
GAZİ ÜNİVERSİTESİ
Gazi
1926

ÖĞRETMENLERİN OLTALAMA SALDIRILARI FARKINDALIKLARININ ARAŞTIRILMASI

Neslihan GENÇ

YÜKSEK LİSANS TEZİ
ELEKTRONİK-BİLGİSAYAR EĞİTİMİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2024

Neslihan GENÇ tarafından hazırlanan "ÖĞRETMENLERİN OLTALAMA SALDIRILARI FARKINDALIĞININ ARAŞTIRILMASI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Elektronik-Bilgisayar Eğitimi Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Murat YÜCEL

Elektronik Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum**.** ...……

Başkan: Doç. Dr. Hüseyin POLAT

Bilgisayar Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……..

Üye: Dr. Öğr. Üyesi Muhammed Mutlu YAPICI

Bilgisayar Programcılığı, Ankara Üniversitesi, Elmadağ MYO

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……..

Tez Savunma Tarihi: 24/06/2024

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

…….…….

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Neslihan GENÇ

24/06/2024

ÖĞRETMENLERİN OLTALAMA SALDIRILARI FARKINDALIKLARININ ARAŞTIRILMASI

(Yüksek Lisans Tezi)

Neslihan GENÇ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2024

ÖZET

Siber güvenliğin önem kazandığı bugünün dijital dünyasında hassas bilgileri ele geçirmek, finansal kazanç sağlamak, sistemlere erişim sağlamak gibi amaçlarla gerçekleştirilen siber saldırıların başında oltalama (phishing) saldırıları gelmektedir. Sosyal mühendislik tekniklerini kullanarak gerçekleştirilen bu saldırılar, küresel çapta bireylerden, küçük işletmelere, büyük çaplı firmalardan devlet kurumlarına kadar her kesimi etkilemektedir. Bu tez çalışmasında Türkiye'deki resmî eğitim kurumlarında çalışan öğretmenlerin oltalama saldırılarına yönelik farkındalığının ne düzeyde olduğunun araştırılması amaçlanmaktadır. Siber güvenlik tehditlerinin giderek arttığı günümüz koşullarında, öğretmenlerin kendi bilgi güvenliklerini sağlamak ve öğrencilere rehberlik edebilmek adına, bu tür saldırılara karşı bilinçli ve hazırlıklı olmaları bir zorunluluktur. Araştırmada, gerçekçi ancak zararsız oltalama e-postaları kullanarak öğretmenlerin bu tür saldırılara karşı farkındalık düzeyleri ve verdikleri tepkiler analiz edilmiştir. Türkiye genelinden 197 öğretmenin gönüllü katıldığı araştırmada, katılımcıların %76'sının gönderilen oltalama e- postalarını açtığı, e-postayı açanların %80,4'ünün ise içerikteki sahte bağlantıya tıkladığı tespit edilmiştir. Bu yüksek oranlar, öğretmenlerin oltalama saldırılarına karşı düşük farkındalığa sahip olduğunu göstermektedir. Bu çalışma, eğitim sektörünün siber tehditlere karşı daha dirençli hale gelmesine yardımcı olacak bir rehber niteliğindedir.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Siber güvenlik, oltalama saldırıları, sosyal mühendislik, siber saldırı, bilgi güvenliği
Sayfa Adedi	:	86
Danışman	:	Prof. Dr. Murat YÜCEL

RESEARCHING TEACHERS' AWARENESS OF PHISHING ATTACKS

(M. Sc. Thesis)

Neslihan GENÇ

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

June 2024

ABSTRACT

In today's digital world, where cybersecurity is gaining importance, phishing attacks are among the foremost cyber threats executed with the aims of capturing sensitive information, gaining financial benefits, and accessing systems. These attacks, carried out using social engineering techniques, affect everyone globally, from individuals to small businesses, from large corporations to government institutions. This thesis aims to investigate the level of awareness of phishing attacks among teachers working in official educational institutions in Turkey. In the current conditions where cybersecurity threats are increasingly rising, it is imperative for teachers to be aware and prepared against such attacks to ensure their own information security and to guide their students. In the research, realistic but harmless phishing emails were used to analyze the awareness levels and reactions of teachers to such attacks. In the study, which 197 teachers across Turkey voluntarily participated in, it was found that 76% of the participants opened the phishing emails sent to them, and 80.4% of those who opened the email clicked on the fake link in the content. These high rates indicate that teachers have low awareness of phishing attacks. This study serves as a guide to help the education sector become more resilient against cyber threats.

Science Code	:	92403
Key Words	:	cyber security, phishing attacks, social engineering, cyber attacks, information security
Page Number	:	86
Supervisor	:	Prof. Dr. Murat YÜCEL

TEŞEKKÜR

Bu tezin hazırlanmasında değerli katkı ve destekleriyle bana yol gösteren, önerileriyle çalışmamı şekillendiren ve devam etmem için motivasyon sağlayan çok değerli danışman hocam Sayın Prof. Dr. Murat YÜCEL'e sonsuz teşekkürlerimi sunarım.

Çalışmam boyunca gösterdiği sabır ve destek ile her daim yanımda olan sevgili eşim Barış GENÇ'e, bu süreçte sürekli onları ihmal etmeme rağmen bana desteklerini ve sevgilerini hiç esirgemeyen, hayatımı anlamlandıran ve bana ilham veren çocuklarım Utku Bora GENÇ ve Miray Ece GENÇ'e minnettarlığımı ifade etmek isterim.

Bu çalışma sürecinde her türlü desteğiyle yanımda olan Ataşehir Dilek Sabancı Mesleki ve Teknik Anadolu Lisesi'ndeki tüm çalışma arkadaşlarım ile gönüllü olarak katılarak tez çalışmama önemli katkılar sağlayan ve kendilerinden olumlu yorumlar aldığım kıymetli öğretmenlerime içten teşekkürlerimi sunarım.

Sizlerin desteği ve katkıları olmasaydı, bu çalışmayı tamamlamak mümkün olmazdı. Herkese en içten teşekkürlerimle.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT..... v

TEŞEKKÜR..... vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ..... ix

ŞEKİLLERİN LİSTESİ x

SİMGELER VE KISALTMALAR..... xii

1. GİRİŞ..... 1

2. KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR 11

2.1. Oltalama Saldırısı..... 11

2.2. Oltalama Saldırı Süreci 13

2.3. Oltalama Aktörleri 18

2.4. Oltalama Saldırıları Etkileri 20

2.5. Oltalama Saldırı Türleri 23

2.5.1. E-posta oltalaması (E-mail phishing) 25

2.5.2. Vishing (Voice phishing - Sesli oltalama)..... 26

2.5.3. Mızrak oltalama (Spear phishing) 27

2.5.4. Balina avı oltalaması (Whaling) 28

2.5.5. Smishing (SMS phishing - SMS oltalama)..... 29

2.5.6. Sosyal medya oltalaması (Social media phishing) 30

2.5.7. BEC (Business Email Compromise – İş e-postası tehdidi) 31

2.5.8. Quishing (QR code phishing - QR kod oltalama) 33

2.6. Oltalama Saldırıları Korunma Yolları..... 34

2.7. Literatür Araştırması 36

Sayfa

3. YÖNTEM 43
3.1. Araştırmanın Modeli 43
3.2. Araştırma Grubu 43
3.3. Veri Toplama Araçları 44
3.3.1. Oltalama e-posta tasarımı 44
3.3.2. Gönderilen oltalama e-postaların takibi 48
3.4. Verilerin Analizi 50
4. BULGULAR VE YORUM 51
4.1. Demografik Bulgular 51
4.2. Oltalama E-Postaları ile İlgili Bulgular 54
5. SONUÇ, TARTIŞMA VE ÖNERİLER 67
5.1. Sonuç ve Tartışma 67
5.2. Öneriler 70
KAYNAKLAR 73
EKLER 81
EK-1. Etik Kurul Onay Yazısı 82
EK-2. Katılımcılar İçin Bilgilendirilmiş Gönüllü Olur Formu 83
EK-3. Google Forms Katılımcılar İçin Bilgilendirilmiş Gönüllü Olur Formu 84
ÖZGEÇMİŞ 86

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. Kuruluşlar için anti-oltalama yönerge ve önerileri [70] 35

Çizelge 2.2. Son kullanıcılar için anti-oltalama yönerge ve önerileri [70] 36

Çizelge 3.1. Oltalama e-postası için öğretmenlerin branşlarına göre belirlenen hizmetiçi eğitimler 47

Çizelge 4.1. Katılımcı öğretmenlerin görev yaptığı okul düzeylerine ilişkin bilgiler 52

Çizelge 4.2. Katılımcı öğretmenlerin branşlarına ilişkin bilgiler 53

Çizelge 4.3. Farklı okul düzeylerinde branşların dağılım bilgileri 54

Çizelge 4.4. Oltalama e-postasının katılımcıya gönderilme durumu 55

Çizelge 4.5. Gönderilen oltalama e-postasının açılıp açılmama durumu 55

Çizelge 4.6. Gönderilen oltalama e-postasındaki bağlantıya tıklanıp tıklanmama durumu 57

Çizelge 4.7. Branşlara göre oltalama e-postasının açılma durumunun dağılımı 58

Çizelge 4.8. Branşlara göre oltalama e-postasının açılma durumunun ki-kare testi analizi 59

Çizelge 4.9. Okul düzeyine göre oltalama e-postasının açılma durumunun dağılımı 60

Çizelge 4.10. Okul düzeyine göre oltalama e-postasının açılma durumunun ki-kare testi analizi 60

Çizelge 4.11. Branşlara göre oltalama e-postasındaki bağlantıya tıklama durumunun dağılımı 61

Çizelge 4.12. Branşlara göre oltalama e-postasındaki bağlantıya tıklama durumunun ki-kare testi analizi 62

Çizelge 4.13. Okul düzeylerine göre oltalama e-postasındaki bağlantıya tıklama durumunun dağılımı 62

Çizelge 4.14. Okul düzeylerine göre oltalama e-postasındaki bağlantıya tıklama durumunun ki-kare analizi 63

Çizelge 4.15. Gönderilen oltalama e-postasının açılma sayısı ile ilgili istatistiki bilgiler 63

Çizelge 4.16. Gönderilen oltalama e-postasındaki bağlantıya tıklanma sayısı ile ilgili istatistiki bilgiler 65

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 1.1. 2012-2023 yılları arası hanelerde internet erişim imkânı ve bireylerde internet kullanımı 1

Şekil 1.2. Dijital 2024 Küresel Genel Bakış Raporu'na göre temel dijital başlıklar 2

Şekil 1.3. 2023 Küresel Endüstri Bazında Oltalama Simülasyon Karşılaştırma Çalışması..... 5

Şekil 2.1. Oltalama saldırılarının 1996-2023 yılları arasındaki tarihsel evrim süreci..... 13

Şekil 2.2. Siber Ölüm Zinciri (Cyber Kill Chain) modeli 14

Şekil 2.3. Oltalama saldırı süreci 15

Şekil 2.4. Oltalama saldırı süreci 16

Şekil 2.5. Oltalama saldırı süreci 17

Şekil 2.6. Oltalama saldırı süreci 17

Şekil 2.7. Oltalama saldırı süreci 18

Şekil 2.8. Oltalama saldırı süreci aktörleri ve eylemleri 19

Şekil 2.9. Gerçek zamanlı küresel oltama saldırıları haritası 20

Şekil 2.10. Ocak 2009-Haziran 2009 oltalama saldırılarının hedef aldığı marka ve meşru kuruluşların sayısı..... 21

Şekil 2.11. 2023'ün 4. çeyreğinde oltalama saldırıları ile en fazla hedeflenen sektörler..... 22

Şekil 2.12. 2021-2023 arası dünya genelinde organizasyonlara gerçekleştirilen başarılı oltama saldırıları istatistikleri 22

Şekil 2.13. Oltalama Sınıflandırması..... 24

Şekil 2.14. Oltama Saldırı Teknikleri..... 25

Şekil 2.15. E-posta oltalama örnekleri 26

Şekil 2.16. Mızrak Oltalama Saldırısının Anatomisi 28

Şekil 2.17. Örnek smishing oltalama kısa mesajı..... 30

Şekil 2.18. Oltalama saldırılarında hedef alınan en popüler sosyal medya platformları 31

Şekil **Sayfa**

Şekil 2.19. 2015-2023 arası BEC kaynaklı finansal kayıplar 32

Şekil 2.20. Gerçek hayattan bir Quishing saldırı örneği 34

Şekil 3.1. MEBBİS Hizmetiçi Eğitim Modülü 45

Şekil 3.2. Orijinal e-posta örneği 45

Şekil 3.3. Oltalama e-postası örneği 46

Şekil 3.4. Oltalama e-postasındaki sahte bağlantının yönlendirdiği sayfa..... 46

Şekil 3.5. Oltalama e-postasının mobil cihazlarda görünümü..... 47

Şekil 3.6. Oltalama çalışması için oluşturulmuş kampanya e-posta örneği 49

Şekil 3.7. Gönderilen kampanya postalarının sayısal takibi 50

Şekil 4.1. Araştırmaya katılım onay durumu 51

Şekil 4.2. Katılımcı öğretmenlerin görev yaptığı okul düzeylerinin grafiksel dağılımı . 52

Şekil 4.3. Gönderilen oltalama e-postasının açılıp açılmama durumu..... 56

Şekil 4.4. Gönderilen oltalama e-postasındaki bağlantıya tıklanma durumu..... 57

Şekil 4.5. Gönderilen oltalama e-postasının açılma sayısının grafiği..... 64

Şekil 4.6. Gönderilen oltalama e-postasındaki bağlantıya tıklanma sayısının grafiği 65

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

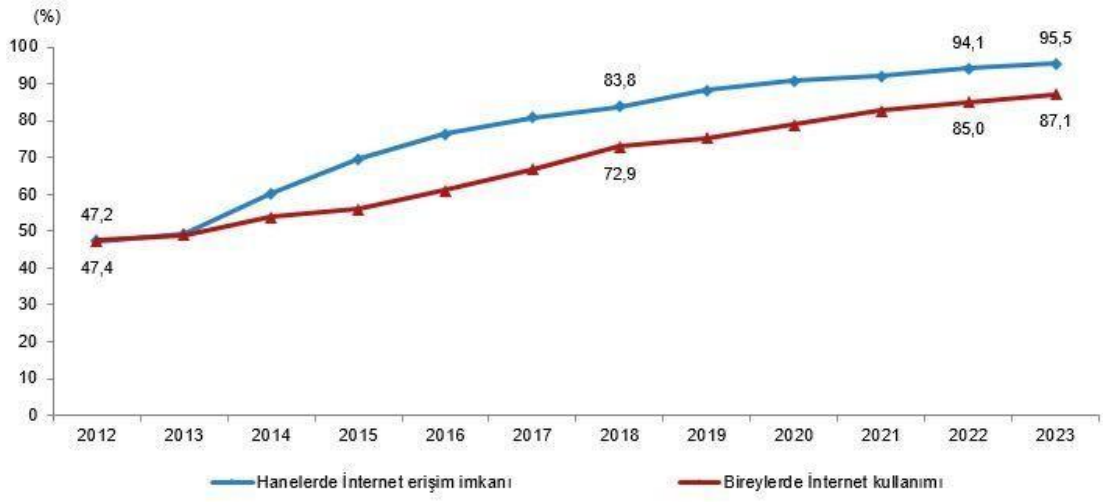
Kısaltmalar	Açıklamalar
ABD	Amerika Birleşik Devletleri
AI	Artificial intelligence
AOL	America Online
APK	Android package kit
APT	Advanced persistent threat
APWG	Anti-Phishing Working Group
BEC	Business email compromise
BT	Bilişim teknolojileri
CEO	Chief executive officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief info security officer
DBIR	Data breach investigations report
DDoS	Distributed denial of service
DNC	Democratic National Committee
FBI	Federal Bureau of Investigation
IBM	International Business Machines
MEBBİS	Millî Eğitim Bakanlığı Bilişim Sistemleri
MFA	Multi-factor authentication
MITM	Man-in-the-middle
QR	Quick response
SEO	Search engine optimization
SMS	Short message service
SPSS	Statistical package for the social sciences
VoIP	Voice over internet protokol
XSS	Cross-site scripting

1. GİRİŞ

Amerika Birleşik Devletleri Patent Ofisi Müdürü Charles H. Duell "Artık yeni hiçbir şey yok. İcat edilebilecek her şey icat edildi.” dediğinde yıl 1899’du [1]. O tarihten itibaren 125 yıllık süreçte birçok önemli icatlar yapılmış ve bu büyük icatlar önemli devrimlere yol açmıştır. Bilgisayarın icadı ile bilginin dijitalleşmesi bundan sonra gerçekleşecek diğer teknolojik yeniliklerin temelini oluşturmuştur. İnternetin keşfi ile dijital bilgi küresel anlamda istenilen zamanda istenilen yerde ulaşılabilir hale gelmiştir ve bu da modern yaşamda büyük bir dönüşüme neden olmuştur.

21. yüzyılda internet olmazsa olmazlardan olmuş ve insanlığa büyük kolaylıklar, avantajlar sağlamıştır. İnsanlar internet tabanlı birçok farklı teknolojiyi destekleyen mobil cihazlar aracılığıyla internete dünyanın dört bir tarafından bağlanabilir duruma gelmişlerdir. İnsanlar, çeşitli amaçlar için e-ticaret ve internet bankacılığı dahil olmak üzere pek çok etkinlikte kolayca web hizmetlerine erişmek için interneti kullanırlar. İnternet, yalnızca web hizmetleri aracılığıyla değil, aynı zamanda uygulamalar ve yazılımlar aracılığıyla da yaygın olarak kullanılabilir [2].

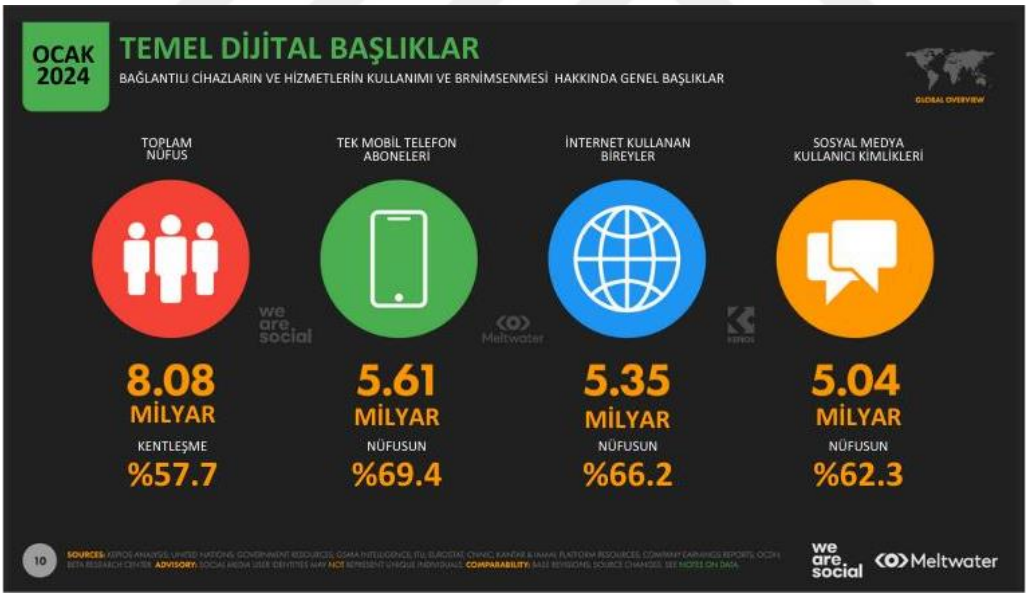
TÜİK’in 29 Ağustos 2023 yılında yayınladığı “Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması 2023” [3] raporuna göre; 2023 yılında evden internete erişim imkânı olan hanelerin oranının bir önceki yıla göre 1,4 puanlık artış gösterdiği ve yüzde 95,5 seviyesine çıktığı, internet kullanımının da 6-74 yaş grubundaki bireylerde 2022 yılında %85,0 iken 2023 yılında %87,1 olduğu görülmüştür (Şekil 1.1).



