) açılmış, 58'i (%29,6) ise açılmamıştır. Çalışmanın bir sınırlılığı olarak, kullanılan takip aracı gönderilen e-postanın gelen kutusuna mı yoksa spam kutusuna mı düştüğünü belirleyememiştir. E-postayı açmayan katılımcıların, bilgi güvenliği farkındalıklarının yüksek olması, e-postanın spam kutusuna düşmesi ya da az kullanılan bir e-posta adresi olması gibi nedenlerle gözden kaçmış olabileceği düşünülmektedir.

Verilerin Analizi

Araştırmada, Google Forms üzerinden toplanan katılımcı bilgileri MS Excel'e aktarılmış ve Mailsuite uygulamasıyla elde edilen oltalama simülasyonu verileri bu tabloya entegre edilmiştir. Verilerin analizi IBM SPSS Version 29.0.1.0 programı kullanılarak gerçekleştirilmiştir. Öncelikle öğretmenlerin demografik bilgileri (okul düzeyi, branş) ve oltalama e-postalarına verdikleri tepkiler (e-postayı açma ve bağlantıya tıklama) betimsel istatistikler ile (frekans ve yüzde) incelenmiştir. Öğretmenlerin branşları ile e-posta açma davranışları ve bağlantıya tıklama davranışları, görev yaptıkları okul düzeyleri ile e-posta açma ve bağlantıya tıklama davranışları arasındaki ilişkiler ayrı ayrı $p<0.05$ anlamlılık düzeyinde Pearson Ki-Kare testi ile incelenmiştir. Ayrıca e-posta açma ve bağlantıya tıklama sayısal tekrarları da değerlendirilmiş ve bu davranışların ortalamaları hesaplanmıştır.

Bulgular

Bu bölümde, araştırmanın ana amaçları ve alt problemlerine ilişkin yapılan istatistiksel analizler ve bu analizlere dayalı yorumlar yer almaktadır.

Demografik Bulgular

Araştırmaya katılan 197 öğretmenin okul düzeyleri ve branşlarına ilişkin dağılım Tablo 1'de gösterilmektedir.

Tablo 1

Demografik istatistikler

	Değişken	***Kişi Sayısı***	***Yüzde***
Hangi okul düzeyinde görev yapıyorsunuz?	*Okul Öncesi*	*12*	*6.1*
	İlkokul	*40*	*20.3*
	Ortaokul	*39*	*19.8*
	Lise	*106*	*53.8*
Branşınız nedir?	*Almanca*	*2*	*1.0*
	Beden Eğitimi	*4*	*2.0*
	Bilgisayar Destekli Makine Ressamlığı	*1*	*0.5*
	Bilişim Teknolojileri	*51*	*25.9*
	Biyoloji	*1*	*0.5*
	Büro Yönetimi	*1*	*0.5*
	Coğrafya	*1*	*0.5*
	Din Kültürü ve Ahlak Bilgisi	*3*	*1.5*
	Elektrik	*1*	*0.5*
	Elektronik	*2*	*1.0*
	Felsefe	*3*	*1.5*
	Fen Bilimleri	*3*	*1.5*
	Fizik	*5*	*2.5*
	Görsel Sanatlar	*4*	*2.0*
	Hayvan Yetiştiriciliği ve Sağlığı	*1*	*0.5*
	İngilizce	*12*	*6.1*
	Kimya	*1*	*0.5*
	Matbaa Teknolojisi	*1*	*0.5*
	Matematik	*14*	*7.1*
	Meslek Dersleri	*1*	*0.5*
	Moda Tasarım	*1*	*0.5*
	Muhasebe ve Finansman	*7*	*3.6*
	Okul Öncesi	*12*	*6.1*
	Özel Eğitim	*3*	*1.5*
	Rehberlik	*9*	*4.6*
	Sağlık Hizmetleri	*1*	*0.5*
	Sınıf	*29*	*14.7*
	Sosyal Bilgiler	*2*	*1.0*
	Tarih	*7*	*3.6*
	Teknoloji ve Tasarım	*4*	*2.0*
	Türk Dili ve Edebiyatı	*5*	*2.5*
	Türkçe	*5*	*2.5*

Tablo 1 incelendiğinde araştırmaya onay veren 197 katılımcı öğretmen *"Hangi okul düzeyinde görev yapıyorsunuz?"* sorusunu yanıtlamış ve bu yanıtlara göre öğretmenlerin %6,1'i (12 kişi) okul öncesinde, %20,3'ü (40 kişi) ilkokulda, %19,8'i (39 kişi) ortaokulda ve %53,8'i (106 kişi) lisede görev yapmaktadır. Araştırmada

öğretmenlerin branş dağılımını belirlemek amacıyla yöneltilen *"Branşınız nedir?"* sorusuna verilen yanıtlar incelendiğinde, katılımcıların 32 farklı branştan geldiği görülmüştür. En fazla temsil edilen branşlar %25,9 ile Bilişim Teknolojileri, %14,7 ile Sınıf Öğretmenliği, %7,1 ile Matematik ve %6,1 ile İngilizce branşlarıdır. Bunun yanı sıra, Okul Öncesi ile Muhasebe ve Finansman branşlarından katılım oranları sırasıyla %6,1 ve %3,6 olarak belirlenmiştir. Diğer branşlardan gelen katılım oranları ise genellikle %2'nin altında kalmıştır.

Oltalama E-Postaları ile İlgili Bulgular

Araştırmada, katılımcılara gönderilen oltalama e-postalarının ulaşıp ulaşmadığı ve verdikleri tepkiler değerlendirilmiştir. Toplam 197 katılımcıya e-posta gönderilmiş, ancak 1 tanesi e-posta adresinin yanlış yazılması veya teknik nedenler sebebiyle adrese ulaşmadığı tespit edilmiştir (Tablo 2). Bu nedenle analizler, 196 katılımcı üzerinden yürütülmüştür.

Tablo 2

Oltalama e-postası ile ilgili bulgular

	Değişken	***Kişi sayısı***	***Yüzde***
Oltalama e-postasının katılımcıya gönderilme durumu	*E-posta gönderilmedi*	*1*	*0.5*
	E-posta gönderildi	*196*	*99.5*
Gönderilen oltalama e-postasının açılıp açılmama durumu	*E-posta açılmadı*	*58*	*29.6*
	E-posta açıldı	*138*	*70.4*
Gönderilen oltalama e-postasındaki bağlantıya tıklama durumu	*Bağlantıya tıklanmadı*	*27*	*19.6*
	Bağlantıya tıklandı	*111*	*80.4*

Tablo 2'de görüldüğü gibi katılımcıların e-posta açma oranları incelendiğinde, 196 kişiden 138'i (%70,4) e-postayı açarken, 58 kişi (%29,6) e-postayı açmamıştır. Yüksek açılma oranı, katılımcıların e-posta iletişimine duyarlı olduklarını ve gönderilen mesajları incelemeye eğilimli olduklarını göstermektedir. Ancak e-postaların açılmaması, spam klasörüne düşme ihtimali, katılımcıların şüphelenerek e-postayı açmama eğiliminde olmaları veya yoğunluk nedeniyle fark etmemelerinden kaynaklanıyor olabilir.

E-postayı açan 138 katılımcının oltalama e-postası içindeki bağlantıya tıklama davranışları incelendiğinde, 111 katılımcı (%80,4) bağlantıya tıklamış, 27 katılımcı (%19,6) ise bağlantıya tıklamamıştır (Tablo 2). Bağlantıya tıklayan oranının yüksek olması, katılımcıların oltalama saldırılarına karşı yeterince farkındalık sahibi olmadığını ve dikkatli davranmadıklarını göstermektedir. Bağlantıya tıklamayan 27

kişinin, oltalama saldırıları hakkında bilgi sahibi olmaları ve bilinçli bir şekilde bağlantıya tıklamaktan kaçınmaları olasıdır. Ancak, bu kişilerin tam olarak neden bağlantıya tıklamadıkları net olarak belirlenememektedir.

Araştırmaya 32 farklı branştan öğretmenler katılmış ve sadece 4 branşta bulunan öğretmenler gönderilen oltalama e-postasını açmamıştır. Ancak, bu 4 branşın her birinden sadece 1 öğretmenin katılım gösterdiği görülmektedir. Branşlara göre yapılan çapraz tablo analizinde, belirli branşlardaki öğretmenlerin e-postaları açma oranlarının diğer branşlara göre daha yüksek olduğu görülmüştür. Bilişim Teknolojileri öğretmenlerinin %72,55'inin (51 öğretmenden 37'si), Matematik öğretmenlerinin %78,57'sinin (14 öğretmenden 11'i) e-postayı açtığı tespit edilmiştir. Rehberlik öğretmenleri ise %100 oranında e-postalarını açmıştır (9/9). Sınıf öğretmenleri %57,1 oranında (28 öğretmenden 16'sı) e-postayı açarken, diğer branşlardan katılım düşük olmakla birlikte genel olarak e-posta açma oranları yüksektir.