Şekil 1.1. 2012-2023 yılları arası hanelerde internet erişim imkânı ve bireylerde internet kullanımı [3]

Yine aynı rapora göre [3] son 12 ay içinde özel amaçla resmi makamların web sitelerini ve uygulamalarını kullanan ve İnternet üzerinden kamu hizmetlerinden yararlanan bireylerin oranı %73,9 iken internet üzerinden özel kullanım amacıyla mal veya hizmet satın alma ya da sipariş verme (e-ticaret) oranı %49,5 olmuştur. Bireylerin en fazla kullandıkları sosyal medya ve mesajlaşma uygulamaları %84,9 ile WhatsApp, %69,0 ile YouTube ve %61,4 ile Instagram olduğu tespit edilmiştir.

We Are Social ve Meltwalter'in yayınladığı "Dijital 2024 Küresel Genel Bakış Raporu (Digital 2024 Global Overview Report)" [4] isimli raporda dünya çapında dijital, sosyal medya, mobil ve internet kullanımı ile ilgili güncel veriler ve istatistikler yer almaktadır. Bu rapora göre; Birleşmiş Milletler'in son nüfus rakamları, Ocak 2024'te Dünya'da 8,08 milyar insanın yaşadığını, bu nüfusun %69,4'ü yani yaklaşık 5,61 milyar kişinin kendi kişisel mobil cihazını kullandığını, internet kullananların sayısının 5,35 milyar ve nüfusun %66,2'si olduğu, dünya nüfusunun %62,3'ünü teşkil eden 5,04 milyar kişinin sosyal medya kullandığını göstermektedir (Şekil 1.2).



Şekil 1.2. Dijital 2024 Küresel Genel Bakış Raporu'na göre temel dijital başlıklar [4]

Bilgi ve iletişim teknolojilerindeki bu hızlı gelişmeler, her türlü bilginin dijital alana taşınmasına olanak tanımış ve bu da suçlular için yeni bir faaliyet alanının oluşmasına zemin hazırlamıştır. Siber suçlar, suçlular için özellikle anonimlik sağlaması nedeniyle çekicidir. Bu özellik, siber saldırıların coğrafi sınırlar olmaksızın herhangi bir yerden başlatılabilmesini ve saldırganların varlıklarını gizli tutarak faaliyetlerine

sürdürebilmelerini mümkün kılmaktadır. Bu durum, siber güvenlik stratejilerinin ve yöntemlerinin sürekli güncellenmesi gerekliliğini de ortaya koymaktadır.

Verizon'un 2023 Veri İhlali Araştırmaları Raporu'na (DBIR 2023 Data Breach Investigations Report) [5] göre tüm siber ihlallerin %74'ünde insan faktörü yer almakta ve saldırganların bir organizasyona erişmesinde çalıntı kimlik bilgileri, oltalama ve zafiyetler olmak üzere üç ana yol olduğu görülmektedir. Dünya Ekonomik Forumu'nun (World Economic Forum) 2022 yılında yayınladığı raporda siber güvenlik ihlallerinin %95'inin insan hatasından kaynaklandığını tespit etmiştir [6].

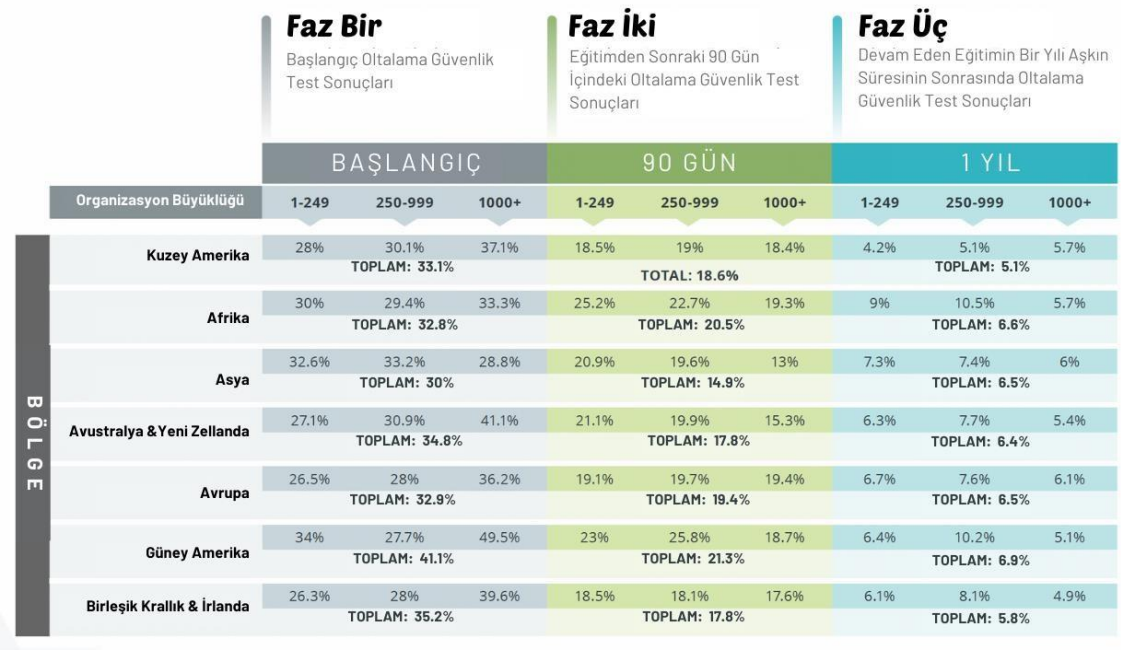
İnsan unsurunun, veri ihlallerini kolaylaştıran etmenler içinde öncelikli bir konumda bulunmasıyla beraber, oltalama saldırıları siber tehditler arasında en yaygın olanı olarak yerini almaya devam etmektedir [7]. Oltalama saldırıları, kişisel bilgileri, finansal verileri veya diğer hassas verileri ele geçirmek amacıyla düzenlenir ve gerçekleştirilmesi oldukça kolay saldırılar olduğundan saldırganların en çok tercih ettiği siber saldırı türlerindendir. Çünkü her kullanıcı, oltalama saldırılarının potansiyel kurbanıdır [8]. Zira, bu tür saldırılar insanın başkalarına olan güven duygusundan, merakından ya da endişe verici iletilere karşı mantık yerine duygusal tepkiler verme eğiliminden faydalanır. Yoğunluk içindeyken bir oltalama mesajındaki kuşkulu noktaları gözden kaçırabiliriz. Daha kurnazca hazırlanmış saldırılarda ise, sahte bir web sitesi veya kötücül bir içeriği, özel eğitim almamış biri tarafından ayırt etmek oldukça güçtür.

Vade'nin son raporunda [9], 2023 yılının üçüncü çeyreğinde oltalama saldırılarının %173 oranında artış gösterdiği, saldırganların üçüncü çeyrekte özellikle Ağustos ayında aktif oldukları görülmektedir. Araştırmaya göre Ağustos ayında 207,3 milyon, Eylül ayında 172,6 milyon ve Temmuz ayında 113,4 milyon oltalama e-postası gönderilmiştir. Ayrıca 2023'ün üçüncü çeyreğinde, Facebook ve Microsoft en sık taklit edilen markalar olduğu tespit edilmiştir. SlashNext'in 2023 Oltalama Durum Raporu (State of Phishing Report for 2023)'na göre [10], e-posta, web ve mobil kanallar arasında oltalama tehditlerinde ve siber suç faaliyetlerinde yapay zeka araçlarının kullanımında endişe verici bir artış olduğu belirtilmektedir. Rapor 2022'nin son çeyreğinden 2023'ün üçüncü çeyreğine kadarlık bir dönemi analiz ederek kötü niyetli oltalama mesajlarında %1265 oranında, hassas kimlik bilgilerini ele geçirmek için e-posta gönderilerek gerçekleştirilen oltalama saldırılarında %967 oranında, SMS oltalama olarak bilinen mobil tabanlı saldırılarda %39 oranında, kuruluşlara ciddi mali kayıplara neden olan metin tabanlı iş e-posta tehdidi %68 oranında

bir artış göstermiş ve ortalama olarak günlük 31000 oltalama saldırısının gerçekleştiği tespit edilmiştir.

İstatistikler, oltalama saldırılarının küresel çapta ne denli yaygınlaştığını ve artış gösterdiğini gözler önüne sermektedir. Bu durum, saldırıların genel bir başarıya ulaştığının ve bu başarının altında, insanların hata yapma eğilimlerinin yattığının bir göstergesidir. Oltalama, özellikle kurumlar için ciddi riskler taşır çünkü kurum içi güvenlik önlemlerini geçmeyi hedefler ve siber güvenlik duvarlarını aşabilir. Kurumlar, siber tehditleri azaltma ve öncelikle oltalama bağlantılarının çalışanlarına ulaşmasını engelleme konusunda siber savunma sistemlerinin güçlü olduğundan emin olmalıdır. Uygun şekilde uygulandığında, siber güvenlik, iş sürekliliğini korumaya yardımcı olur ve finansal kayıpların ya da iş kesintilerinin olasılığını azaltır. Ancak, siber güvenlik sistemlerinin teknik yeterliliği tek başına yeterli değildir. Çalışanların siber güvenlik ve oltalama saldırıları farkındalıklarının da artırılması gerekmektedir.

Kurumlar, oltalama saldırılarına karşı koymak amacıyla, çalışanlarını şüpheli e-postaları tanıma ve rapor etme konusunda eğitmek için farkındalık programları düzenlemektedirler. Özellikle, veri ihlallerinin önlenmesinde, son kullanıcıların oltalama tehlikelerini tanıyıp bu konuda gerekli adımları atma kapasitesine olan güven kritik önem taşımaktadır [11]. Özel kurumlar siber güvenlik önlemleri ile, hem kurum içinde belli aralıklarla yaptıkları simülasyon testleri ile, hem de çalışanlarının siber güvenlik ve oltalama saldırıları farkındalıklarını artırıcı eğitimler almasını sağlayarak özellikle oltalama saldırılarına karşı dirençli bir hale gelmektedirler. KnowBe4'un 5,681 organizasyonda 12,5 milyon kullanıcıyı kapsayan ve 32,1 milyondan fazla oltalama simülasyon testi yaptığı araştırmasında kullanıcıların yaklaşık üçte birinin (%33.1) şüpheli bir linke tıklama ya da e-posta yoluyla sahte bir talebe uyma olasılığının olduğunu ortaya koymuş; ancak 3 fazda gerçekleştirilen araştırmada 90 günlük ve 12 aylık eğitimler sonucunda bu tıklama oranlarının düştüğü gözlemlenmiştir [12](Şekil 1.3).



Şekil 1.3. 2023 Küresel Endüstri Bazında Oltalama Simülasyon Karşılaştırma Çalışması [12]

Türkiye'de kamu kurum ve kuruluşlarında çalışanların bilgi güvenliği farkındalıklarının düşük olduğu çeşitli araştırmaların sonucunda görülmüştür. Yapılan bir çalışmada Türkiye'de siber güvenlik konulu yüksek lisans ve doktora tez çalışmaları incelenmiş ve bazı genel sonuçlar ortaya çıkarılmıştır [13]. Türkiye'nin, siber güvenlik alanında gelişmiş ülkelere göre geride kaldığı, siber güvenlik politikaları ile eylem planlarının yetersiz kaldığı, kurumların kendini güncellemede geri kaldığı gibi sonuçlar örnek verilebilir. Bu araştırmanın sonucunda siber güvenlik ile ilgili çalışmaların ülkenin geneli için ne kadar önemli olduğunun fark edildiği önemle vurgulanmıştır [13]. Yapılan farklı bir çalışmada ise Türkiye'de akademik olarak 2004-2021 yılları arasında siber güvenlik alanında yapılan çalışmalar ile gelecek dönem siber güvenlik stratejileri ve politikaları planlamalarına dair çalışmalar incelenmiş, Türkiye'deki siber güvenlik durumunun kapsamlı bir değerlendirmesini sunarak ulusal güvenlik ile milli değerlerin korunması için gelecekteki teknolojilere uyum sağlanmasının önemi vurgulanmıştır [14]. Araştırma, kurumların iç güvenlik önlemlerini güçlendirmesi gerektiğini, interaktif dolandırıcılığın en yaygın siber suç olduğunu ve eğitim seviyesinin siber suçlarla mücadelede yetersiz kaldığını ortaya koymaktadır. Ayrıca, Türkiye'nin siber güvenlik ve hukuk mevzuatı alanında gelişmiş ülkelerle kıyaslandığında geride kaldığı, siber saldırıların artış gösterdiği ve kişisel güvenlik önlemlerinin yetersiz kaldığı belirtilmiştir. Bu bağlamda, özel sektör

işbirliklerinin, eğitim metodolojilerinin güncellenmesi ve siber güvenlik politikalarının yeniden gözden geçirilmesi gerektiği sonuçlarına ulaşılmıştır [14].

Problemin Durumu

Türkiye'de e-devlet uygulamaları ile birlikte kamu kurumları bu uygulamaları aktif olarak kullanmaya başlamıştır. 2007 yılında okullarda E-Okul uygulamasının kullanımının başlanmasına paralel olarak öğretmenler bilgi ve iletişim teknolojilerini aktif olarak kullanmaya, sonrasında okullar için geliştirilen Fatih projesi kapsamında öğretmenler bilgi ve iletişim teknolojilerini ders içinde de kullanmaya başlamışlardır. COVID-19 pandemisiyle beraber dünya genelinde olduğu gibi Türkiye'de de uzaktan eğitime geçilmiş ve öğretmenler ile öğrencilerin de dahil olmasıyla beraber ülke genelinde internet, uzaktan eğitim uygulamaları, çeşitli bulut uygulamaları kullanımı artmıştır. Ancak öğretmenlerin bilgi ve iletişim teknolojileri kullanımı ve güvenliği konusunda eğitimlerinin, bilgi ve deneyimlerinin az olması pek çok sorunu da beraberinde getirmiştir. Bu dönemde internet kullanımının artması sebebiyle oltalama saldırıları da artış göstermiştir. Öğretmenlerle beraber öğrenciler de siber zorbalık, siber taciz, dolandırıcılık, gizlilik ihlali gibi siber tehditlere maruz kalmışlardır. Bu nedenle öğretmenlerin hem kendi bilgi güvenliklerini sağlamak için hem de öğrencilerine bu konuda rehberlik sağlamak amacıyla farkındalıklarını artırmalarına, ciddi eğitimler almalarına gerek vardır.

Öğretmenler siber güvenlik konusunda Millî Eğitim Bakanlığı bünyesinde açılan hizmetiçi eğitimler alabilmektedirler. Ancak bu eğitimlerin sayısı ya çok az ya da bu eğitimleri genellikle bilişim teknolojileri öğretmenleri almaktadır. Örneğin 2023 yılı içerisinde merkezi olarak hizmetiçi eğitimlerde Siber Güvenlik, Büyük Veri ve Yapay Zekâ (Temel Seviye) Kursu isminde 3, Siber Güvenliğe Giriş Eğitimi Seminer isminde 2 eğitim verildiği görülmektedir [15]. Siber Güvenlik, Büyük Veri ve Yapay Zekâ (Temel Seviye) Kursu isimli eğitim sadece mesleki ve teknik eğitim liselerinde görev yapan çoğunluğu Bilişim Teknolojileri öğretmenlerine verilmiştir.

Öğretmenlerin özellikle oltalama saldırıları farkındalıklarının ne düzeyde olduğunun tespit edilmesi alınması gereken önlemler ve gerçekleştirilmesi gereken eğitimler, stratejik planlar için önem teşkil etmektedir.

Araştırmanın amacı

Bu araştırmanın amacı, uygun bir senaryoya dayalı simüle edilmiş oltalama e-postaları yoluyla öğretmenlerin siber güvenlik farkındalıklarını ölçmek ve analiz etmektir. Bu simülasyon, öğretmenlerin gerçekçi oltalama tehditlerini tanıma ve buna uygun tepkiler verme becerilerini değerlendirmek için tasarlanacaktır. Katılımcılara gönderilecek olan bu sahte e-postalar, eğitimcilerin siber saldırılara karşı reaksiyonlarını ve savunma stratejilerini belirlemeye yardımcı olacak, böylece eğitim kurumlarının siber güvenlik önlemlerini güçlendirme yönünde etkili öneriler geliştirilmesine rehberlikte bulunacaktır. Bu çalışma, eğitim sektörünün siber tehditlere karşı direncini artırmak ve öğretmenlerin bu konudaki bilinç ve becerilerini geliştirmek için bir temel oluşturmayı, siber güvenlik eğitimleri ve politikalarının geliştirilmesi için temel bir referans kaynağı oluşturmayı hedeflemektedir.

Araştırmada "Öğretmenlerin siber güvenlik ve özellikle oltalama saldırıları konusundaki farkındalıkları ne düzeydedir?" sorusuna yanıt aranacaktır. Ayrıca araştırmada yanıt aranacak alt sorular şunlardır:

- Öğretmenler, simüle edilmiş oltalama e-postalarını tanıma konusunda ne kadar yeteneklidir?
- Farklı senaryolar altında öğretmenlerin siber tehditlere karşı tepkileri nasıl değişmektedir?
- Siber güvenlik farkındalığının artırılması için öğretmenlere hangi tür eğitimlerin verilmesi gerekmektedir?
- Öğretmenlerin siber güvenlik konusundaki bilgi ve becerilerini geliştirmek için hangi stratejik adımlar atılmalıdır?

Bu sorular, araştırmanın yönünü belirleyecek ve veri toplama, analiz etme ve sonuçları yorumlama sürecine rehberlik edecektir.

Araştırmanın önemi

Bu araştırma, öğretmenlerin oltalama saldırılarına karşı farkındalığını ölçmek ve bu farkındalığın eğitim ortamlarında nasıl artırılabileceğini anlamak için önemlidir. Siber güvenlik tehditleri, her geçen gün eğitim sektöründe artmakta ve öğretmenlerin yanı sıra öğrencilerin de hassas verileri risk altında bulunmaktadır. Öğretmenlerin siber tehditleri

etkili bir şekilde tanıyıp yanıt verme yetenekleri, öğrencilerin güvenliği ve eğitim kurumlarının bütünlüğü için kritik bir savunma hattı oluşturur. Bu çalışma, öğretmenleri siber güvenlik konusunda bilinçlendirmek ve eğitim kurumlarının mevcut güvenlik protokollerini güçlendirmek için gerekli verileri sağlamayı amaçlamaktadır.