Tablo 3

Branşlara göre oltalama e-postasının açılma durumunun ki-kare testi analizi

	Değer	***Serbestlik derecesi***	***Asimtotik önem (2 taraflı)***
Pearson Ki-Kare	*42.666[a]*	*31*	*0.079*
Geçerli vaka sayısı	*196*		

a. *56 hücrede (%87,5) beklenen sayı 5'ten azdır. Minimum beklenen sayı 0,30'dur.*

Yapılan Ki-kare testi ile branş ile e-posta açma davranışı arasındaki istatistiksel ilişki incelenmiş ve Pearson Ki-Kare değeri 42.666, serbestlik derecesi 31 ve p-değeri 0.079 olarak hesaplanmıştır (Tablo 3). Bu sonuçlara göre 0.05 anlamlılık düzeyine göre öğretmenlerin branşları ile e-posta açma davranışları arasında anlamlı bir ilişki olmadığı belirlenmiştir.

Öğretmenlerin görev yaptıkları okul düzeyine göre e-posta açma davranışları incelendiğinde, lise öğretmenleri %69,81, okul öncesi öğretmenleri %75, ortaokul öğretmenleri %74,36 ve ilkokul öğretmenleri %66,67 oranında gönderilen oltalama e-postalarını açmıştır.

Tablo 4

Okul düzeylerine göre oltalama e-postasının açılma durumunun ki-kare testi analizi

	Değer	***Serbestlik Derecesi***	***Asimtotik Önem (2 taraflı)***
Pearson Ki-Kare	*0.694[a]*	*3*	*0.875*
Geçerli Vaka Sayısı	*196*		

a. *1 hücrede (%12,5) beklenen sayı 5'ten azdır. Minimum beklenen sayı 3,55'tir.*

Bu değişkenler arasındaki ilişkiyi belirlemek için yapılan Ki-kare testinde, Pearson Ki-Kare değeri 0.694, serbestlik derecesi 3 ve p-değeri 0.875 olarak hesaplanmıştır (Tablo 4). Bu sonuçlara göre, öğretmenlerin görev yaptığı okul düzeyleri ile e-posta açma davranışları arasında anlamlı bir ilişki bulunmamaktadır.

E-postayı açan öğretmenlerin e-posta içindeki bağlantıya tıklama davranışları branşlara göre incelendiğinde, Bilişim Teknolojileri öğretmenlerinin %83,78'inin (37 öğretmenden 31'i), Matematik ve İngilizce öğretmenlerinin %90,9'unun (11 öğretmenden 10'u), Sınıf öğretmenlerinin %68,75'inin (16 öğretmenden 11'i) bağlantıya tıkladığı görülmüştür.

Tablo 5

Branşlara göre oltalama e-postasındaki bağlantıya tıklama durumunun ki-kare testi analizi

	Değer	***Serbestlik derecesi***	***Asimtotik önem (2 taraflı)***
Pearson Ki-Kare	*33.334[a]*	*26*	*0.153*
Geçerli vaka sayısı	*138*		

a. *47 hücrede (%87) beklenen sayı 5'ten azdır. Minimum beklenen sayı 0,20'dir.*

Yapılan Ki-kare testi ile branş ile bağlantıya tıklama davranışı arasındaki ilişki değerlendirilmiş ve Pearson Ki-Kare değeri 33.334, serbestlik derecesi 26 ve p-değeri 0,153 olarak hesaplanmıştır (Tablo 5). Bu sonuçlara göre, branş ile bağlantıya tıklama davranışı arasında istatistiksel olarak anlamlı bir ilişki bulunmamaktadır.

Görev yapılan okul düzeyine göre bağlantıya tıklama oranları okul öncesi öğretmenlerinde %100, lise öğretmenlerinde %83,78, ilkokul öğretmenlerinde %76,92 ve ortaokul öğretmenlerinde %68,97 olarak hesaplanmıştır.

Tablo 6

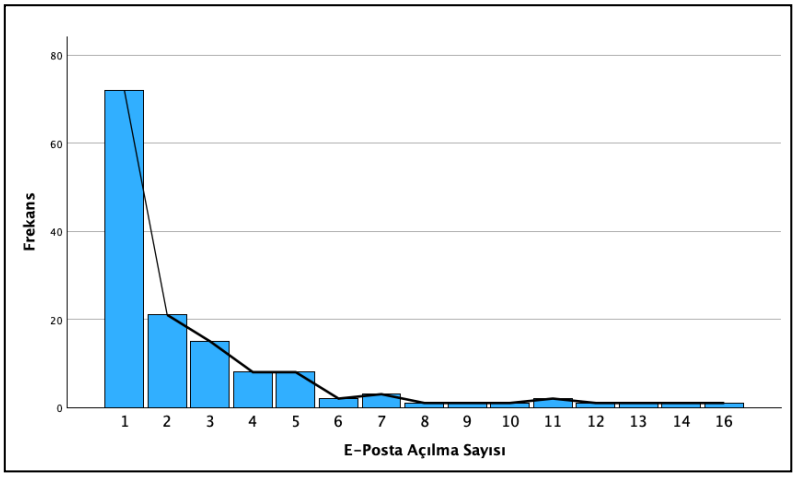
Okul düzeylerine göre oltalama e-postasındaki bağlantıya tıklama durumunun ki-kare testi analizi

	Değer	***Serbestlik derecesi***	***Asimtotik Önem (2 taraflı)***
Pearson Ki-Kare	*5.344[a]*	*3*	*0.148*
Geçerli Vaka Sayısı	*138*		

a. 1 hücrede (%12,5) beklenen sayı 5'ten azdır. Minimum beklenen sayı 1,76'dır.

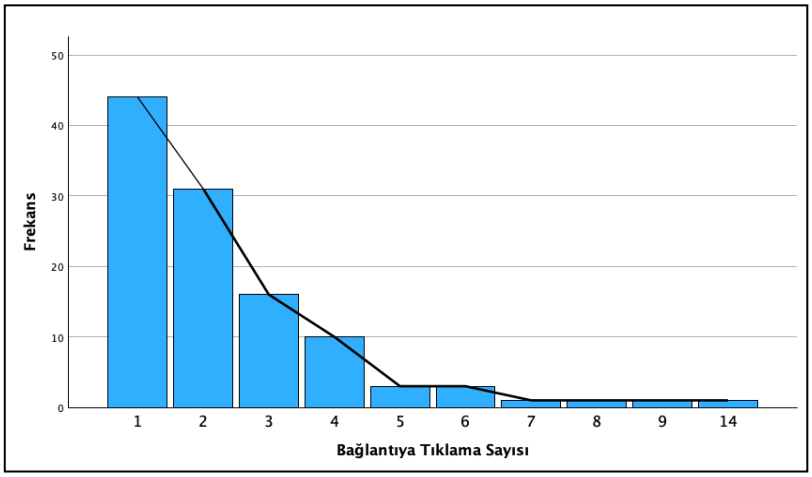
Bağlantıya tıklama davranışı ile öğretmenlerin görev yaptığı okul düzeyi arasındaki ilişkiyi inceleyen Ki-kare testinde, Pearson Ki-Kare değeri 5.344, serbestlik derecesi 3 ve p-değeri 0.148 olarak hesaplanmıştır (Tablo 6). Bu sonuçlara göre, okul düzeyi ile bağlantıya tıklama davranışı arasında istatistiksel olarak anlamlı bir ilişki bulunmamaktadır.

Yapılan Ki-kare analizlerinde örneklem büyüklüğünün bazı kategorilerde düşük olması, sonuçların güvenirliği üzerinde etkili olabilecek bir faktör olarak değerlendirilebilir.



Şekil 1. *Gönderilen oltalama e-postasının açılma sayısının grafiği*

E-posta açma ve bağlantıya tıklama sayıları açısından yapılan analizler, katılımcıların önemli bir kısmının gönderilen oltalama e-postalarını tekrar tekrar açtığını ve oltalama e-postasındaki bağlantıya birden fazla kez tıkladığını ortaya koymuştur. E-posta açma sayılarının ortalaması 2.67 olup, katılımcılardan oltalama e-postasını 16 defa açtığı görülmüştür (Şekil 1). Bu durum, kullanıcıların gelen e-postaları tekrar gözden geçirdiğini, içeriği doğrulamaya çalıştığını veya içeriği daha dikkatli incelediğini gösterebilir.



Şekil 2. *Gönderilen oltalama e-postasındaki bağlantıya tıklanma sayısının grafiği*

Öte yandan, Şekil 2'de görüldüğü gibi bağlantıya tıklama ortalaması 2.39 olup, bazı katılımcıların bağlantıya 14 defaya kadar tıkladığı belirlenmiştir. Bu durum, kullanıcıların bağlantıyı açtıktan sonra tekrar tekrar tıklayarak içeriği doğrulamaya veya işlem yapmaya çalıştıklarını gösterebilir. Ancak bu aynı zamanda, oltalama saldırılarına karşı katılımcıların yeterince şüpheci yaklaşmadıklarını ve bilinçsiz bir şekilde bağlantılara tıklamaya eğilimli olduklarını da göstermektedir.

Tartışma, Sonuç ve Öneriler

Bu araştırma, öğretmenlerin oltalama saldırılarına karşı farkındalıklarını belirlemek amacıyla gerçekleştirilmiş ve önemli sonuçlar elde edilmiştir. Türkiye'deki resmî kurumlarda görev yapan öğretmenlerin siber güvenlik farkındalıklarını ve reaksiyonlarını simüle edilmiş oltalama e-postaları aracılığıyla analiz ederek öğretmenlerin siber güvenlik konusundaki bilinç ve becerilerini geliştirmek için

öneriler sunulmuş ve eğitim sektöründe siber tehditlere karşı daha dirençli bir yapı oluşturulması gerekliliğini ortaya çıkarılmıştır.