Ayrıca, bu araştırma, siber güvenlik eğitimlerinin içerik ve yöntemlerini geliştirme konusunda yol gösterici olacak ve eğitim sektörünün siber tehditlere karşı daha dirençli hale gelmesine yardımcı olacaktır. Simüle edilmiş oltalama e-postaları, gerçek dünya koşullarını yansıtan senaryolarla hazırlanacak ve bu da öğretmenlerin gerçek saldırıları tanıma becerilerini doğru bir şekilde değerlendirmeye olanak tanıyacaktır. Elde edilecek sonuçlar, siber güvenlik politikalarının şekillendirilmesinde ve eğitimcilerin siber tehditlere karşı nasıl daha iyi donatılabileceğinde belirleyici olacaktır.

Varsayımlar / Sayıltılar

Araştırma, katılımcıların oltalama e-postalarına nasıl tepki vereceklerine dair varsayımlar üzerine kuruludur. Özellikle, öğretmenlerin bilgi güvenliği konusunda yeterli ön bilgiye sahip olmadıkları ve bu yüzden oltalama girişimlerine karşı savunmasız oldukları düşünülmektedir. Bu tür bir varsayım, eğitim programlarının ve farkındalık stratejilerinin geliştirilmesine katkıda bulunacak temel bir dayanak oluşturmaktadır. Ek olarak, araştırmanın şu varsayımlar üzerine kurulduğu düşünülmektedir:

- Katılımcıların, araştırma sürecine gönüllü olarak katıldıkları ve gönderilen oltalama e-posta senaryolarını ciddiye alarak gerçekçi tepkiler verdikleri varsayılmaktadır.
- Araştırma süresince katılımcıların, günlük iş akışlarının doğal bir parçası olarak simüle edilmiş oltalama e-postalarını alacakları ve bu e-postalara tepki verirken herhangi bir dış etkiden bağımsız hareket edecekleri varsayılmaktadır.
- Araştırma sonuçlarının, eğitim kurumlarının mevcut siber güvenlik protokollerinin ve farkındalık programlarının etkinliğini değerlendirmek için kullanılabileceği varsayılmaktadır.
- Katılımcıların, oltalama e-postalarını alıp almadıklarına dair geri bildirimlerin doğru ve eksiksiz olacağı varsayılmaktadır.

Bu varsayımlar, araştırmanın tasarımı ve yürütülmesi sırasında dikkate alınmalı ve sonuçların yorumlanması sürecinde göz önünde bulundurulmalıdır. Bu varsayımların doğruluğu, araştırmanın genel geçerliliği ve güvenilirliği açısından önemlidir.

Sınırlılıklar

Araştırmaya katılım gönüllülük temelinde olup, öğretmenler belirli bir coğrafi bölge ve sosyal ağ üzerinden, özellikle İstanbul üzerinden araştırmaya davet edilmişlerdir ki bu, Türkiye'nin diğer bölgelerindeki öğretmenlerin deneyimlerini yeterince yansıtmayabilir. Katılımcıların hangi illerden oldukları ve diğer demografik bilgiler toplanmayacak olup, bu durum araştırmanın demografik çeşitliliğini ve sonuçlar üzerindeki etkilerini derinlemesine anlama sınırlılığını beraberinde getirir.

Ayrıca, katılımcıların farklı e-posta hizmet sağlayıcılardan (örneğin Gmail, Yahoo, Outlook, vb.) e-posta edinip kullanmaları, gönderilen oltalama e-postalarının takibini zorlaştırmaktadır. Kullanılan e-posta takip uygulamaları, gönderilen oltalama e- postalarının spam klasörüne mi yoksa gelen kutusuna mı düştüğünü izleyememektedir. Bu durum, epostaların katılımcılar tarafından fark edilip edilmediğini ve simülasyonun etkinliğini doğrudan etkileyebilecektir. Ayrıca, kullanılan e-posta takip uygulamaları ile bir günde kısıtlı sayıda e-posta gönderilebilmektedir. Bu kısıtlama, araştırmanın belirli bir zaman diliminde yeterli veri toplayabilmesini engelleyebilir ve simülasyonun sürekliliğini sınırlayabilir.

Bu sınırlamalar, araştırmanın sonuçlarının etkileyebilecek önemli faktörlerdir. Dolayısıyla, sonuçlar yorumlanırken bu sınırlamalar dikkate alınmalıdır.

Tanımlar

Bilgi Güvenliği: Bilgi güvenliği, bilgilerin yetkisiz erişimden, değişiklikten, ifşa edilmesinden, yok edilmesinden veya kötüye kullanılmasından korunmasını amaçlayan uygulamalar bütünüdür. Bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik adında üç temel prensibi vardır.

Siber Tehdit: Bilgisayar sistemlerine, ağlara ve verilere zarar vermeyi veya bu sistemlerin bütünlüğünü ve gizliliğini ihlal etmeyi amaçlayan her türlü kötü niyetli faaliyetlerdir. Siber

tehditler arasında virüsler, truva atları, solucanlar, fidye yazılımları, DDoS saldırıları ve oltalama saldırıları gibi çeşitli kötü amaçlı yazılımlar ve teknikler bulunmaktadır.

Kötü Amaçlı Yazılım (Malware): Bilgisayar sistemlerine zarar vermek, veri çalmak veya yetkisiz erişim sağlamak amacıyla tasarlanmış yazılımlardır. Virüsler, solucanlar, truva atları ve casus yazılımlar kötü amaçlı yazılım türleri arasındadır.

Siber Saldırı: Bir bilgisayar sistemine veya ağa yönelik olarak yapılan, yetkisiz erişim elde etmeyi, bilgileri çalmayı, sistemi bozmayı veya çalışmaz hale getirmeyi amaçlayan herhangi bir girişimdir. Siber saldırılar, bireysel saldırganlardan organize suç gruplarına kadar birçok farklı kaynak tarafından gerçekleştirilebilir.

Siber saldırgan: Bilgisayar sistemlerine, ağlara veya dijital cihazlara yetkisiz erişim sağlamak, zarar vermek veya verileri çalmak amacıyla kötü niyetli faaliyetlerde bulunan kişi ya da kişilerdir.

Fidye yazılımı: Bir bilgisayar sistemine veya dosyalara erişimi engelleyen ve bu erişimi geri almak için bir fidye talep eden kötü amaçlı yazılımlardır. Fidye yazılımları genellikle kullanıcıların dosyalarını şifreleyerek çalışır ve fidye ödenene kadar bu dosyalara erişimi kısıtlar.

2. KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR

2.1. Oltalama Saldırısı

Sosyal mühendislik, bir siber saldırı yöntemidir. Bu tarz saldırıların temel amacı, bireyleri hassas bilgilerini ifşa etmeye ikna etmektir. Bu tür saldırılar, şifreler, gizli veriler veya sistemlere erişim gibi kritik bilgileri elde etmeye yöneliktir. İnsan faktörünü hedef aldıkları için, güvenlik sistemlerindeki en büyük zayıflığı temsil ederler ve bu nedenle son derece etkilidirler [16].

İngilizce phishing olarak bilinen bazı kaynaklarda kimlik avı saldırısı olarak da geçen oltalama saldırısı sosyal mühendislik saldırılarının en yaygın türüdür. Günümüzde oltalama, birçok birey ve kuruluşu etkileyen, sürekli büyüyen bir siber suç türüdür [17]. 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. Hassas bilgilerin sızdırılması ve kötü amaçlı kodların dağıtılması da bu saldırıların potansiyel sonuçları arasındadır.

Phishing teriminde “Ph” harflerinin kullanımı, erken dönem hackerlarının telekomünikasyon sistemlerini inceleyen ve deneyler yapan “phreaks” olarak bilinmelerinden dolayıdır ve bu terimi bu yeraltı toplulukları ile bağdaştırmak içindi [18]. “Phishing” kelimesinin basılı medyada ilk kullanımı 16 Mart 1997’de Florida Times Union’da Ed Stansel tarafından yazılan bir makalede görülmüştür [19]. Dolandırıcılık ve sahtekarlık konseptleri zamanla gelişerek bugünkü karmaşık oltalama saldırılarına dönüşmüştür.

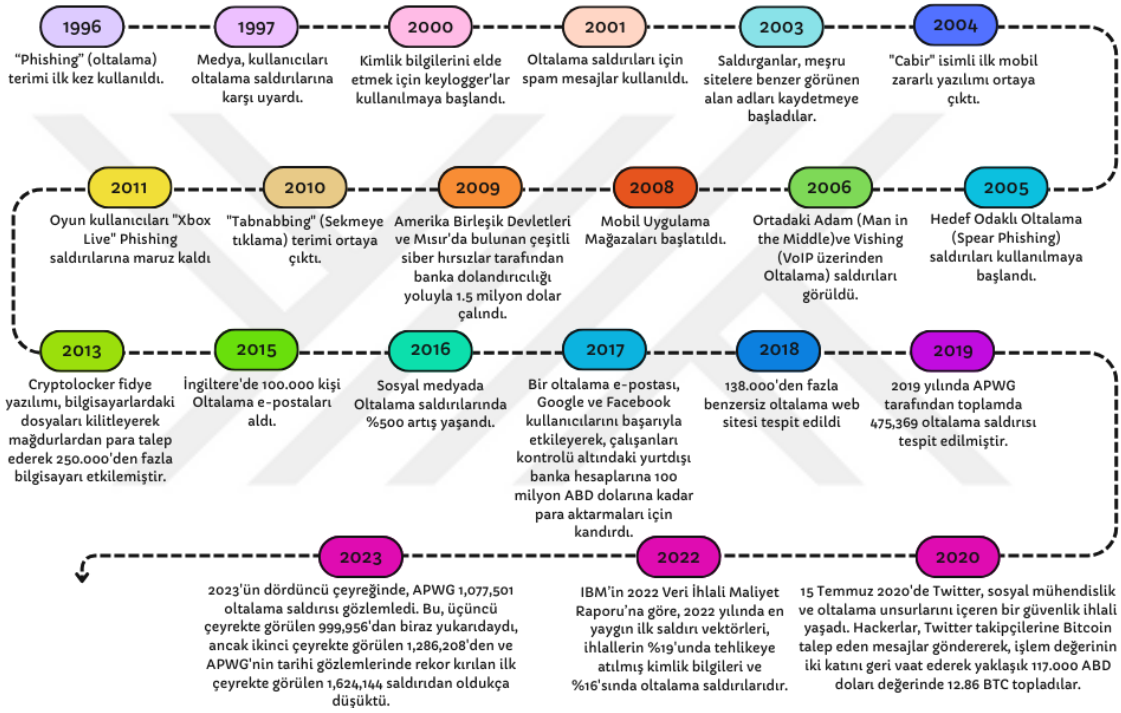
Oltalama, değişik tanımlara sahiptir ve bu tanımlar, terimin kullanıldığı bağlama göre değişiklik göstermektedir. Oltalama saldırıları, genellikle aldatıcı yöntemler kullanarak hedefin saldırganın istediği eylemi gerçekleştirmesini sağlamayı amaçlar. Çeşitli kaynaklarda oltalama terimi farklı şekillerde tanımlanmaktadır; bazıları yalnızca web sitelerini, bazıları ise yalnızca e-postalarını saldırı aracı olarak belirtmektedir. Örneğin bir çalışmada oltalama, genellikle bankalar, çevrimiçi hizmet sağlayıcılar gibi güvenilir kurumlar gibi davranarak, acil eylemde bulunmaları gerektiği yönünde tehditlerle bireyleri kandıran ve onları gerçek kurumun web sitesine bilgilerini girmeye inandıran, e-posta,

SMS veya WhatsApp yazışmaları, telefon mesajları aracılığıyla kişisel verileri (kullanıcı adı ve şifre) ele geçirmeyi amaçlayan dolandırıcılık yöntemi olarak tanımlanmıştır [17]. Vade [21] ise oltalamayı sıklıkla e-posta yoluyla yapılan, dolandırıcıların tanınmış bir marka veya kişi kılığına girerek meşruiyet ve otorite görünümü yarattıkları ve hassas bilgileri elde etmeyi amaçlayan bir siber tehdit türü olarak ifade etmiştir. APWG (Anti- Phishing Working Group) 2023 yılının 4. çeyreği için yayınladığı raporda oltalamayı hem sosyal mühendislik hem de teknik aldatma kullanarak tüketicilerin kişisel kimlik bilgilerini ve finansal hesap bilgilerini çalmayı amaçlayan, tüketicileri sahte web sitelerine yönlendirerek finansal verilerini ele geçirirken, bilgisayarlara zararlı yazılım yerleştirerek doğrudan kimlik bilgilerini çalan bir suç olarak tanımlamıştır [22]. Oltalama, saldırganın amacının para çalmak, hassas veri ve giriş bilgilerine erişim kazanmak veya kurbanın cihazına zararlı yazılım yüklemek olduğu, genellikle e-posta ve metin mesajları yoluyla gerçek ve güvenilir bir kaynaktan gelmiş gibi görünen sahte iletiler gönderme uygulamasıdır ve tehlikeli, zarar verici ve giderek daha yaygın bir siber saldırı türüdür [23]. CISA (Cybersecurity and Infrastructure Security Agency) yayınladığı bilgilendirme broşüründe "Oltalama, bir siber tehdit aktörünün güvenilir bir meslektaş, tanıdık veya kuruluş rolünü üstlenerek kurbanın hassas bilgilerini veya ağ erişimini sağlamasını amaçladığı bir sosyal mühendislik formudur." şeklinde ifade etmiş ve sonuçları arasında veri ihlali, veri ve hizmet kaybı, kimlik dolandırıcılığı, kötü amaçlı yazılım ya da fidye yazılımının yüklenmesinin yer alabileceğini belirtmiştir [24]. Birçok çalışmada da belirtildiği gibi oltalama, bireyleri meşru bir kaynak gibi davranarak kandırmak ve kişisel bilgilerini (şifreler, hesap bilgileri, kredi kartı numaraları vb.) ele geçirmek amacıyla gerçekleştirilen bir tür sosyal mühendislik saldırısıdır [25-28].

Bu tanımlamalardan yola çıkarak oltalama şu şekilde tanımlanabilir: Oltalama, güvenilir bir kaynak gibi davranan siber suçluların sosyal mühendislik ve teknik aldatma yöntemleri kullanarak bireyleri kandırmaya çalıştıkları ve bu sayede onların hassas bilgilerini, finansal hesap bilgilerini çalmayı hedefleyen bir suç türüdür ve saldırganlar, sahte e-postalar, SMS (Short Message Service)'ler veya web siteleri aracılığıyla, genellikle acil eylemde bulunmaları gerektiğine dair korkutucu mesajlar göndererek kurbanları hedef alır ve bu mesajlar yardımıyla kişisel verilerini ele geçirmeyi amaçlar.

Oltalama teriminin ilk kez kullanıldığı tarih Ocak 1996 olarak internet kayıtlarına geçmiştir [29, 30] ve AOL (America Online) kullanıcılarına yönelik kullanıcıların AOL

hesap bilgilerini aldatma yoluyla ele geçirmek için sosyal mühendislik saldırılarıyla gerçekleşmiştir [18, 30]. 1996 yılından sonra farklı türlerde gerçekleşen oltalama saldırıları yaygınlaşmış, daha karmaşık hale gelmiştir. 2014'te yaşanan büyük finansal kaybın ardından oltalama saldırıları, hem ciddi bir sorun olarak kabul edilmeye başlanmış hem de araştırmacıların yoğun ilgisini çekmiştir ve internet ile sosyal medyanın yaygınlaşmasıyla 2016'dan itibaren bu saldırıların sayısı hızla artarak yükseliş trendine girmiştir [30]. Şekil 2.1'de oltalama saldırılarının tarihsel evrim süreci yer almaktadır [19, 22, 29-33].



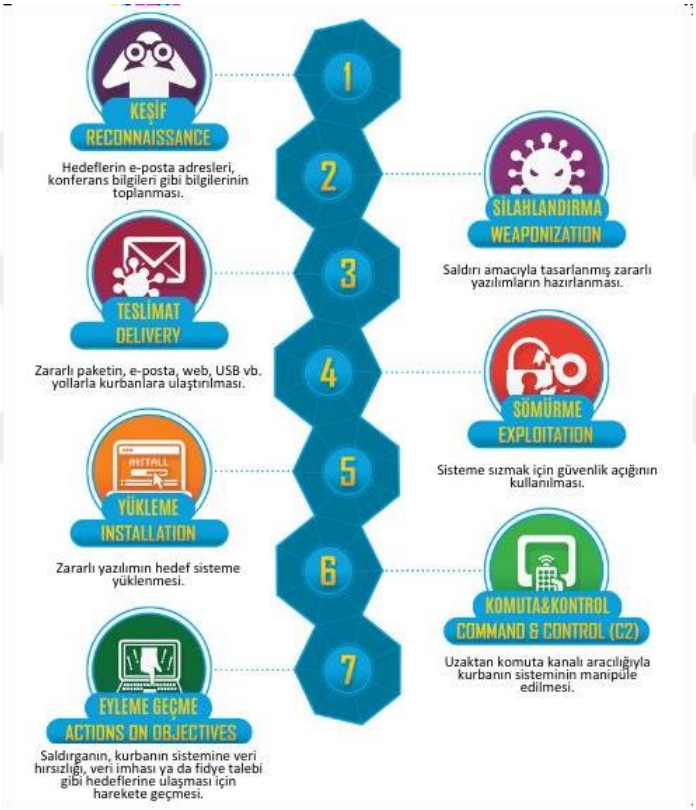
Şekil 2.1. Oltalama saldırılarının 1996-2023 yılları arasındaki tarihsel evrim süreci

Oltalama saldırıları sürekli olarak gelişmekte ve yeni güvenlik önlemlerine adaptasyon göstermektedir. Saldırganlar, sistem zafiyetlerinden yararlanmak amacıyla sürekli olarak yeni teknolojileri ve araçları keşfederken, kullanıcıları aldatmak için de sosyal mühendislik tekniklerine başvurmaktadırlar. Bu yaklaşımların etkisiyle, oltalama saldırıları siber suçluluk alanında önemli bir başarı oranına sahip olmayı sürdürmektedir.

2.2. Oltalama Saldırı Süreci

Yetenekli siber saldırganlar, gerçekleştirecekleri siber saldırılar öncesinde derinlemesine kapsamlı bir planlama sürecinden geçerler. Öncelikle hedef belirleyip, bu hedef hakkında bilgi toplarlar. Daha sonra, düzenli ve organize bir biçimde hareket ederek saldırılarının

başarı şansını artırmaya çalışırlar. Bu süreç, siber savunma tarafındaki kurbanların, saldırganların metotlarını kavramasını ve saldırılara karşı önlem almasını zorunlu kılar. Bu amaçla siber saldırı analiz modelleri oluşturulmuştur. Bunun analiz modellerinden en bilinen ve kabul göreni 2011 yılında Lockheed Martin firması tarafından geliştirilen "Siber Ölüm Zinciri (Cyber Kill Chain)" modelidir [24]. 7 aşamadan oluşan bu model (Şekil 2.2), saldırı aşamalarını tanımlayarak savunma için gerekli taktiklerin geliştirilmesine olanak tanır, analistlere ve güvenlik ekiplerine saldırıları daha iyi anlama ve önleme fırsatı sunar.



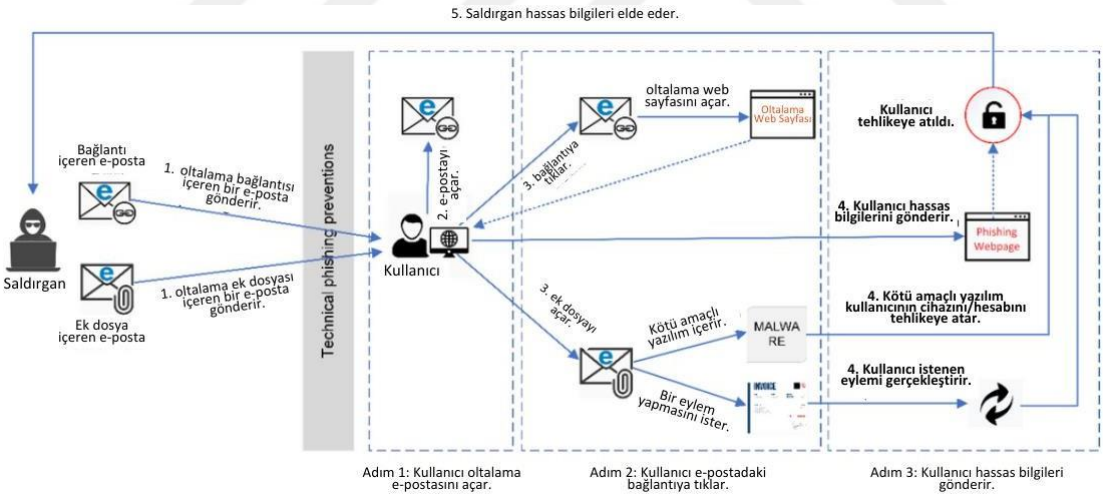
Şekil 2.2. Siber Ölüm Zinciri (Cyber Kill Chain) modeli [34]

Oltalama saldırıları, siber saldırıların gerçekleştirilmesinde kullanılan bir yöntemdir ve Siber Ölüm Zinciri modelinin çeşitli aşamalarında yer alabilir. Oltalama saldırıları bu modelin genellikle hedefin bilgisini toplama (Keşif), zararlı içerik oluşturma (Silahlandırma) ve hedefe gönderme (Teslimat) ve hedefin sistemine sızma veya güvenlik açıklarını istismar etme (Sömürme) aşamalarında kullanılır.

Oltalama saldırı süreci kendi içerisinde farklı aşamalarla ifade edilebilir. En yaygın oltalama saldırıları, üç ana bileşenden oluşur: Yem (The Lure), Kanca (The Hook) ve Yakalama (The Catch) [35]. Yem, bir saldırganın genellikle internet üzerinde varlık

gösteren meşru bir kurumdan geldiği izlenimini veren ikna edici bir hikayeyle dolu bir e-posta ile büyük sayıda kullanıcıya mesaj göndermesidir. Kanca, meşru hedef kurumunun görünümünü taklit eden bir web sitesinden oluşur ve amacı, kurbanların bu siteye gizli bilgilerini ifşa etmeleri için yönlendirilmeleridir. Yakalama, saldırganın toplanan bilgileri dolandırıcılık veya kimlik hırsızlığı gibi kötü amaçlar için kullanmasıdır.

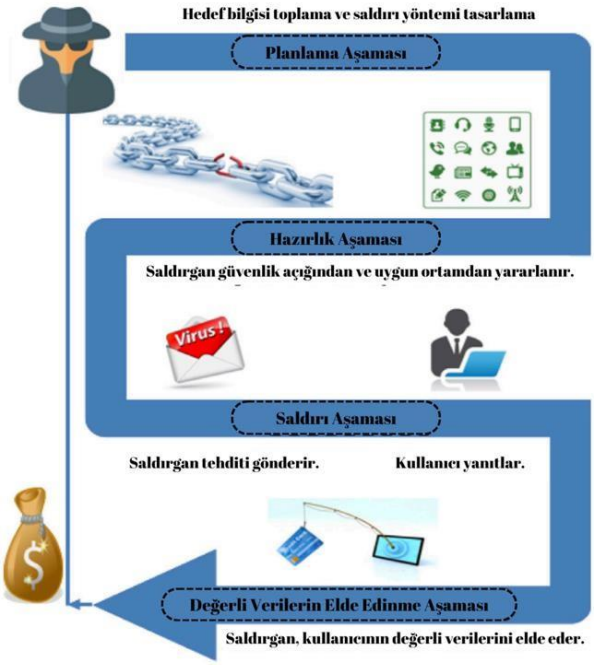
Abroshan ve diğerleri (2021), Şekil 2.3'te görüldüğü gibi oltalama saldırı sürecini 3 adımda incelemiştir [36]. İlk adımda, saldırgan potansiyel kurbanlara, ya oltalama bağlantısı içeren ya da kötü amaçlı ekler barındıran e-postalar gönderir. Bu e-postalar, teknik güvenlik sistemleri tarafından engellenebilir; ancak, sistemlerden sıyrılıp kullanıcıya ulaşırsa, kullanıcı e-postayı açma riskiyle karşı karşıya kalır. İkinci adımda, kullanıcı ya kötü amaçlı bağlantıya tıklar ya da ek dosyayı açar. Üçüncü adımda ise, kullanıcı ya sahte web sayfasında hassas bilgilerini girer ya da kötü amaçlı yazılım cihazına sızarak güvenlik önlemlerini aşar. Bu süreç, oltalama saldırısının temel adımlarını ve kullanıcıların karşılaşabileceği riskleri göstermektedir.



Şekil 2.3. Oltalama saldırı süreci [36]

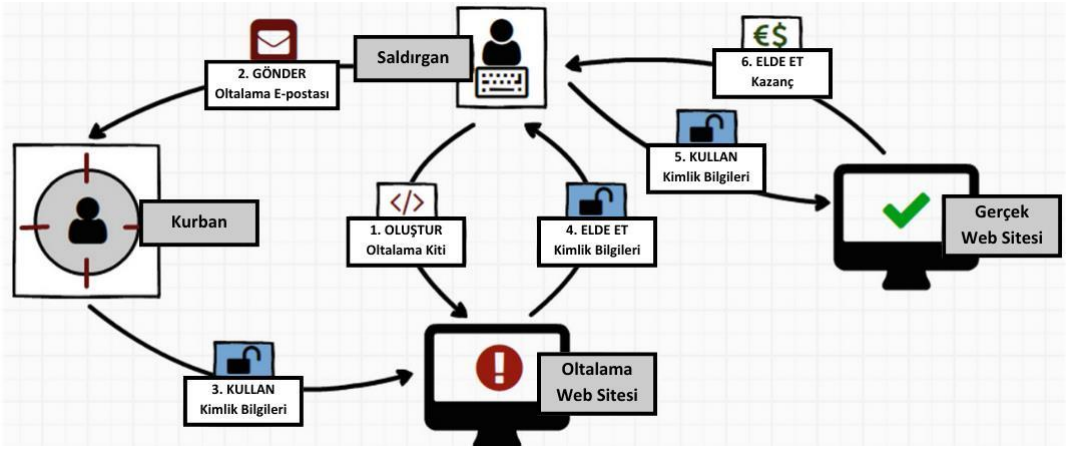
Mohammad ve diğerleri (2015) çalışmalarında oltalama saldırı sürecini Planlama (saldırgan, hedeflerini, elde etmek istediği bilgileri ve saldırıda kullanılacak teknikleri belirler), Toplama (kurban eyleme geçirilerek, güvenilir görünen bir web sayfası aracılığıyla kimlik bilgileri istenir) ve Dolandırıcılık (saldırgan, kurbanın kimliğine bürünerek dolandırıcılık yapar veya bilgileri internetin kara borsasında satar) olmak üzere 3 aşamada göstermişlerdir [37].

Alkhalil ve diğerleri (2021), oltalama saldırılarını 4 aşamada incelemişlerdir [38] (Şekil 2.4). Oltalama saldırıları, genellikle hedef hakkında bilgi toplama ile başlar ve saldırgan, saldırıyı planlamak için bir yöntem seçer. Hazırlık aşamasında, saldırgan kurbanı tuzağa düşürebileceği zayıflıkları arar. Saldırı aşamasında, saldırgan eylemini gerçekleştirir ve kurbanın tepkisini bekler. Son olarak saldırgan, değerli verileri elde etme aşamasında, topladığı bilgileri çeşitli kötü amaçlar için kullanır.



Şekil 2.4. Oltalama saldırı süreci [38]

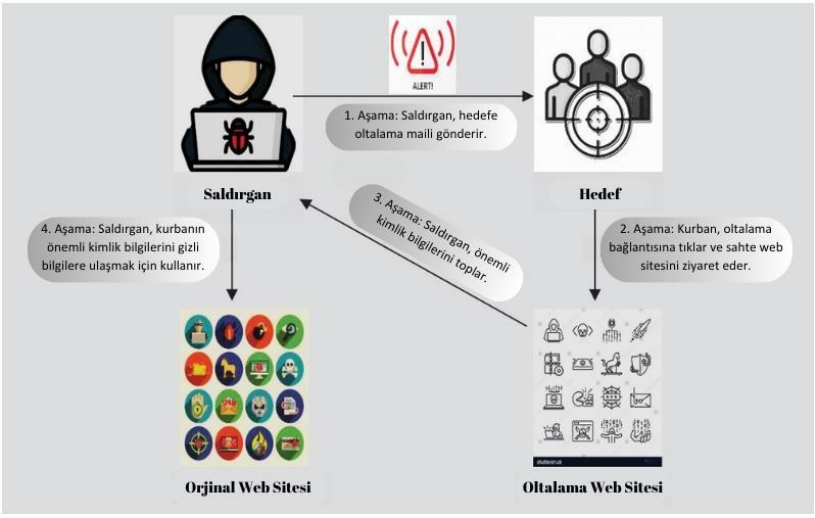
Korkmaz ve diğerleri (2021) ise oltalama saldırıları sürecini Şekil 2.5'teki gibi 6 adımda göstermişlerdir [39]. Bu sürecin başında saldırgan, kurbanı belirler ve onun hakkında bilgi toplar. Ardından kurbanı tuzağa düşürecek olan sahte web sitesi ve ikna edici içerikli e-postalar oluşturulur. Kurbana gönderilen bu e-postalar, onların sahte siteye erişmelerini ve duyarlı bilgilerini girmelerini sağlamak için tasarlanmıştır. Kurban, genellikle tanıdık bir kaynaktan geldiğine inandığı bu e-postada yer alan bağlantıya tıklayarak veya sahte sitede belirtilen eylemi gerçekleştirerek bilgilerini saldırgana kaptırabilir. Son aşamada ise saldırgan, elde ettiği bilgilerle dolandırıcılık yapabilir veya bu bilgileri karaborsada satabilir. Her adımın etkili bir şekilde işlemesi için saldırgan, kurbanın güvenini kazanmayı ve teknik güvenlik önlemlerini aşmayı hedefler [39].



Şekil 2.5. Oltalama saldırı süreci [39]

Kaur ve Mian (2023), oltalama saldırılarını 4 aşamada ifade etmişlerdir [40]. Şekil 2.6'da da gösterilen oltalama saldırıları aşamaları şöyledir:

1. Aşama: Saldırgan, güvenilir bir kaynak izlenimi vererek, hedefe zararlı bir içerik taşıyan bir e-posta gönderir.
2. Aşama: Alıcı, bu e-postadaki sahte bağlantıya tıkladığında kendini, saldırganın kurbanlarını tuzağa düşürmek için kullandığı yanıltıcı bir web sayfasında bulur.
3. Aşama: Kurban, sahte site üzerinde kendi gizli bilgilerini girerken, hacker bu bilgileri hemen toplar.
4. Aşama: Hacker, kurbanın bilgilerini ele geçirip onları kendi çıkarları için kullanabilir ya da en yüksek fiyatı verene satabilir.



Şekil 2.6. Oltalama saldırı süreci [40]

Literatürdeki çalışmalarda [35-40] oltalama süreci farklı sayılarda aşamalarla ifade edilse de ortak noktaları vardır. Bu çalışmalardan yola çıkılarak oltalama saldırı süreci 5 adımda gösterilebilir.

1. **Keşif:** Saldırgan, hedefi ve zafiyetleri belirler. Bu aşamada, hedefin bilgileri toplanır.
2. **Hazırlık:** Saldırgan, sahte web siteleri oluşturur ve ikna edici e-postalar hazırlar.
3. **Dağıtım:** Hazırlanan sahte e-postalar hedeflere gönderilir.
4. **Eylem:** Hedef, e-postadaki sahte bağlantıya tıklar ve hassas bilgilerini girer.
5. **Sömürü:** Saldırgan, elde edilen bilgileri kullanır veya kazanç sağlar.

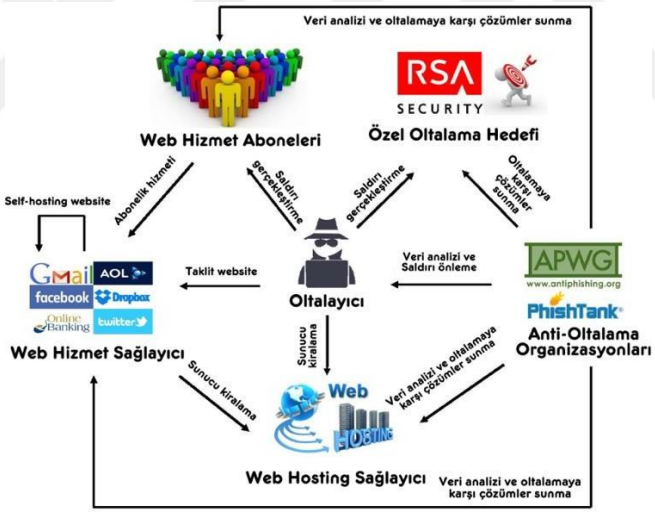


Şekil 2.7. Oltalama saldırı süreci

2.3. Oltalama Aktörleri

Oltalama saldırı süreci farklı araştırmalarda farklı adımlarla tanımlanmasına rağmen; bu süreçte yer alan bazı ortak aktörler vardır. Şekil 2.8'de de görüldüğü gibi oltalama saldırı sürecindeki aktörler altı başlıkta incelenmektedir [41]:

1. **Oltalayıcılar:** Finansal kazanç, ün veya kimlik gizleme gibi çeşitli faydalar elde etmek için oltalama saldırıları düzenleyen bireyler veya kuruluşlar.
2. **Web Hizmet Sağlayıcıları:** İnternet üzerinden e-posta, sosyal medya, çevrimiçi alışveriş ve e-bankacılık gibi çeşitli hizmetleri sunan şirketler.
3. **Web Hizmet Aboneleri:** Web hizmet sağlayıcıları tarafından sunulan hizmetlere abone olan müşteriler; geleneksel oltalama saldırılarının birincil hedefleridir.
4. **Web Hosting Sağlayıcıları:** Web hizmeti sağlayıcılarına web sitesi barındırma hizmeti sunan şirketler.
5. **Anti-Oltalama Organizasyonları:** Oltalama saldırılarıyla mücadelede bireylere ve kuruluşlara destek veren, anti-oltalama kontrolleri ve çözümleri sunan, oltalama verilerini toplayıp analiz eden organizasyonlar.
6. **Özel Oltalama Hedefleri:** Oltalayıcılar tarafından hedef alınan belirli bireyler veya şirketler.



Şekil 2.8. Oltalama saldırı süreci aktörleri ve eylemleri [41]

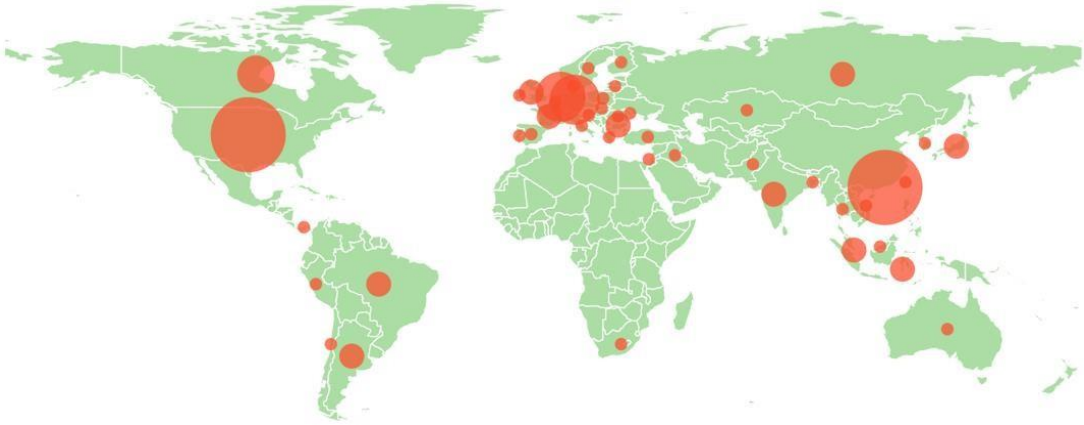
Bu aktörler, oltalama sürecinin çeşitli aşamalarında farklı rol ve sorumluluklara sahiptirler ve her biri oltalama saldırılarını tespit etme, engelleme veya bunlara yanıt verme konusunda önemli işlevler görür [41]. Oltalayıcılar, sahte iletişim yolları kullanarak kişisel bilgileri çalmayı amaçlar ve bu süreçte ileri düzey oltalamaya karşı olan teknikleri atlatmaya çalışırlar. Web servis sağlayıcıları, kullanıcıların güvenliğini sağlamak amacıyla kara listeler duyurur ve güçlü kimlik doğrulama yöntemleri önerir. Web servis aboneleri, genellikle tarayıcı filtreleri ve oltalama engelleyici araçları kullanarak saldırıları engellemeye çalışır. Web hosting sağlayıcıları, güvenlik politikaları uygular ve marka

izleme gibi önlemler alır. Anti-oltalama organizasyonları, oltalama verilerini analiz eder. Özel oltalama hedefleri ise, özellikle hedef alınan bireyler veya kuruluşlar olarak, çalışanlarını oltalama tehditlerine karşı eğitir ve bilinçlendirir.

2.4. Oltalama Saldırıları Etkileri

Oltalama saldırıları, internet kullanıcılarını gerçek gibi görünen sahte platformlara yönlendirerek kişisel verilerini çalmayı hedefleyen gelişmiş dolandırıcılık taktikleridir. Bu tür saldırılarda, saldırganlar sıkça sosyal medya profilleri gibi kamuya açık kaynaklardan edindikleri bilgilerle kişisel ve ikna edici saldırı senaryoları geliştirirler. Saldırılar, genellikle kullanıcıların güvendikleri bir banka veya hizmet sağlayıcıdan gelmiş gibi tasarlanmış e-postalarla başlatılır ve alıcıları, giriş bilgilerini girecekleri veya zararlı yazılımların bulaşacağı sahte sitelere çeker. Saldırganlar, çaldıkları verileri kullanarak finansal kazanç elde eder veya kara borsada satarlar. Bu sürecin karmaşıklığı ve uluslararası boyutu, saldırıların tespitini ve suçluların adalet önüne çıkarılmasını güçleştirir.