Araştırmanın doğası gereği hedeflenen katılımcı sayısına ulaşmak bazı zorluklar içermiştir. Ancak, araştırmaya katılmayı kabul eden 197 öğretmen, farklı okul düzeylerinde görev yapan ve 32 farklı branşa mensup katılımcılardan oluşmaktadır. Katılım oranları incelendiğinde, en fazla katılımın %53,8 ile lise düzeyindeki öğretmenlerden geldiği görülmektedir. Branş bazında değerlendirildiğinde, en yüksek katılım %25,9 ile Bilişim Teknolojileri öğretmenlerinden, %14,7 ile ise Sınıf öğretmenlerinden olmuştur. Katılımcıların geniş bir branş yelpazesinden gelmesi araştırmanın kapsamını artırsa da, bazı branşlardan yalnızca bir katılımcının yer alması, bazı kategorilerde temsiliyetin sınırlı kaldığını göstermektedir.

Araştırma sonucunda, branş ve okul düzeyleri ile e-posta açma ya da bağlantıya tıklama davranışı arasında anlamlı bir ilişki bulunamamıştır. Bu durum, öğretmenlerin siber güvenlik farkındalığının branştan ya da okul düzeyinden bağımsız olduğunu göstermektedir. Özellikle Bilişim Teknolojileri öğretmenleri arasında bile oltalama saldırılarına yönelik düşük farkındalık düzeyinin gözlemlenmesi, eğitim sektörü genelinde siber güvenlik konusunda ciddi bir eksikliğin varlığını göstermektedir. Bu bulgular, Mohebzada vd. (2012), Gordon vd. (2019) ve Rizzoni vd. (2022) gibi çalışmalarda da benzer şekilde gözlemlenmiş; meslek ve eğitim düzeyi fark etmeksizin, bireylerin oltalama saldırılarına karşı yüksek oranda duyarsız kaldığı raporlanmıştır.

Özellikle, e-posta açma ve bağlantıya tıklama oranlarının yüksek olması, öğretmenlerin siber tehditlere karşı savunmasız olduğunu göstermektedir. Bu durum, eğitim sektöründeki güvenlik açıklarının giderilmesi için kapsamlı siber güvenlik eğitimlerine ve farkındalık programlarına duyulan ihtiyacı ortaya koymaktadır. Örneklem büyüklüğünün sınırlı olması sonuçların genellenebilirliğini kısıtlasa da elde edilen veriler, eğitim politikalarının güncellenmesi ve öğretmenlerin siber tehditlere karşı bilinçlendirilmesinin gerekliliğini vurgulamaktadır. Literatürde de benzer şekilde, hem eğitimciler hem de farklı sektör çalışanları üzerinde yapılan çalışmalarda oltalama saldırılarına karşı savunmasızlık düzeylerinin yüksek olduğu ve eğitim müdahalelerinin bu farkındalığı artırmada etkili olduğu görülmektedir (Mohebzada vd., 2012; Gordon vd., 2019; Carella vd., 2017; Hillman vd., 2023; Yeoh vd., 2021).

Mohebzada vd. (2012), üniversite çalışanları ve öğrencilerle gerçekleştirdikleri çalışmada, eğitim ya da branş farkı gözetmeksizin katılımcıların oltalama e-

postalarına karşı savunmasız olduğunu ortaya koymuştur. Benzer şekilde, Gordon vd. (2019) sağlık sektöründe görev yapan personel üzerinde yaptıkları simülasyon çalışmasında yüksek tıklama oranları tespit etmiş ve demografik değişkenlerin oltalama farkındalığı üzerinde sınırlı etkisi olduğunu bildirmiştir. Carella vd. (2017) ise güvenlik farkındalığı eğitimi almayan bireylerin kötü niyetli bağlantılara tıklama olasılıklarının daha yüksek olduğunu saptamış; bu da eğitim müdahalelerinin önemini vurgulamaktadır. Mustafa vd. (2019) meslek lisesi öğrencileri ile gerçekleştirdikleri model geliştirme çalışmasında farkındalık eğitiminin etkinliğini doğrulamıştır. Ek olarak, Hillman vd. (2023) ve Yeoh vd. (2022) tarafından yapılan çalışmalar, tekrarlayan oltalama simülasyonlarının ve gömülü eğitimlerin, uzun vadeli farkındalık gelişimi açısından etkili bir yöntem olduğunu göstermektedir.

Bu bağlamda, öğretmenlere yönelik sürdürülebilir ve kapsayıcı siber güvenlik eğitimlerinin planlanması, dijital güvenlik tehditlerinin azaltılmasında stratejik bir gereklilik olarak değerlendirilmektedir. Gerek literatürdeki mevcut bulgular gerekse bu araştırmadan elde edilen sonuçlar, eğitim kurumlarında bilgi güvenliği farkındalığını artırmaya yönelik bütüncül yaklaşımların benimsenmesi gerektiğini açıkça ortaya koymaktadır.