Şekil 2.9'da OpenPhish'in dünya genelinde gözlemlenen aktif oltalama sayfaları hakkında gerçek zamanlı bilgi sunduğu The Global Phishing Activity (Küresel Oltalama Aktivite) sayfasındaki harita görülmektedir [42]. Bu veriler son 24 saatlik döneme ait bilgilerle her beş dakikada bir güncellenmektedir. Görsele göre tüm dünya oltalama saldırılarından etkilenmektedir.

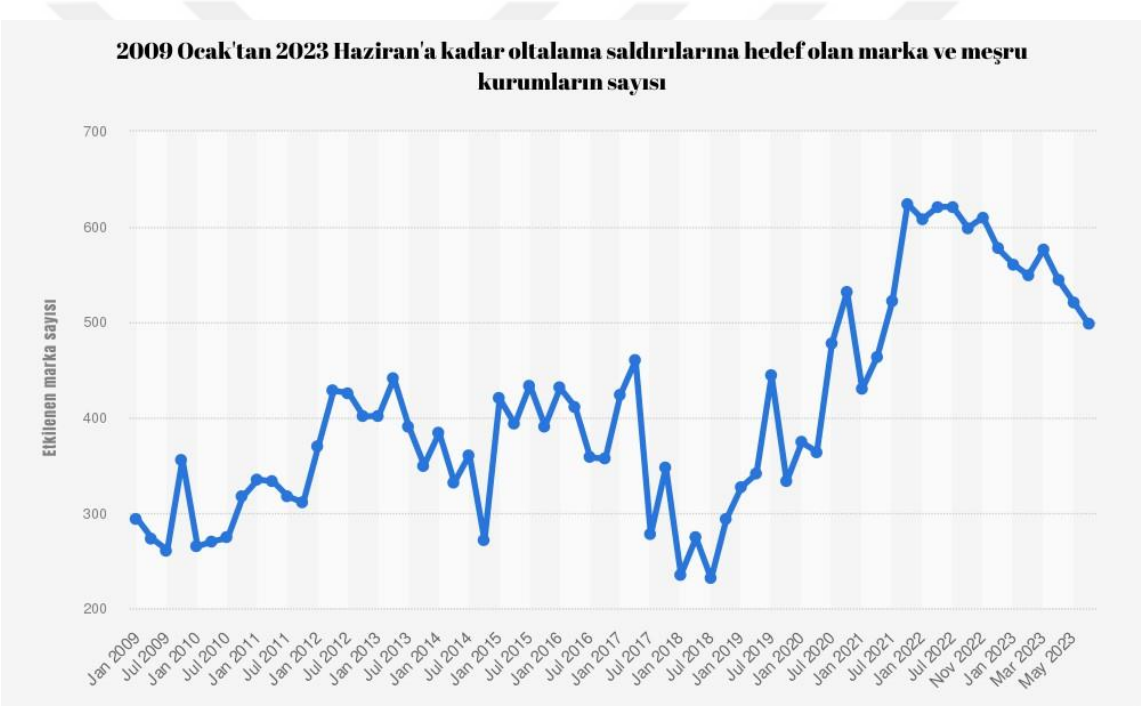


Şekil 2.9. Gerçek zamanlı küresel oltama saldırıları haritası [42]

Oltalama saldırıları, finansal kayıpların ötesinde geniş çaplı ekonomik etkiler yaratmaktadır. Her yıl gerçekleşen milyarlarca dolarlık doğrudan kayıpların yanı sıra, bu

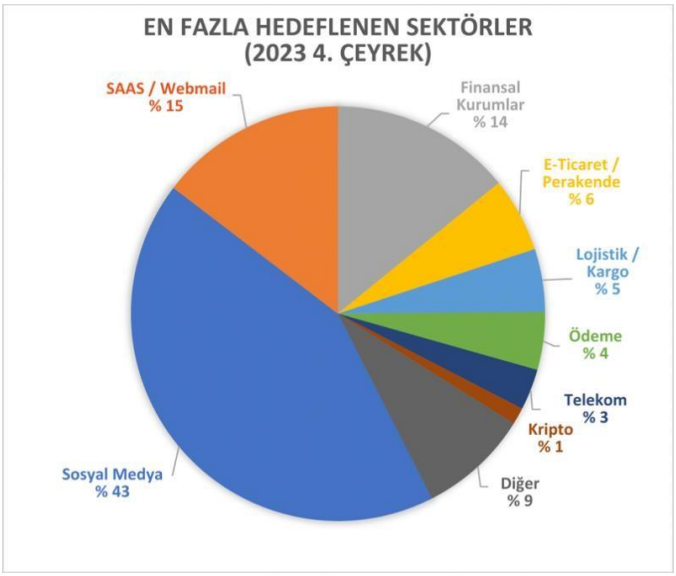
saldırıların yol açtığı iyileşme süreci, soruşturmalar ve alınan güvenlik önlemleri ek maliyetler yaratır. Dijital güvenilirlik zarar gördüğünde, e-ticaret ve online hizmetlerin gelişimi sekteye uğrayabilir. Küçük ve orta ölçekli işletmeler, müşterilerin güven kaybıyla karşı karşıya kalabilirler, bu da başarılı oltalama saldırılarının itibarlarına zarar verebilir [43].

Şekil 2.10'da Ocak 2009 ile Haziran 2023 arasında oltalama saldırılarına hedef olan marka ve meşru kuruluş sayısı görülmektedir [44]. Grafiğe göre saldırıya maruz kalan kuruluşların sayısında her ne kadar dalgalanmalar söz konusu olsa da özellikle Covid-19 pandemi döneminde uzaktan çalışma, alışveriş, eğitim gibi pek çok önemli işin dünya genelinde çevrimiçi platformlarda gerçekleşmesinden dolayı hızlı bir artış olduğu gözlemlenmektedir.



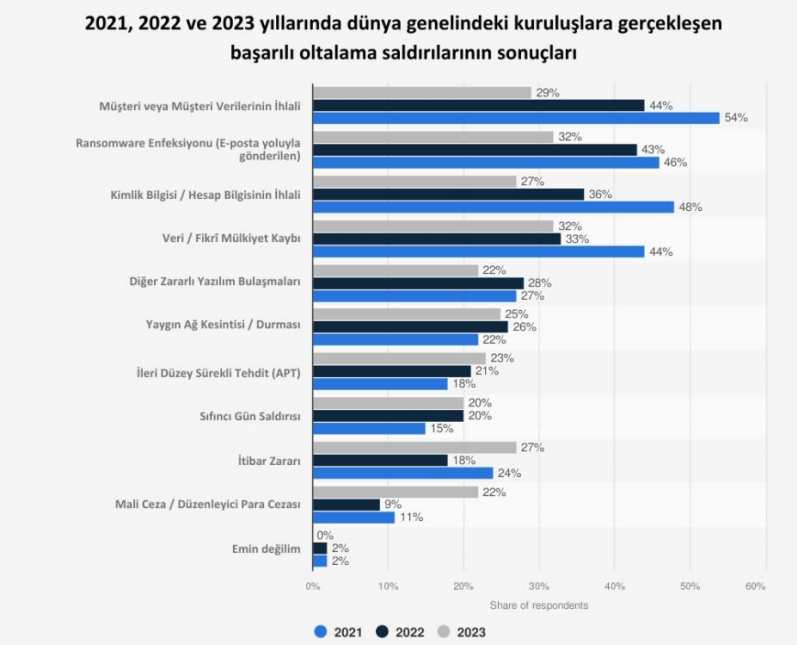
Şekil 2.10. Ocak 2009-Haziran 2023 oltalama saldırılarının hedef aldığı marka ve meşru kuruluşların sayısı [44]

2023'ün son çeyreğinde, APWG üyesi OpSec Security'nin araştırmasına [22] göre, sosyal medya platformlarına yönelik oltalama saldırıları tüm oltalama saldırılarının %42,8'ini oluşturdu ve üçüncü çeyrekteki %18,9'luk orana göre büyük bir artış gösterdi (Şekil 2.11). Finansal kurumlara yönelik saldırılar, üçüncü çeyrekteki tüm saldırıların %24,9'undan, dördüncü çeyrekte %14'e düştü. Çevrimiçi ödeme hizmetlerine yönelik saldırılar ise tüm saldırıların %4'ünü oluşturdu.



Şekil 2.11. 2023'ün 4. çeyreğinde oltalama saldırıları ile en fazla hedeflenen sektörler [22]

Proofpoint'un "State of the Phish 2024 (Oltalamanın Durumu 2024)" [45] raporuna göre, oltalama saldırılarının organizasyonlar üzerindeki etkileri 2023 yılında hem finansal hem de itibar açısından büyük hasarlara yol açmıştır. Organizasyonların %71'i en az bir başarılı oltalama saldırısına uğramıştır. Başarılı saldırı oranları bir önceki yıla göre düşse de, olumsuz sonuçlarda büyük artışlar görülmüştür; özellikle finansal cezalar ve itibar kaybı raporlarında sırasıyla %144 ve %50'lik artışlar yaşanmıştır.



Şekil 2.12. 2021-2023 arası dünya genelinde organizasyonlara gerçekleştirilen başarılı oltama saldırıları istatistikleri [46]

Şekil 2.12'ye göre, 15 ülke ve 17 sektörde, 7.500 son kullanıcı ve 1.050 güvenlik profesyoneli arasında gerçekleştirilen araştırmada; 2021 ve 2023 yılları arasında, organizasyonlara gerçekleştirilen başarılı oltalama saldırılarından etkilenme oranlarında değişimler gözlemlenmiştir. Genel olarak 2021'deki oranların Covid-19'dan kaynaklı yüksek olduğu görülmektedir. Örneğin; müşteri veya müşteri verilerinin ihlali yüzdesi %54'ten %29'a düşmüş olup bu durum önemli bir azalmayı işaret etmektedir. Ransomware enfeksiyonları da %46'dan %32'ye düşmüş olup, kimlik bilgisi ve hesap bilgisinin ihlal vakaları %48'den %27'ye azalmıştır. Bu düşüşler, kuruluşların siber güvenlik önlemlerindeki artan etkinliğini veya saldırılara karşı daha hazırlıklı olmalarını yansıtmaktadır. Ancak finansal ceza ve düzenleyici para cezaları 2023'te %22'ye yükselmiş, bu da ilgili düzenlemelere uyum konusunda artan zorlukları göstermektedir. Oltalama saldırılarının kurumlar ve bireyler üzerindeki etkileri geniş ve çeşitlidir. İstatistiklerden yola çıkarak bu etkiler şöyle özetlenebilir:

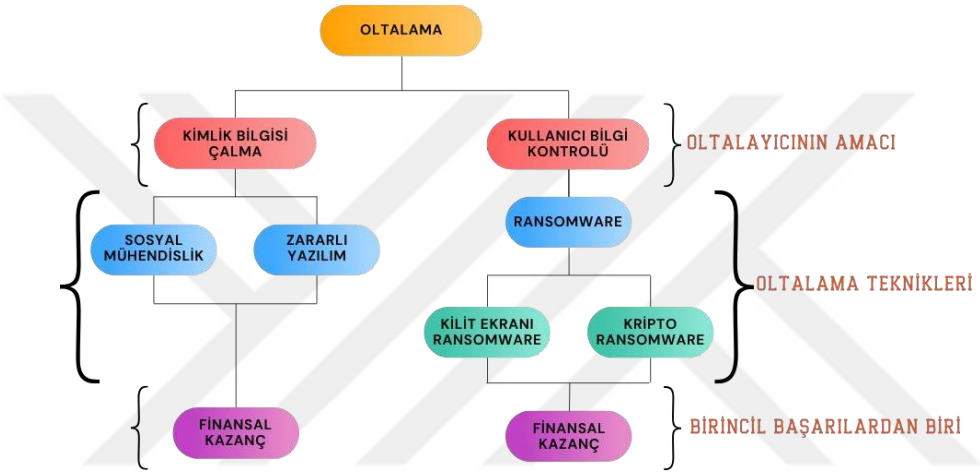
1. Kurumsal güvenliğin zayıflaması, kurum içi verilerin ve hassas bilgilerin tehlikeye girmesi.
2. Mali kayıplar, dolandırıcılık sonucu finansal zararlar ve düşen kar marjları.
3. İtibar zararı, müşteri güveninin sarsılması ve marka değerinin düşmesi.
4. Çalışanların ve müşterilerin kişisel bilgilerinin ifşa olması, kimlik hırsızlığı riskinin artması.
5. İş sürekliliğinin bozulması, saldırılardan kaynaklanan iş aksamaları ve verimlilik kayıpları.
6. Hukuki sorumluluklar ve cezai yaptırımlar, veri ihlallerinden dolayı oluşabilecek hukuki süreçler ve potansiyel cezalar.
7. Güvenlik önlemlerinin artırılması için yapılacak ek yatırımlar ve kaynakların yeniden dağıtılması.
8. E-ticaret ve dijital işlemlere olan güvenin azalması, kullanıcıların çevrimiçi aktiviteleri sınırlaması.

2.5. Oltalama Saldırı Türleri

Oltalama saldırıları, her biri benzersiz taktikler ve hedefler içeren çeşitli formlarda gerçekleşir. Bu çeşitli teknikleri anlamak, etkili önlemler geliştirmek için hayati önem taşır. Oltalama saldırılarının sınıflandırması ile ilgili literatürde farklı çalışmalar yer

almaktadır. Bunlardan bazılarında taksonomi adı altında ortak bir sınıflandırma yer alırken, bazılarında amaçlarına göre sınıflandırma yapılmış, bazılarında da doğrudan sınıflandırma yapmadan oltalama saldırı türleri incelenmiştir.

Örneğin, Chanti ve Chithralekha (2022) literatürdeki çalışmaları inceleyip oltalama tanımlarından yola çıkarak saldırıların amaçlarına yönelik bir sınıflandırma gerçekleştirmişlerdir ve bu saldırıların genellikle finansal kazanç elde etmek amacıyla kullanıcıların kimlik bilgilerini çalmayı amaçladığı belirtmişlerdir [47] (Şekil 2.13).

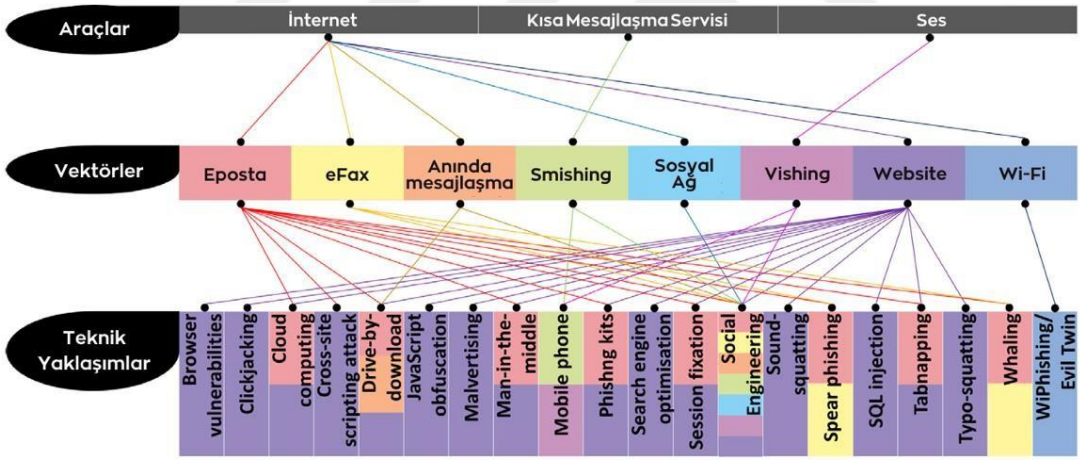


Şekil 2.13. Oltalama Sınıflandırması [47]

Heartfield ve Loukas (2015), siber saldırıların sınıflandırılması konusunda, saldırıların yöntemi, hedefi ve sürekliliği gibi çeşitli ölçütleri temel alan bir taksonomi önermişlerdir [48]. Bu çalışmada, saldırı yöntemleri bölümünde, e-posta ile oltalama, mızrak oltalama, balina avı, web sitesi üzerinden oltalama, vishing ve smishing gibi farklı teknikler ele alınmıştır. Ayrıca, saldırıların hedeflediği gruplar; bireysel kullanıcılar, kurumlar ve sistemler olarak ayırt edilir ve her bir grup için saldırı stratejileri ve bu stratejilerin getirdiği sonuçlar üzerinde durulmuş ve saldırıların sürekliliği de değerlendirilerek, tek seferlik saldırılar ile sürekli saldırılar arasındaki farklar ortaya konmuştur.

Chiew ve diğerleri (2018) çalışmalarında oltalama tekniklerini ve bu tekniklerin uygulanmasında kullanılan araçları, vektörleri ve teknik yaklaşımları derinlemesine incelemişlerdir [49]. Bu çalışmaya göre Şekil 2.14'te görüldüğü gibi oltalama saldırıları üç temel bileşenden oluşmaktadır:

1. **Oltalama Aracı:** Oltalama eylemlerinin kurbanlara iletildiği temel araçlardır. İnternet, ses ve kısa mesaj servisi (SMS) gibi araçlar, oltacıların kurbanlarına ulaşmasını sağlayan en yaygın yöntemlerdir. Özellikle internetin geniş kapsamlı kullanımı, oltacılara geniş bir erişim imkânı sunmaktadır.
2. **Oltalama Vektörleri:** Oltalama saldırılarını gerçekleştirmek için kullanılan iletim kanallarıdır. E-posta, web siteleri, anlık mesajlaşma ve sosyal ağlar gibi vektörler, oltacıların internet üzerinden saldırılarını yürütebilmeleri için mevcuttur. Ses tabanlı vishing ve SMS tabanlı smishing, diğer önemli oltalama vektörleridir.
3. **Teknik Yaklaşımlar:** Oltalama saldırılarının başarısını artırmak amacıyla kullanılan metotlardır. Bu yaklaşımlar arasında drive-by-download, ortadaki adam (MITM – man-in-the-middle), çapraz site betikçiliği (XSS – cross-site scripting) saldırıları, mızrak oltalama, balina avı, arama motoru optimizasyonu (SEO – search engine optimization), oturum sabitleme, kötü niyetli reklamcılık, sosyal mühendislik, JavaScript karıştırma, tarayıcı zafiyetleri gibi teknikler yer almaktadır.



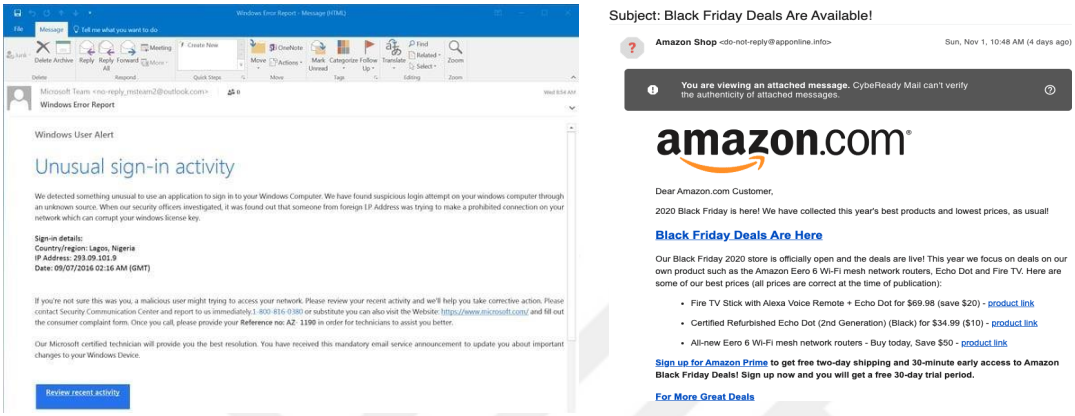
Şekil 2.14. Oltama Saldırı Teknikleri [49]

Bu sınıflandırmalara göre en yaygın oltalama saldırıları türleri örnekleriyle beraber şöyledir [50]:

2.5.1. E-posta oltalaması (E-mail phishing)

E-posta oltalama, en yaygın oltalama taktiklerinden biridir ve saldırganlar, meşru bir kuruluş gibi davranarak hedeflerden hassas bilgileri çalmaya çalışır. Bu tür saldırılar genellikle geniş bir hedef kitlesine ulaşmayı amaçlar. Oltalama e-postaları genellikle toplu

halde gönderilir ve içlerinde, Şekil 2.15'teki gibi tıklanınca alıcının cihazına zararlı yazılımlar yükleyen sahte web sitelerine yönlendiren bağlantılar veya zararlı dosyalar bulunur [36]. Aranılan bilgiler genellikle kimlik hırsızlığı, finansal dolandırıcılık ve hassas hesaplara yetkisiz erişim gibi çeşitli kötü amaçlar için sömürülebilecek kullanıcı adları, şifreler, kredi kartı detayları ve diğer kişisel verileri içerir [51].



Şekil 2.15. E-posta oltalama örnekleri [52,53]

E-posta oltalama stratejilerinde kullanılan ana yöntemlerden biri, güvenilen ve tanınmış olan bankalar, sosyal medya platformları, çevrimiçi perakendeciler veya devlet kurumları gibi kuruluşların kimliklerinin taklit edilmesidir [54]. Saldırganlar, bu tür saygın kaynaklardan gelen gerçek iletişimleri andıran yanıltıcı e-postalar hazırlar ve mesajların gerçekçi görünmesini sağlamak için özenle seçilmiş dil, logolar ve hatta sahte e-posta adresleri kullanırlar. Bu nedenle, alıcılar genellikle yanıltıcı bir güvenlik duygusuna kapılarak bu tür oltalama girişimlerini gerçek iletişimlerden ayırt etmekte zorlanır. Bu durum, bireyleri ve kuruluşları sürekli olarak bu tür dolandırıcılıklara karşı savunmasız bırakır ve finansal zararlara, veri ihlallerine ve diğer olumsuz sonuçlara neden olabilir.

Bir araştırma raporuna göre [55], 2023 yılında toplam 1,76 milyar oltalama e-postası gönderilmiş ve bu rakam kaydedilen en yüksek miktardır. Oltalama e-postalarının oranı 2022'ye göre %51 artmıştır.

2.5.2. Vishing (Voice phishing - Sesli oltalama)

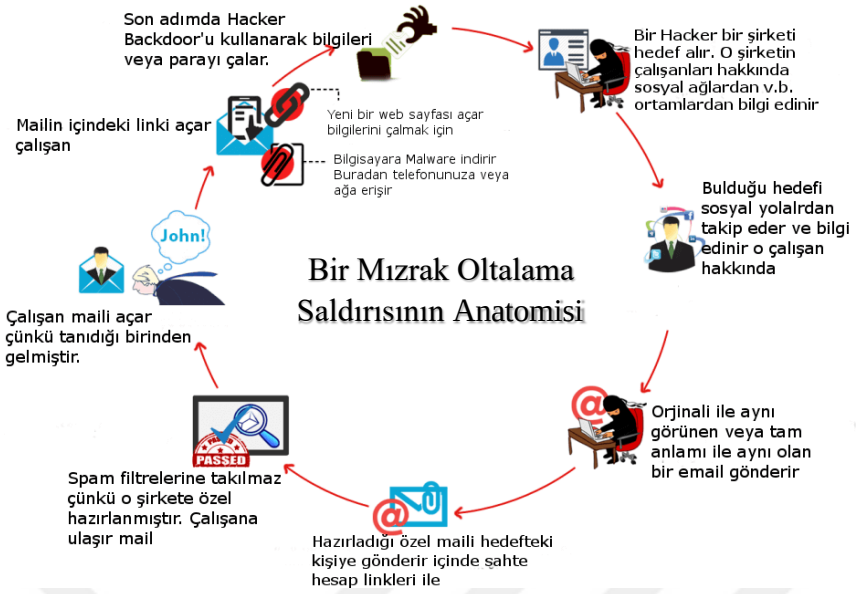
Sesli oltalama olarak da bilinen vishing, bireyleri telefon aramaları ve ses mesajları ile aldatma yöntemidir. Sıklıkla kullanılan tanıdık ya da otoriteye ait seslerle güven sağlanarak, hassas bilgiler ele geçirilir. Saldırganlar bunun için ses değiştiriciler

kullanabilir ve bu ses değiştiriciler hedeflenen kurbanlarla konuşurken saldırganın aksanını veya cinsiyetini gizler. Dünya genelinde giderek artan karmaşık vishing kampanyaları, siber suçluların psikoloji ve teknolojiyi kullanarak kişi ya da kurumları çok ciddi maddi zararlara uğratmaktadır.

Örneğin, Güney Kore'de vishing saldırılarında büyük bir artış yaşamış ve bu saldırılardan birinde, Ağustos 2022'de bir doktor, suçlulara 3 milyon dolar nakit, sigorta, hisse senetleri ve kripto para kaybetmiştir. Bu olayda, dolandırıcılar Güney Kore'deki bölgesel kolluk kuvvetleri yetkililerini taklit etmişlerdir [56]. Başka bir örnekte ise; 2023 yazında, saldırganlar Zscaler'in CEO'su Jay Chaudhry'i taklit ederek AI teknolojisini kullanarak bir vishing saldırısı gerçekleştirmiştir. Olayda saldırgan, bir Zscaler çalışanını WhatsApp üzerinden aramış, AI tarafından üretilen ses klonlama teknolojisi ile Jay'in sesini simüle ederek iletişim kuran saldırgan, uzun süreli etkileşimi ve potansiyel maruz kalmayı önlemek için hemen telefonu kapatmıştır. Saldırgan hemen ardından Whatsapp üzerinden Jay olarak poz vererek ağın zayıf olduğunu ve Zscaler çalışanından belirli bir miktar için hediye kartları satın almasını istemiştir. Bu durumu şüpheli bulan çalışan durumu bildirmiş ve araştırma sonucunda bunun bir vishing saldırısı olduğu tespit edilmiştir [56].

2.5.3. Mızrak oltalama (Spear phishing)

Bu oltalama yöntemi bireye ya da kuruma yönelik gerçekleştirilen hedefli bir saldırı yöntemidir [49]. Bu yüzden bu oltalama saldırısı *Hedef Odaklı Oltalama* olarak da adlandırılmaktadır. Mızrak oltalama, kitlesel ve rastgele e-posta oltalamasına kıyasla yüksek başarı oranı nedeniyle oltacılar tarafından popüler bir seçenek haline gelmiştir. Mızrak oltalama, kurbanın tanıdığı bir göndericiyi taklit eden özel olarak hazırlanmış e- postalar kullanır [49]. E-postanın içeriği, kurbanın şüphelenmesini tetiklemeyecek şekilde ona uygun olarak hazırlanır. Saldırganlar, kurbanın kişisel veya profesyonel hayatı hakkında önceden araştırma yaparak, e-postalarını daha inandırıcı hale getirirler. Şekil 2.16'da mızrak oltalama saldırısının nasıl gerçekleştiği görülmektedir. Mızrak oltalama saldırıları, genelde daha yüksek başarı oranlarına sahiptir; çünkü saldırganlar, kurbanların dikkatini çekecek ve güvenlerini kazanacak özel bilgilerle e-postalarını kişiselleştirirler. Bu yüzden, mızrak oltalama genel oltalama taktiklerinden çok daha tehlikeli ve zararlı olabilir. Mızrak oltalama özellikle İleri Sürekli Tehdit (APT) saldırısı gerçekleştirmek için oltalamacılar tarafından tercih edilen bir yöntemdir [57].



Şekil 2.16. Mızrak Oltalama Saldırısının Anatomisi [58]

Demokratik Ulusal Komitesi (DNC), 2016 ABD Başkanlık Seçimi'ni etkileyen önemli bir e-posta sızıntısına yol açan bir mızrak oltalama saldırısının kurbanı olmuştur [59]. Bu saldırının Rusya tarafından desteklenen bilgisayar korsanları tarafından düzenlendiği iddia edilmiştir. Hackerlar, DNC'nin iletişimlerine erişmek ve onları sızdırmak için DNC yetkililerinin e-postalarını hedef almıştır. Bu olay, siber güvenlik önlemlerinin önemini ve ulusal seçimler üzerinde yabancı etkilerin potansiyel tehdidini ön plana çıkarmıştır.

2022'de dünya çapında ABD, Avustralya, Hindistan, Birleşik Krallık, Fransa, Almanya, Avusturya, İsviçre, Belçika, Hollanda, Lüksemburg, Danimarka, Finlandiya, Norveç ve İsveç'ten ankete katılan 678 kuruluşun yarısından fazlası, mızrak oltalama saldırısı nedeniyle kötü amaçlı yazılım bulaşmalarıyla karşılaştı. Ayrıca neredeyse %50'si hassas veya gizli verilerin, kimlik bilgilerinin ve hesapların ele geçirilmesinin kaybedildiğini gördü. Yalnızca %3 herhangi bir etki fark etmediğini belirtti [60].

2.5.4. Balina avı oltalaması (Whaling)

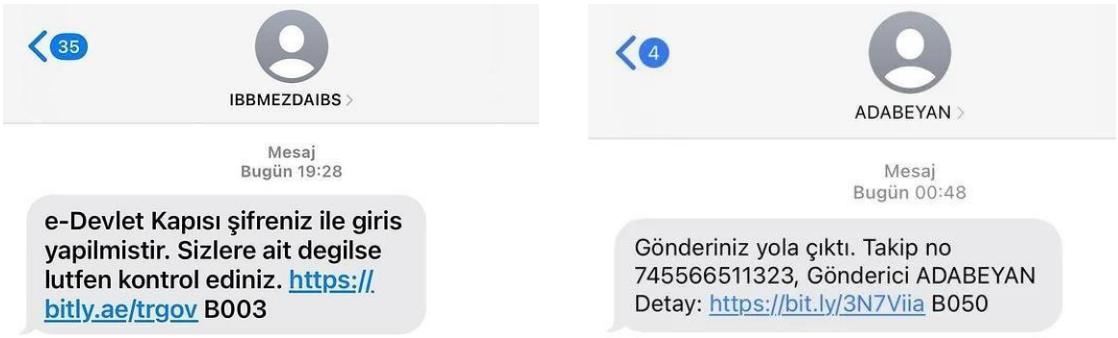
Bu oltalama türü ayrıca *CEO Dolandırıcılığı* olarak da bilinmektedir. Balina avı saldırısı, özellikle şirketlerin üst düzey yöneticilerini hedef alarak hassas bilgileri çalmayı amaçlayan özelleştirilmiş bir oltalama türüdür. Bu saldırılar, sahte e-postalar ve web siteleri kullanarak, genellikle yöneticilerin veya yetkili kişilerin kimliğini taklit eder. Saldırganlar, kurbanları yüksek değerli finansal işlemleri yetkilendirmeye veya zararlı

yazılımlar yüklemeye ikna etmek için sosyal mühendislik tekniklerinden yararlanır [61]. Örneğin bir saldırgan, kurbanın tanıdığı bir üst düzey yöneticinin e-posta adresini taklit ederek, acil ödeme yapılması gerektiğini talep edebilir. Bu saldırılar, kurbanlar üzerinde zaman baskısı yaratarak onları hızlı ve düşünmeden hareket etmeye itebilir. Balina avı, kurbanın daha önce ziyaret ettiği web sitelerini belirlemek için tarayıcı koklama gibi tekniklerle daha da sofistike hale getirilebilir, bu da saldırganın daha inandırıcı sahtekarlıklar yapmasına olanak tanır.

2016 yılında Snapchat, üst düzey bir çalışanının CEO dolandırıcılığı içeren bir e-postaya kanması sonucu bir balina avı saldırısına uğramış ve çalışan maaş bilgilerini ifşa etmiştir. Snapchat, olayı FBI'a bildirmiş ve çalışanlarına iki yıl boyunca ücretsiz kimlik hırsızlığı sigortası sunmuştur [61].

2.5.5. Smishing (SMS phishing - SMS oltalama)

SMS oltalama veya smishing, vishinge benzer, ancak smishing saldırganların SMS veya anlık mesajlar aracılığıyla kurbanları manipüle ettiği bir yöntemdir. Bu tür saldırılarda, saldırganlar genellikle bir banka, sigorta şirketi, e-devlet veya tanınmış bir marka gibi güvenilir bir kaynaktan gönderiliyormuş gibi mesajlar göndererek alıcının güvenini kazanır (Şekil 2.17). Bu saldırılar URL tabanlı, e-posta tabanlı ve telefon numarası tabanlı olmak üzere üç kategoriye ayrılabilir [62]. URL tabanlı smishing'te, kurbanlar bir mesaj içindeki link aracılığıyla zararlı bir siteye yönlendirilir ve burada genellikle ödül puanları ya da hediyeler vaadiyle kişisel ya da finansal bilgi girmeleri istenir. Bazı durumlarda, bu siteler kurbanın cihazına zararlı APK (Android Package Kit) dosyaları indirebilir. E-posta ve telefon numarası ile gerçekleştirilen smishing saldırılarında ise, kurban saldırganla iletişime geçmek için verilen e-posta adresini veya telefon numarasını kullanmaya teşvik edilir. Smishing oltalama saldırısının tehlikeli olmasının nedeni, birçok kurbanın bu tür mesajları tanıyamaması ve zararlı içeriğin farkında olmamasıdır.



Şekil 2.17. Örnek smishing oltalama kısa mesajı [63,64]

2.5.6. Sosyal medya oltalaması (Social media phishing)

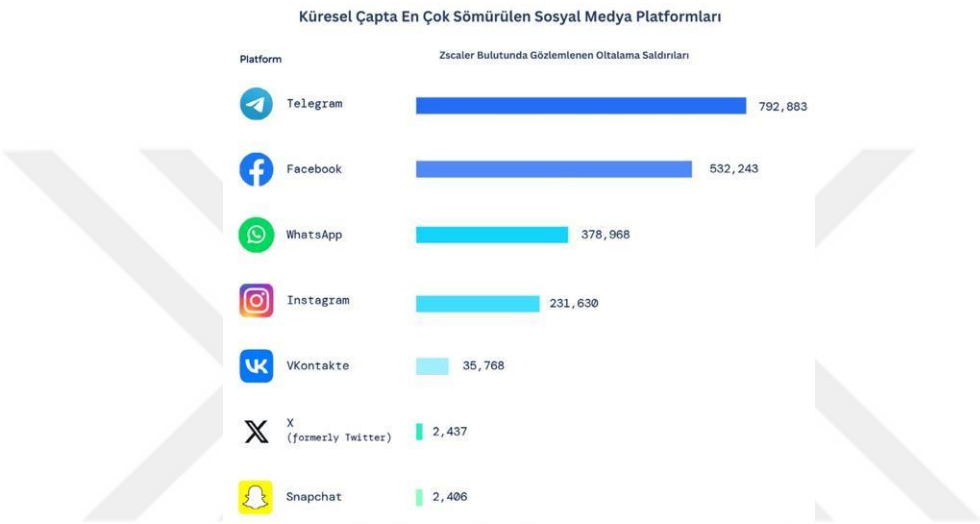
Sosyal medya, günümüzde siber suçlular için oltalama saldırılarını yürütmek üzere tercih edilen başlıca alanlardan biri haline gelmiştir. Kişisel bilgilerin yoğun bir şekilde paylaşıldığı sosyal medya platformları, saldırganların sosyal mühendislik tekniklerini kullanarak hassas verilere ulaşmalarını kolaylaştırır. Facebook, Instagram, Snapchat ve LinkedIn gibi dünya genelinde milyarlarca insanın kullandığı bu platformlar, oltalama girişimleri için ideal bir ortam sunar.

Sosyal medyada gerçekleşen saldırılar, genellikle kullanıcıyı zararlı web sitelerine yönlendiren bağlantılar veya kişisel bilgileri istismar etmeyi amaçlayan dolandırıcıların arkadaşlık teklifleri içerebilir. Bu saldırılar, sahte indirim teklifleri, anketler, yarışmalar veya videolar gibi cazip görünen içeriklerle desteklenir. Ayrıca, kullanıcı yorumları veya videolar üzerinden yapılan etkileşimler, kullanıcıların dikkatini çekmek ve onları aldatmak için kullanılır.

Örneğin, 2016 yılında LinkedIn kullanıcıları, platformun resmi iletişimlerine benzeyen e-postalarla hedef alındı [59]. Bu oltalama girişimlerinin amacı, kullanıcıların giriş bilgilerini kaparak hassas bilgilere yetkisiz erişim sağlamaktı. Bu olay, phishing tehlikeleri konusunda sürekli eğitim ve e-posta doğrulamanın önemini hatırlattı ve sosyal medya platformlarının kullanıcı koruma sorumluluğunu tartışmaya açtı. LinkedIn, bu duruma güvenlik ve kullanıcı eğitimi programlarını güçlendirerek yanıt verdi. Diğer bir olayda da 2020'de Twitter, yüksek profilli hesapların bir Bitcoin dolandırıcılığını tanıtması için ele geçirildiği büyük bir güvenlik ihlali yaşadı [59]. Bu olay, sosyal mühendislikle gerçekleştirilen saldırılarla Twitter'ın güvenlik zafiyetlerini ortaya çıkardı ve platformun karmaşık siber tehditlere karşı korunması için sürekli güvenlik iyileştirmelerine olan

ihtiyacı vurguladı. Saldırı, Twitter'ın mali kayıplar yaşamasının yanı sıra itibarını ve kullanıcı güvenini de olumsuz etkiledi.

Sosyal medyanın hüküm sürdüğü bir dünyada, saldırganlar bu platformları oltalama çabaları için giderek daha fazla kullanıyorlar. İstatistiksel olarak sosyal medya oltalama saldırıları incelendiğinde Şekil 2.18, ThreatLabz [56] tarafından gözlemlenen en çok hedef alınan sosyal medya platformlarını göstermektedir.