Türkiye'de de bazı özel ya da kamu kurum/kuruluşlarında oltalama simülasyon çalışmaları gerçekleştirilmiştir (Arslan, 2021; Aslan, 2022). Örneğin, Arslan (2021) tarafından yapılan geniş ölçekli bir çalışmada, kamu kurumlarında görevli çalışanların özellikle taşra birimlerinde oltalama saldırılarına karşı daha düşük farkındalık düzeyine sahip olduğu belirlenmiş; Aslan'ın (2022) çalışmasında ise sistematik biçimde uygulanan eğitim, tatbikat ve bilgilendirme faaliyetlerinin farkındalığı artırmada etkili olduğu ortaya konmuştur. Ancak öğretmenleri kapsayan kapsamlı bir oltalama simülasyonu çalışması literatürde rastlanmamıştır. Bu çalışma, eğitim sektöründeki öğretmenlerin oltalama saldırılarına farkındalığını ölçen ilk çalışma olma özelliğini taşımakta ve eğitim kurumlarında siber güvenlik farkındalığını artırmaya yönelik önemli bir katkı sunmayı hedeflemektedir.

Elde edilen bulgular doğrultusunda, öğretmenlerin oltalama saldırılarına karşı farkındalıklarının artırılması için çeşitli stratejik öneriler sunulmuştur. Öncelikle, öğretmenlere yönelik düzenli ve kapsamlı siber güvenlik eğitim programları oluşturulmalıdır. Bu eğitimler, yalnızca Bilişim Teknolojileri öğretmenleriyle sınırlı kalmamalı, tüm branşları kapsayacak şekilde genişletilmelidir. Eğitim içerikleri, interaktif simülasyonlar ve gerçekçi oltalama senaryoları ile desteklenerek öğretmenlerin pratik deneyim kazanması sağlanmalıdır. Ayrıca, öğretmenlerin

siber güvenlik farkındalığını sürekli artırmak amacıyla, okullarda periyodik olarak farkındalık kampanyaları düzenlenmeli, afişler, broşürler, e-posta bilgilendirmeleri ve video içerikleri gibi çeşitli materyallerle desteklenmelidir.

Bununla birlikte, öğretmenlerin siber saldırılara karşı reflekslerini ölçmek ve geliştirmek için düzenli oltalama simülasyonları yapılmalı ve bu simülasyonların sonuçlarına göre öğretmenlere bireysel geri bildirim sağlanmalıdır. Dijital okuryazarlık dersleri, öğretmenlerin mesleki gelişim programlarına entegre edilmeli ve güvenli internet kullanımı, güçlü şifre oluşturma, veri koruma ve oltalama saldırılarını tanıma gibi konular kapsamlı bir şekilde işlenmelidir. Siber güvenlik konusunda daha etkin bir eğitim altyapısı oluşturulması için Millî Eğitim Bakanlığı, üniversiteler ve siber güvenlik alanında uzman kuruluşlarla iş birliği yaparak, öğretmenlere yönelik güncel ve kaliteli eğitim materyalleri sunmalıdır.

Ayrıca, okullarda kullanılan teknolojik altyapının güçlendirilmesi, güncel güvenlik yazılımlarının kullanımı ve düzenli sistem güncellemelerinin yapılması, siber tehditlere karşı koruma sağlamak için kritik öneme sahiptir. Öğretmenlerin kişisel e-posta hesapları yerine, Millî Eğitim Bakanlığı tarafından sağlanan kurumsal e-posta hesaplarını kullanmaları teşvik edilmeli ve bu hesaplar üzerinden düzenli farkındalık çalışmaları yürütülmelidir. Son olarak, öğretmenlerin siber güvenlik konusundaki geri bildirimleri düzenli olarak toplanmalı ve eğitim programları bu geri bildirimler doğrultusunda sürekli olarak güncellenmelidir.

Bu öneriler, eğitim sektöründe siber güvenlik farkındalığını artırmaya yönelik stratejik adımlar sunmaktadır. Eğitim politikalarının güncellenmesi ve öğretmenlerin bilinçlendirilmesi, eğitim sektöründe siber güvenliği sağlamak için kritik öneme sahiptir.