Şekil 2.18. Oltalama saldırılarında hedef alınan en popüler sosyal medya platformları [56]

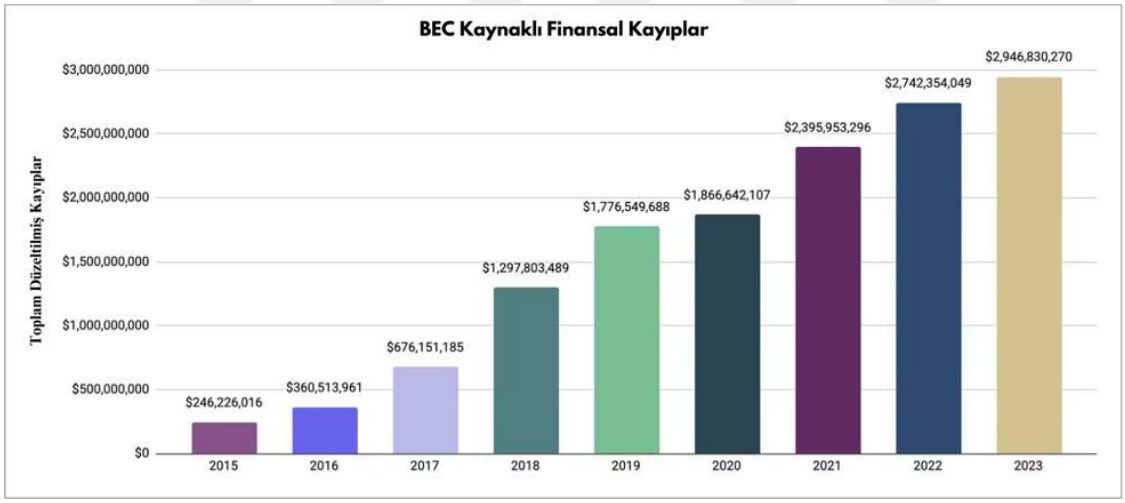
Telegram, 792.883 oltalama girişimi ile kötü niyetli faaliyetler için popüler bir hedef olmaya devam etmektedir [56]. Saldırganlar, kullanıcı hesaplarına yetkisiz erişim sağlamak veya kötü amaçlı içerik dağıtmak için Telegram'ın güvenlik önlemlerindeki zafiyetleri sömürmeye çalışmaktadırlar. 532.243 oltalama girişimi ile Facebook, kullanıcı verilerini ve gizliliğini koruma konusunda sürekli zorluklarla karşılaşmaya devam etmektedir [56].

2.5.7. BEC (Business Email Compromise – İş e-postası tehdidi)

BEC saldırıları, son birkaç yılda giderek artan, gelişen ve büyüyen bir tehdit haline gelmiştir. İş E-Postası Tehdidi olarak bilinen bu oltalama saldırıları, dolandırıcıların finansal kazanç elde etmek için kurbanların büyük meblağlarda para transferi yapmalarını veya hassas bilgileri suçlu yönetimindeki hesaplara göndermelerini ikna ettikleri bir dolandırıcılık türüdür [65]. Bu saldırılar, özellikle finansal işlemler yapan kuruluşları hedef alır ve sosyal mühendislik yoluyla gerçekleştirilen kötü niyetli e-postaları kullanır.

BEC saldırıları beş farklı şekilde gerçekleşebilir [65]. Sahte fatura dolandırıcılığı durumunda, yabancı bir tedarikçiyle çalışırken saldırgan iki şirket arasındaki var olan ilişkiyi kullanarak, çalışanın gerçek bir tedarikçiden geldiğine inandığı fakat içerisinde saldırganın banka hesap bilgilerinin yer aldığı bir fatura ödemesi talep eder. Kişisel dolandırıcılık veya CEO hesabı türünde, saldırgan acil banka transferi yapılmasını talep ederken, bu isteğin üst düzey bir yetkiliden geldiği yönünde yanıltıcı bilgiler verir. Ödeme çalışanının e-posta hesabının hacklenmesi durumunda saldırgan, kendi hesabına ödemeler yapılmasını sağlar. Yönetici veya avukat kimliğinin kullanılması durumunda, saldırgan gizlilik ve hassasiyet gerektiren durumlar için banka transferleri talep eder. Veri hırsızlığı girişiminde ise, saldırgan yöneticinin e-posta hesabını ele geçirdikten sonra, finansal işlemlerle ilgili çalışanlardan hassas bilgileri sızdırarak bunları kendi finansal yararına kullanır.

2023 yılında, FBI İnternet Suçları Şikayet Merkezi (IC3), 2.9 milyar doların üzerinde düzeltilmiş kayıpla 21.489 BEC şikayeti almıştır (Şekil 2.19) ve BEC saldırısı, FBI IC3 tarafından takip edilen en maliyetli ikinci suç türü olmuştur [66].



Şekil 2.19. 2015-2023 arası BEC kaynaklı finansal kayıplar [67]

2013 ve 2015 yılları arasında, Evaldas Rimasauskas ve ortakları, Quanta Computer adında sahte bir şirketten gelen ikna edici sahte faturalar kullanarak Facebook ve Google'ı hedef alan sofistike ve milyonlarca dolarlık bir BEC saldırısını başarıyla gerçekleştirmişlerdir [68]. Bu saldırgan grup, işlemlerin başlatılmasının ardından bankaların fonları kabul etmelerini sağlamak için sahte avukat mektupları ve sözleşmeler de kullanmıştır. Bu stratejiler sayesinde grup üyeleri iki teknoloji devinden toplamda 121 milyon dolar çalma

imkanına erişmişlerdir. Bu olay, BEC saldırılarının ne kadar yıkıcı olabileceğini ve teknoloji şirketlerinin bile nasıl savunmasız kalabileceğini gözler önüne sermektedir.

2.5.8. Quishing (QR code phishing - QR kod oltalama)

QR kod oltalaması, siber suçluların kurbanları aldatarak onları zararlı web sitelerine yönlendirmek için QR kodları kullandığı nispeten yeni bir yöntemdir. Bu taktik, özellikle fiziksel ya da dijital olarak geniş kitlelere kolayca ulaşılabilecek alanlarda etkilidir. Kullanıcılar genellikle QR kodlarının nereye bağlandığını göremediklerinden, bu durum dolandırıcılar için ideal bir fırsat yaratır. Kurbanlar, sahte bir reklam, sahte bir hizmet teklifi veya güvenli olduğuna inandıkları bir kaynaktan gelen bir mesaj gibi masum görünen bir kılıf altında zararlı QR kodlarını tarayabilirler.

QR kod dolandırıcılıklarında, tehdit unsurları kurbanları aldatarak QR kodlarını taramaya ikna eder ve bu kodlar sonuçta zararlı bağlantılara yönlendirir. Bu dolandırıcılık türü, zararlı yönlendirmeler, pdf dosyası gibi e-posta ekleri ve diğer dijital iletişim formları dahil olmak üzere çeşitli yöntemlerle gerçekleştirilir. Tehdit unsurlarının en yaygın yöntemi, QR resmi içeren bir pdf dosyasını e-posta yoluyla göndermektir. Kurban tarafından taratılan bu kod kişiyi bir oltalama web sitesine yönlendirmektedir [56].

E-posta yoluyla gönderilen zararlı QR kodları çeşitli amaçlar için kullanılabilirken, öncelikli olarak oltalama için kullanılmaktadır. Yapılan istatistiksel çalışmalarda tespit edilen QR kodu saldırılarının %89,3'ü oltalama saldırılarıdır [69]. 2023 yılının ikinci yarısında toplanan verilere göre, siber suçlular QR kodu oltalama saldırılarında özellikle iki stratejiyi sıklıkla kullanmışlardır: İlki tüm quishing saldırılarının yaklaşık %27'sinde görülen çok faktörlü kimlik doğrulama (MFA-Multi-factor authentication) ile ilgili sahte bildirimler, ikincisi ise QR kodu saldırılarının yaklaşık %21'inde uygulanan, hedeflere paylaşılmış bir dokümanla ilgili sahte bildirimler göndermektir [69]. Şekil 2.20'de yer alan örnek Quishing saldırısında saldırgan, kurbanın MFA yönteminin o gün sona ereceğini ve Microsoft 365 uygulamalarına erişimini kaybetmemesi için yeniden doğrulanması gerektiğini belirtmektedir.



Şekil 2.20. Gerçek hayattan bir Quishing saldırı örneği [69]

2.6. Oltalama Saldırıları Korunma Yolları

Naqvi ve diğerleri (2023), 2018 başından 2023 Mart'ına kadar ana dijital kütüphanelerde yer alan 248 makale üzerinden sistematik bir literatür taraması yapmış ve bunun sonucunda da kuruluşlar ve son kullanıcılar için anti-oltalama yönergeler ve önerilerini sunmuşlardır [70]. Bu yönergeler ve öneriler, özellikle oltalama saldırılarına karşı etkili stratejilerin belirlenmesinde ve uygulanmasında yardımcı olacak şekilde tasarlanmıştır.

Kuruluşlar için belirlenen anti-oltalama yönerge ve önerileri, kuruluşların oltalama saldırılarına karşı daha dirençli hale gelmelerine yardımcı olmak için tasarlanmıştır ve hem teknoloji hem de insan odaklı yaklaşımları içermektedir. Bu öneriler, kuruluşların oltalama saldırılarına karşı korunmalarını sağlamak için kapsamlı stratejiler içermektedir. Kuruluşlar için belirlenen anti-oltalama yönerge ve önerileri; güvenlik politikalarının uygulanması, erişim kontrol sistemlerinin kurulması, uç nokta güvenliğinin sağlanması, eğitim ve farkındalık programlarının kullanılması, cihaz politikalarının geliştirilmesi ve genel tavsiyelerin dikkate alınması şeklinde ana kategorilere ayrılmıştır [70]. Bu ana kategoriler Çizelge 2.1'de özetlenmiştir.

Çizelge 2.1. Kuruluşlar için anti-oltalama yönerge ve önerileri [70]

Yönergelerin Ana Kategorileri	Yönergelerin Özeti
Güvenlik politikalarını takip et	Kuruluşlar, riskli ve yüksek riskli kullanıcılar için özel güvenlik ve anti-oltalama eğitimleri içerecek şekilde şirket politikalarını güncellemeli, raporlama protokolleri ve güvenli çalışma rutinleri oluşturmalıdır. Ayrıca, şifre koruma politikaları belirlemeli ve uygulamalıdır.
Erişim kontrolü uygula	Çok faktörlü kimlik doğrulama sistemleri (MFA), web tuzakları ve DMARC e-posta doğrulama sistemleri gibi yöntemlerle güçlü erişim kontrol mekanizmaları kurulmalıdır.
Uç nokta güvenliğini sağla	Akıllı ağ tehdit algılama sistemleri geliştirilmeli, bilgisayar donanım ve yazılımları düzenli olarak güncellenmeli, antivirüs programları ve e-posta engelleyiciler kullanılmalıdır.
Eğitim ve farkındalık programları kullan	Hata yapıldığında hemen eğitim materyalinin sunulduğu, aldatıcı ipuçlarına dayalı ve insan merkezli tasarım yaklaşımlarıyla desteklenen eğitim ve farkındalık programları düzenlenmelidir. Ayrıca, sanal laboratuvarlar ve oyunlaştırma teknikleri kullanılarak etkileşimli öğrenme ortamları oluşturulmalıdır.
Cihazlar için politikalar geliştir	Cihazların yaşam döngüsü yönetimi için stratejiler geliştirilmeli, tüm cihazların düzenli olarak envanteri çıkarılmalı ve zamanında güncellemeler için politikalar oluşturulmalıdır.
Tavsiyeleri dikkate al	Gelen çağrılar yetkilendirilmeli, bilgi paylaşımı konusunda dikkatli olunmalı ve siber güvenlik uzmanları işe alınmalıdır. Yönetim kurulu üyeleri, CISO'lar ve güvenlik profesyonelleri için özel tavsiyeler sunulmuş, düşük sürtünmeli çözümler geliştirilmesi ve güvenlik kültürünün tüm organizasyona yayılması hedeflenmiştir.

Son kullanıcılar için belirlenen yönergeler ve önergeler ise, kullanıcıların oltalama tehditlerine karşı bilinçlenmelerini ve güvenlik önlemlerini artırmalarını amaçlamaktadır. Bu öneriler iki ana kategori altında toplanmıştır: Bilinçlendirme stratejileri kullanmak ve güvenlik tavsiyeleri uygulamak [70]. Bu ana stratejilerin altında kullanıcılara önerilenler Çizelge 2.2'de özetlenmiştir.

Çizelge 2.2. Son kullanıcılar için anti-oltalama yönerge ve önerileri [70]

Yönergelerin Ana Kategorileri	Yönergelerin Özeti
Bilinçlendirme stratejisi olarak kullan	• Bilinmeyen veya şüpheli kaynaklardan gelen e-postalara karşı uyanık olun. • Anonim göndericilerden gelen e-postalara güvenmeyin. • Şüphe durumunda alanında uzman bir profesyonele başvurun. • Oltalama potansiyeli taşıyan e-postaları açmadan doğrudan silin. • Kişisel bilgileri yalnızca kaynağından emin olduğunuz durumlarda paylaşın. • Zararlı bağlantılara tıklamadan önce iki kez düşünün. • Açılır pencerelere karşı dikkatli olun.
Güvenlik tavsiyesi kullan	• Bilgisayar donanımı ve yazılımını düzenli olarak güncelleyin. • Antivirüs yazılımı kullanarak bilgisayarınızı tehditlere karşı koruyun. • Çevrimiçi hesaplarınızı düzenli olarak kontrol edin. • Güçlü ve benzersiz şifreler kullanın. • Farklı hesaplarda aynı şifreleri kullanmaktan kaçının. • Web sitelerini ziyaret ederken URL'in "https://" ile başladığından emin olun. • Güvenlik sertifikalarını kontrol edin. • Hassas bilgileri girerken halka açık bilgisayarları kullanmaktan kaçının. • Bilgisayarınızı gözetimsiz bırakmayın. • Bilinmeyen göndericilerden gelen ekleri açmayın. • Bu e-postalardaki bağlantılara tıklamaktan kaçının. • İki faktörlü kimlik doğrulama (2FA) sistemi kullanın. • Kimlik doğrulama uygulamalarını SMS/telefon yerine tercih edin. • Şüpheli bağlantıları kontrol etmek için araçlar kullanın. • Tarayıcının oltalama listesini etkinleştirin. • Açılır pencereleri engelleyin.

2.7. Literatür Araştırması

Literatürde farklı kuruluşlarda çalışan ya da okuyan bireylerin oltalama saldırıları farkındalığını ölçen çalışmalar yer almaktadır.

Mohebzada ve diğerleri (2012)[71], 10000 üniversite çalışanı ve öğrencisi üzerinde oltalama saldırılarının yaygınlığını ve etkinliğini değerlendirmek amacıyla büyük ölçekli iki oltalama deneyi gerçekleştirmişlerdir. Araştırmacılar, katılımcıların oltalama e- postalarına nasıl tepki verdiklerini gözlemlemişler, bu süreçte e-postaların tasarımı ve sunumu üzerinde çeşitli değişiklikler yapmışlardır. Bulgular, katılımcıların oltalama e-

postalarını tanıma ve uygun şekilde tepki verme konusunda ciddi zorluklar yaşadıklarını ortaya koymuştur.

Kuzey Kentucky Üniversitesi'nden 150 üniversite öğrencisi üzerinde yapılan bir çalışmada [72], güvenlik farkındalığı eğitiminin, kişilerin kötü amaçlı linklere tıklama oranları üzerindeki etkisi araştırılmıştır. Araştırmada, eğitim düzeylerine göre farklı gruplara ayrılan katılımcılara yönelik farklı güvenlik farkındalığı eğitimleri verilmiştir. Bu gruplar; eğitim almayan kontrol grubu, belge ile eğitim alan grup ve sınıf içi sunum ile eğitim alan grup olarak üçe ayrılmıştır. Çalışmanın bulgularına göre, güvenlik farkındalığı eğitimi alan gruplar, eğitim almayan kontrol grubuna kıyasla kötü amaçlı bağlantılara tıklama oranlarında önemli ölçüde düşüş göstermiştir. Özellikle belge ile eğitim alan grup, kampanya süresince tıklama oranlarında en büyük düşüşü yaşamıştır, bu da güvenlik eğitiminin kullanıcı davranışları üzerinde etkili olduğunu göstermektedir.

Othman Mustafa ve diğerleri (2019) [73] Malezya'daki bir enstitüdeki meslek öğrencilerinin oltalama saldırıları farkındalıklarını artırmayı amaçlayan bir çalışma yapmışlardır. Bu çalışma, mesleki eğitim öğrencilerinin oltalama saldırılarına karşı farkındalığının artırılmasına yönelik bir model sunmaktadır. Araştırmada, öncelikle öğrencilerin mevcut oltalama saldırıları farkındalıkları seviyesi ölçülmüş, ardından geliştirilen eğitim modeli ile eğitim müdahalesi yapılmış ve sonuçlar analiz edilmiştir. Bulgular, önerilen modelin öğrencilerin oltalama saldırıları bilgi ve farkındalıklarını güçlendirmede etkili olduğunu göstermektedir.

Gordon ve diğerleri (2019) [74] gerçekleştirdikleri çalışma ise ABD'deki sağlık kurumlarındaki çalışanların oltalama saldırılarına karşı duyarlılığını değerlendiren uzun dönemli bir çalışmadır. 2011 ve 2018 yılları arasında, ABD'de coğrafi olarak farklı yerlerde bulunan altı sağlık kurumu çalışanlarına yönelik 95 oltalama simülasyonu kampanyası yürütülmüştür. Toplamda 2.971.945 e-posta gönderilmiş ve bu e-postaların %14,2'si (422.062) tıklanmıştır. Araştırma, tekrarlanan oltalama kampanyalarının, bir sonraki oltalama e-postasına tıklama olasılığını azalttığını ortaya koymuştur, bu da oltalama simülasyonu ve farkındalık oluşturma çalışmalarının potansiyel faydalarını göstermektedir. Ancak, tespit edilen tıklama oranları, hastaneler için önemli bir siber güvenlik riskini temsil etmektedir.

Bir araştırmada [75] İtalya'daki bir şirketteki çalışanların oltalama saldırılarına karşı hassasiyetini incelenmiştir ve 191 çalışan üzerinde gerçekleştirilmiştir. Çalışma, aciliyet ve otorite gibi ikna edici tekniklerin, demografik özelliklerin ve yerleşik eğitimin, çalışanların oltalama e-postalarına yanıt verme olasılıkları üzerindeki etkilerini değerlendirmiştir. Bulgular, aciliyet hissi uyandırıldığında çalışanların daha savunmasız olduğunu, demografik faktörlerin etkisinin sınırlı olduğunu ve eğitimin, beklenen etkide bir azalma sağlamadığını göstermiştir.

Yenal Arslan'ın "Oltalama Saldırıları Farkındalık Tatbikatı Örneği" [76] başlıklı çalışmasında Türkiye'de 33.000 çalışanı ve 400 taşra birimi olan büyük bir devlet kurumunda, bu kurumun çalışanları üzerinde gerçekleştirilen bir oltalama saldırısı simülasyonu incelenmiştir. Çalışmada, çalışanların sahte web sayfalarına ve e-postalara tepkileri ölçülmüş, ayrıca 20 farklı lokasyona USB bellekler yerleştirilerek, bulan personelin bu belleklere karşı davranışları incelenmiştir. Değerlendirme iki aşamada ve yedi farklı senaryo üzerinden yapılmış, her personel statüsü için ayrı oltalama testleri uygulanmıştır. Elde edilen bulgular, çalışanların oltalama e-postalarını tespit etme konusunda düşük bir başarı oranına sahip olduğunu göstermiştir. Özellikle taşra personelinin sahte web sayfalarına bilgi girişi yapma oranı daha yüksek bulunmuş, yönetici kademesindeki kişilerin ise daha dikkatli olduğu ancak yine de saldırılara maruz kaldıkları tespit edilmiştir.