Etik Beyan

Bu çalışma, Prof. Dr. Murat Yücel danışmanlığında tamamladığımız *"Öğretmenlerin Oltalama Saldırıları Farkındalıklarının Araştırılması"* başlıklı yüksek lisans tezi esas alınarak hazırlanmıştır (Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara, Türkiye, 2024). Bu araştırmanın bütün aşamalarında (hazırlık, literatür taraması, veri toplama, veri analizi, sunum) bilimsel etik, ilke ve kurallara uygun davrandığımızı; bu çalışma kapsamında yararlanılan eserlerin tamamına kaynakçada yer verdiğimizi; verileri kullanırken veriler üzerinde bir değişiklik yapmadığımızı; araştırmanın intihal içermediğini; Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesi ile Yayın Etiği Komitesi (COPE) İlkelerinin tüm şartlarını ve koşullarını kabul ederek etik görev ve sorumluluklara

riayet ettiğimizi; araştırmamızla ilgili burada yazılı olan ifadelerimize aykırı herhangi bir durumun saptanması durumunda ortaya çıkabilecek ahlaki ve hukuki bütün sonuçları kabul edeceğimizi beyan ederiz. Ayrıca araştırmamızda *ChatGPT* adlı yapay zekâ uygulamasını dil düzenleme ve çeviri kontrolü yapmak amacıyla yukarıda belirttiğimiz etik yönerge ve ilkelerini takip ederek kullandığımızı beyan ederiz.

Etik Kurul Onayı

"*Öğretmenlerin Oltalama Saldırılarına Karşı Farkındalık Düzeyleri*" başlıklı çalışmanın verileri, Gazi Üniversitesi Rektörlüğü Etik Komisyonu'nun 12.12.2023 tarihli ve E-77082166-302.08.01-819251 sayılı etik onayı alındıktan sonra toplanmıştır.

Çıkar Çatışması Beyanı

"Öğretmenlerin Oltalama Saldırılarına Karşı Farkındalık Düzeyleri" başlıklı çalışmanın hiçbir şahıs, kurum ve kuruluş ile bir çıkar çatışması bulunmadığı gibi yazarlar arasında da bir çıkar çatışması yoktur.

Yazar Katkı Beyanı

"Öğretmenlerin Oltalama Saldırılarına Karşı Farkındalık Düzeyleri" başlıklı çalışmanın yazarları olarak katkı oranlarının aşağıda belirtildiği gibi olduğunu beyan ederiz.

1. Fikir/Kavram (Araştırma için fikir ya da hipotezin oluşturulması)
2. Tasarım/Dizayn (Araştırma sonucuna ulaşmak için yöntemin planlanması)
3. Denetleme/Danışmanlık (Araştırmanın organizasyonu ve seyrinin gözetimi için sorumluluk alınması)
4. Kaynaklar (Araştırma için personel, katılımcı, mekân, finansal kaynak, araç gereç sağlanması)
5. Malzemeler (Araştırma için malzeme temin edilmesi)
6. Veri Toplama/İşleme (Araştırma verisinin toplanması ve verinin işlenmesi)
7. Analiz/Yorum (Verinin analiz edilmesi ve yorumlanması)
8. Literatür Taraması (literatür taraması için sorumluluk alınması)
9. Makale Yazımı (Araştırmanın tümü veya asıl bölümünün yazımı için sorumluluk alınması)
10. Eleştirel İnceleme (Araştırmayı teslim etmeden önce sadece imlâ ve dil bilgisi açısından değil, aynı zamanda entelektüel ve akademik içerik açısından araştırma üzerinde eleştirel inceleme yapılması)

Tablo 7
Yazar katkı beyanı

Katkı veren yazar	***Katkı türü ve katkı oranı***
Neslihan Genç	*1-3-10 %70, 2-4-5-6-7-8-9 %100*
Murat Yücel	*1-3-10 %30*

Destek ve Teşekkür Beyanı

"*Öğretmenlerin Oltalama Saldırılarına Karşı Farkındalık Düzeyleri*" başlıklı çalışma için herhangi bir destek ve teşekkür beyanımız bulunmamaktadır.

Kaynakça

Abreu, G. (2023). Snowball sampling: Unveiling the secrets of a powerful research tool. Mind the GRAPH. https://mindthegraph.com/blog/snowball-sampling/ adresinden 10 Nisan 2024 tarihinde alınmıştır.

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access, 9,* 44928–44949. http://doi.org/10.1109/access.2021.3066383

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet, 11*(3), 73. https://doi.org/10.3390/fi11030073

Arslan, Y. (2021). Oltalama saldırıları farkındalık tatbikatı örneği. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 9(3),* 348-358. https://doi.org/10.29130/dubited.832862

Aslan, M. (2022). Maintaining cybersecurity awareness in large-scale organizations: A pilot study in a public institution [Yayımlanmamış yüksek lisans tezi]. Çankaya Üniversitesi.

Ateş, S. ve Küçük, S. (2023). Öğretmenlerin bilgi güvenliği farkındalık ve dijital okuryazarlık durumlarının incelenmesi. *Necmettin Erbakan Üniversitesi Ereğli Eğitim Fakültesi Dergisi, 5*(2), 491–534. https://doi.org/10.51119/ereegf.2023.66

Çakır, H. ve Taşer, M. (2023). Türkiye'de yapılan siber güvenlik faaliyetlerinin ve eğitim çalışmalarının değerlendirilmesi. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, 11*(2), 347-366. https://doi.org/10.29109/gujsc.1165131

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi, 11*(2), 651–679.https://doi.org/10.23863/kalem.2021.219

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *2017 IEEE International Conference on Big Data (Big Data),* 4458–4466. https://doi.org/10.1109/BigData.2017.8258485

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies, 27*(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

De Bona, M., & Paci, F. (2020). A real world study on employees' susceptibility to phishing attacks. *Proceedings of the 15th International Conference on Availability, Reliability and Security, 4*, 1-10. https://doi.org/10.1145/3407023.3409179

Goel, D., & Jain, A.K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Comput. Secur, 73*, 519-544. https://doi.org/10.1016/j.cose.2017.12.006

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Network Open, 2(3),* e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security, 132,* 103364. https://doi.org/10.1016/j.cose.2023.103364

Kahriman, Y. (2022). *Türkiye'de siber güvenlik alanında yapılan tezlerin incelenmesi: Bibliyografik bir çalışma* [Yayımlanmamış yüksek Lisans tezi]. Necmettin Erbakan Üniversitesi.

KnowBe4. (2023). *Phishing by industry benchmarking report 2023*. https://www.knowbe4.com/hubfs/2023-Phishing-by-Industry-Benchmarking-Report-Research-EN_US.pdf adresinden 10 Nisan 2024 tarihinde alınmıştır.

Korkmaz, M., Kocyigit, E., Sahingoz, O. K., & Diri, B. (2021). Deep neural network based phishing classification on a high-risk url dataset. *Advances in Intelligent Systems and Computing,* 648–657. https://doi.org/10.1007/978-3-030-73689-7_62

LivingSecurity. (2024). *Recent phishing attacks: How they were executed and what we can learn*. https://www.livingsecurity.com/blog/recent-phishing-attacks-and-lessons adresinden 10 Nisan 2024 tarihinde alınmıştır.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review, 17,* 1–24. https://doi.org/10.1016/j.cosrev.2015.04.001

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *2012 International Conference on Innovations in Information Technology (IIT),* 249-254. https://doi.org/10.1109/innovations.2012.6207742

Mustafa, M. S. B. O., Kabir, M. N., Ernawan, F., & Jing, W. (2019). An enhanced model for increasing awareness of vocational students against phishing attacks. *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS),* 10-14. https://doi.org/10.1109/i2cacis.2019.8825070

Olsen, R. V., & Tokerud, S. (2020). *Teachers' information security awareness: A qualitative study of primary and lower secondary school teachers in Kristiansand and Vennesla municipalities* [Master's thesis]. University of Agder.

Phishing.org. (2024). *History of phishing*. https://www.phishing.org/history-of-phishing adresinden 27 Şubat 2024 tarihinde alınmıştır.

Proofprint. (2024). *State of the phish 2024*. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf adresinden 27 Şubat 2024 tarihinde alınmıştır.

Rader, M. A., & Rahman, S. S. (2013). Phishing techniques and mitigating the associated security risks. *International Journal of Network Security & Its Applications, 5*(4), 23–41. https://doi.org/10.5121/ijnsa.2013.5402

Ravichandran, R., Singh, S., & Sasikala, P. (2025). Exploring school teachers' cyber security awareness, experiences, and practices in the digital age. *Journal of Cybersecurity Education, Research and Practice, 1,* 1-27. https://doi.org/10.62915/2472-2707.1214

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security, 136*, 103558. https://doi.org/10.1016/j.cose.2023.103558

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health, 8*. https://doi.org/10.1177/20552076221081716

Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. *Frontiers in Psychology, 13*, Article 986561. https://doi.org/10.3389/fpsyg.2022.986561

Vade Secure. (2023). *Phishing and malware report*. https://www.vadesecure.com/hubfs/Ressource%20Marketing%20Website/Report/Q3%202023%20Phishing%20and%20Malware%20Report-EN.pdf adresinden 27 Şubat 2024 tarihinde alınmıştır.

Verizon. (2023). *Data breach investigations report*. https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf adresinden 27 Şubat 2024 tarihinde alınmıştır.

Vikisöz. (2022). Charles Duell. https://tr.wikiquote.org/wiki/Charles_Duell adresinden 12 Aralık 2023 tarihinde alınmıştır.

World Economic Forum (WEF) (2022). *Global risks report 2022*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf adresinden 12 Aralık 2023 tarihinde alınmıştır.

Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2021). Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems, 62*(4), 802–821. https://doi.org/10.1080/08874417.2021.1919941