Suudi Arabistan'da oltalama saldırılarına karşı farkındalığı artırmayı amaçlayan başka bir araştırmada [77] Suudi internet kullanıcılarının oltalama saldırıları hakkında bilgi ve farkındalık düzeylerini ölçmek için 1208 kullanıcıya bir anket uygulanmıştır. Araştırma, pandemi döneminde oltalama saldırılarının arttığı, bu tür saldırıların kullanıcı bilgisi ve farkındalığını hedef aldığı ve genellikle yüksek başarı oranına sahip olduğu bir dönemi kapsamaktadır. Anket sonuçlarına göre genç kullanıcıların yaşlı kullanıcılardan daha fazla bilgiye sahip olduğunu göstermektedir. Bu durum, eğitim ve bilgilendirme faaliyetlerinin özellikle yaşlı kullanıcılara yönelik olması gerektiğini belirtmektedir. Ayrıca, kullanıcıların kendilerini koruma konusundaki güvenleri yeterli değildir. Eğitim ve SMS kampanyalarının farkındalığı artırabileceği ancak tüm kullanıcılara ulaşmadığı belirlenmiştir.

Büyük ölçekli bir firmada 15 aylık uzun bir süreçte 14.773 çalışan üzerinde yürütülen bir çalışmada [78], çalışanların oltalamaya karşı duyarlılıklarını keşfetmek amacıyla, normal iş akışlarına entegre edilmiş oltalama simülasyonu e-postaları gönderilerek ve e-posta istemcisine eklenen bir raporlama butonu aracılığıyla şüpheli e-postaların bildirilmesini sağlayarak gerçekleştirilmiştir. Ana bulgular arasında, belirli çalışan demografilerinin oltalamaya daha yatkın olduğunu, gömülü oltalama eğitiminin çalışanların dirençlerini artırmak yerine onları daha da savunmasız hale getirebileceğini ve çalışanların toplu bir oltalama algılama mekanizması olarak kullanılmasının etkili olduğunu gösteren sonuçlar bulunmaktadır.

Başka bir oltalama saldırıları simülasyonu çalışması [79], Tayland'daki büyük bir finansal kuruluşta yaklaşık 20.000 çalışanın oltalama saldırıları farkındalığını ölçmek amacıyla gerçekleştirilmiştir. Üç aşamalı bir süreçle gerçekleştirilen bu çalışmada, ilk olarak çalışanlara bir oltalama saldırısı simülasyonu yapılmış, ardından bilgi aktarımının gerçekleştirildiği bir eğitim verilmiş ve son olarak farklı içerikli ikinci bir oltalama saldırısı simülasyonu daha yapılmıştır. Bulgular, bilgi aktarımından sonra çalışanların siber güvenlik farkındalığının önemli ölçüde arttığını göstermiştir. Ayrıca, cinsiyetin Tayland'daki siber güvenlik ekosisteminde önemli bir rol oynadığı bulunmuş, kadın çalışanların erkek çalışanlara kıyasla daha yüksek bir siber güvenlik farkındalığına sahip olduğu tespit edilmiştir. Farklı nesiller arasında (Y ve X kuşakları ile Boomer'lar) siber güvenlik farkındalığı üzerinde anlamlı bir etki bulunmamıştır.

Öğrencilerin ve akademisyenlerin oltalama saldırılarına karşı ne kadar bilinçli olduğunu belirlemek, simüle edilmiş oltalama saldırılar ve gömülü eğitim kampanyasıyla bu farkındalığı nasıl artırabileceklerini incelemek için Yeoh ve diğerleri (2021) büyük bir eğitim kurumu üzerinde bir vaka çalışması yürütmüşlerdir [80]. Çalışmanın uygulanma yöntemi, katılımcılara farklı türlerde oltalama e-postaları gönderilerek onların bu e-postalara nasıl tepki vereceklerinin gözlemlenmesi şeklinde olmuştur. Eğer bir katılımcı oltalama e-postasına yanıt verirse veya zararlı bağlantıya tıklarsa, bu durum onların bir sonraki e-posta saldırısına nasıl tepki vereceklerini öğrenmelerine yardımcı olacak şekilde bir eğitim sayfasına yönlendirmiştir. Bu eğitim, operant koşullandırma teorisi temel alınarak düzenlenmiştir, yani doğru davranışlar ödüllendirilirken yanlış davranışlar cezalandırılarak katılımcıların davranışlarının değiştirilmesi amaçlanmıştır. Sonuç olarak, bu kampanya sırasında katılımcıların oltalama e-postalarını bildirme oranlarında artış

gözlenmiş ve e-posta bağlantılarına tıklama oranlarında azalma görülmüştür. Ayrıca, kampanya süresince katılımcıların oltalama saldırılarına karşı dirençlerinin nasıl geliştirilebileceğine dair değerli bilgiler sunmuş ve bu tür bir eğitimin etkinliğini göstermiştir.

Rizzoni ve diğerleri (2022) çalışmalarında İtalya'daki büyük bir hastanede 6000'den fazla sağlık çalışanlarına oltalama simülasyonu kampanyaları uygulamışlardır [81]. Araştırmadaki bulgular, özelleştirilmiş oltalama e-postalarının, genel olanlara kıyasla daha yüksek oranda açılıp üzerindeki bağlantılara tıklandığını göstermiştir. Ancak, organizasyon içinde karşılaşılan sorunlar nedeniyle kampanyalar planlandığı gibi yürütülememiştir.

Carroll ve diğerleri(2022) gerçekleştirdikleri çalışmalarında [82] COVID-19 pandemisi süresince artan uzaktan çalışma ve öğrenme yöntemlerinin siber güvenlik endişelerini nasıl etkilediği incelenmiştir. Araştırmacılar, katılımcılara çeşitli e-posta kategorileri üzerinden bir dizi deney yaparak, modern oltalama saldırılarının tespit edilmesindeki zorlukları değerlendirmişlerdir. Bulgular, katılımcıların geleneksel oltalama saldırılarını tanıma konusunda daha yetkin olduğunu, ancak yeni ve daha sofistike saldırı türlerini ayırt etmekte zorlandıklarını göstermiştir. Ayrıca, insanların mevcut siber güvenlik teknolojilerine olan güvensizliğini ve daha fazla bilgilendirme ve eğitim taleplerini ortaya çıkarmıştır.

Aslan (2022), yüksek lisans tez çalışmasında büyük ölçekli kurumlarda çalışanların siber güvenlik farkındalığını artırmaya yönelik bir pilot çalışma gerçekleştirmiştir [83]. Çalışma, bir kamu kurumunda gerçekleştirilmiş ve oltalama tatbikatları, farkındalık eğitimleri ve düzenli bilgi güvenliği bültenleri yoluyla çalışanların siber güvenlik konusunda ne kadar bilinçlendiğini araştırmıştır. Bulgulara göre, sistematik oltalama tatbikatları yapmak, farkındalık eğitimleri sağlamak ve düzenli olarak bilgi güvenliği bültenleri yayımlamak, kullanıcıların siber güvenlik farkındalığını artırabilir. Çalışma ayrıca, bu tür eğitim ve bilgilendirme faaliyetlerinin uzun vadede farkındalığı artırdığını ve bülten okuma alışkanlıklarını olumlu yönde etkilediğini göstermiştir.

Başka bir çalışmada ise [84] Jamaika'daki bireylerin web sitesi oltalama saldırılarını tanıma düzeylerini ölçmek amacıyla üniversite kampüsünde düzenlenen bir atölye çalışması gerçekleştirilmiş ve katılımcılara, 14 web sitesi ekran görüntüsünden

hangilerinin oltalama içerdiğini belirlemeleri istenmiştir. Toplam 327 katılımcı, çeşitli akademik ve idari personel, öğrenciler ve ebeveynler arasından seçilmiştir. Bulgular, Jamaikalıların oltalama saldırılarını tanıma konusunda oldukça bilgisiz olduğunu göstermiştir; katılımcıların %62'si oltalama risklerini doğru bir şekilde tanımlamış, ancak %19'u tüm riskleri tanıyabilmiştir. %38'lik bir kısım, oltalama sitelerini meşru olarak yanlış tanımlarken, %36'sı meşru siteleri oltalama siteleri olarak yanlış tanımlamıştır, bu da katılımcıların genel olarak bir web sitesini oltalama tehdidi yapan unsurlar konusunda bilgisiz olduğunu öne sürmektedir.

Hilmann ve diğerleri (2023), İsrail'deki bir finans kuruluşunda yaklaşık 5,000 çalışana yönelik gerçekleştirilen 3 aşamalı oltalama simülasyon deneyi gerçekleştirmişlerdir [85]. Çalışanlar, kişiselleştirilmiş ve genel olmak üzere iki farklı e-posta metniyle test edilmiştir. Kişiselleştirilmiş e-postalar, alıcının adını içerirken, genel e-postalar bu tür kişisel bilgileri içermemektedir. Bulgular, kişiselleştirilmiş e-posta ifadelerinin genel ifadelere göre daha fazla tıklanma oranına sahip olduğunu göstermektedir.

Üniversite öğrencileri arasında oltalama saldırılarına karşı farkındalığının araştırıldığı bir çalışmada araştırmacılar, öğrencilerin oltalama e-postalarına nasıl tepki verdiklerini belirlemeye çalışmışlardır [86]. Bu çalışmada, öğrencilere önceden hazırlanan bir oltalama web sitesine yönlendiren ve bir bağlantı içeren sahte bir e-posta gönderilmiş, sonrasında katılımcıların yanıtları toplanmış ve analiz edilmiştir. Çalışma üç günlük bir süre zarfında toplam 100 e-posta gönderilmiş ve bu e-postalara verilen yanıtlar değerlendirilmiştir. Bulgular, e-postaların %76'sının açıldığını, açılan e-postaların %22,36'sının ise bağlantıya tıkladığını göstermiştir. Araştırma, öğrencilerin oltalama saldırılarına karşı makul bir farkındalığa sahip olduğunu, ancak hala geliştirilmesi gereken alanlar olduğunu ortaya koymuştur.

3. YÖNTEM

Bu bölümde araştırmanın amacına uygun bir biçimde, araştırmanın modeli, araştırma grubu, veri toplama araçları, verilerin analizi ve verilerin çözümlenmesinde kullanılan istatistiksel yöntem ve teknikler açıklanmıştır.

3.1. Araştırmanın Modeli

Bu çalışma, nicel yöntem araştırması olarak tasarlanmıştır. Araştırmada öğretmenlere gerçekçi ama zararsız oltalama e-postaları gönderilerek, onların bu tür saldırıları tanıma ve tepki verme yani e-postaları açma, bağlantılara tıklama durumları sayısal verilere dönüştürülerek analiz edilerek ve bu sayısal veriler sonucunda genel oltalama farkındalık düzeyleri nicel olarak belirlenmiştir.

3.2. Araştırma Grubu

Araştırmada, Türkiye Millî Eğitim Bakanlığı resmî okullarının anaokulu, ilkokul, ortaokul, lise fark etmeksizin her kademesinde herhangi bir branşta çalışan öğretmenlerin oltalama saldırılarına karşı farkındalık düzeyleri değerlendirilmiştir. Araştırma grubu olarak, Türkiye genelinde farklı illerden, özellikle İstanbul ili ağırlıklı olmak üzere, tahmini olarak 200-250 öğretmen hedeflenmiştir. Örneklem seçimi için olasılıklı olmayan örneklem yöntemlerinden biri olan kartopu örneklem yöntemi benimsenmiştir.

Kartopu örneklemesi, sosyal bilimlerde, özellikle geleneksel yöntemlerle ulaşılması zor olan grupları incelemek için kullanılan olasılıklı olmayan bir örnekleme tekniğidir. Zincirleme yönlendirme örneklemesi veya ağ örneklemesi olarak da bilinen bu yöntem, başlangıçta seçilen katılımcıların referansları aracılığıyla örneklem büyütülerek gizli veya marjinal popülasyonlara erişim sağlar, bu sayede damgalanmış veya göz ardı edilen topluluklardaki bireylerle bağlantı kurulabilir [87]. Kartopu örnekleme yöntemi, araştırma amaçlarına göre iki farklı biçimde uygulanabilir: Homojen kartopu örneklemesi, benzer deneyimlere sahip bireylerden oluşan özel alt grupları araştırmak için kullanılır ve bu sayede derinlemesine bilgiler elde edilirken; heterojen kartopu örneklemesi ise, farklı geçmişlere sahip katılımcıları dahil ederek araştırma konusuna geniş bir perspektiften yaklaşılmasını sağlar ve böylece konunun kapsamlı bir şekilde incelenmesine olanak tanır

[87]. Buradan yola çıkarak bu araştırmada homojen kartopu örneklemesi ile katılımcılara ulaşılmıştır. Araştırmanın başlangıç noktası olarak, araştırmacının bağlı olduğu kurum ile kurumun bağlı olduğu ilçedeki okullarda görev yapan öğretmenler belirlenmiştir. Daha sonra araştırmaya katılan ya da katılmayan bu öğretmenler, kendi mesleki ağlarındaki çeşitli sosyal medya uygulamalarını da kullanarak diğer öğretmenleri araştırmaya katılmaya davet etmişlerdir. Bu şekilde, gönüllü katılım esasına dayalı olarak genişleyen bir öğretmen grubu oluşturulmuştur.

Katılımcılar için bilgilendirilmiş gönüllü olur formuna yanıt veren 231 katılımcıdan 33'ü araştırmaya katılmaya onay vermemiştir. Çalışma araştırmaya katılan 197 katılımcı ile gerçekleştirilmiştir.

3.3. Veri Toplama Araçları

Üniversite Etik Kurulu'ndan alınan izinle (EK-1) Google Forms üzerinden hazırlanan Katılımcılar İçin Bilgilendirilmiş Gönüllü Olur Formu (EK-3) ile araştırma hakkında bilgilendirilmiş ve araştırmaya katılıp katılmama kararları bu form üzerinden alınmıştır. Araştırmaya katılmaya onay veren katılımcıların görev yaptıkları okulun düzeyi, branşları ile gerçekçi fakat zararsız oltalama e-postalarının gönderileceği e-posta adresleri toplanmıştır.

3.3.1. Oltalama e-posta tasarımı

Katılımcılardan toplanan e-posta adreslerine gönderilecek oltalama e-postaları, özellikle mesleki hayatlarında aldıkları e-posta içerikleriyle aynı olacak şekilde tasarlanmıştır. Bu e-postalar katılımcı öğretmenlerden toplanan okul düzeyi ve branşlara uygun farklı farklı oluşturulmuş, bir bağlantı adresi eklenmiş ve bağlantıya tıklandığında bir oltalama simülasyonu gerçekleştirildiğine dair bilgilendirme içeren bir görsel tasarlanmıştır.

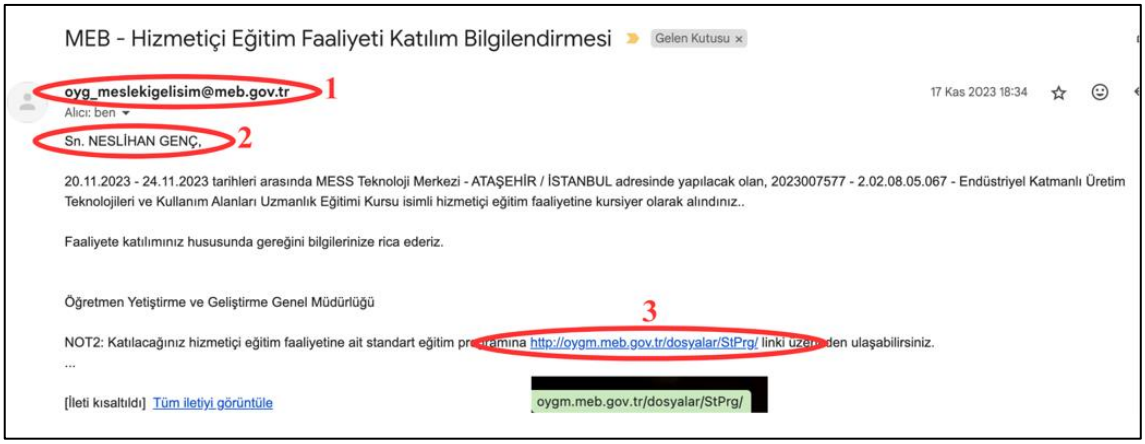
Oltalama e-postası öğretmenlerin belirli dönemlerde ya kendi tercihleriyle istedikleri ya da resen taraflarına atanan hizmetiçi eğitimlerle ilgili tasarlanmıştır. Bu eğitimleri öğretmenler MEBBİS [88] olarak bilinen Millî Eğitim Bakanlığı Bilişim Sistemleri uygulamasının Hizmetiçi Eğitim Modülü'nden tercih etmektedirler (Şekil 3.1). Tercih edilen eğitimler uzaktan eğitim olabileceği gibi başka bir şehirde gerçekleştirilen eğitimler

de olabilir. Özellikle ister tercih edilsin isterse resen atansın başka şehirlerde olan bu eğitimler öğretmenlerin daha çok ilgisini çekmektedir.



Şekil 3.1. MEBBİS Hizmetiçi Eğitim Modülü [88]

Oltalama e-postasına ilham olan orijinal e-posta içeriği Şekil 3.2'de incelenmiştir. Şekildeki 1 numaralı alanda yer alan e-posta adresi, Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü'nün öğretmenleri hizmetiçi eğitimler konusunda bilgilendirme postası gönderdiği orijinal e-posta adresidir. Bu bilgilendirme postaları 2 numaralı alanda görüldüğü gibi bilgilendirme yapılan öğretmenin adı ve soyadı yazılarak oluşturulur. 3 numaralı alanda yer alan bağlantı adresi incelendiğinde de bu bağlantı adresinin metni ile bağlantı aynıdır ve eğitim ile ilgili bilgilerin olduğu web sitesine yönlendirmektedir.



Şekil 3.2. Orijinal e-posta örneği

Şekil 3.2'de yer alan orijinal e-posta örnek alınarak öğretmenlerin branşlarına uygun belirlenmiş bir hizmetiçi eğitimi ile oltalama e-postası tasarlanmıştır ve bu e-postanın orijinalinden farklı birkaç noktası vardır. Şekil 3.3'teki 1 numaralı alanda gönderici ismi *oyg_meslekigelisim* şeklinde görülse de yanında yer alan e-posta adresinin bir Gmail'den

alınmış bir hesap olduğu, bir kamu kurumunun e-posta hesabı olmadığı ancak orijinal e-posta hesabına benzediği görülmektedir. 2 numaralı alanda postanın gönderildiği öğretmenin adı ve soyadı yerine Sayın Öğretmenim ibaresi yer almaktadır. Çünkü veri toplarken katılımcıların ad ve soyad bilgileri alınmamıştır. 3 numaralı alanda orijinaldeki gibi bir bağlantı adresi görülmemesine rağmen üzerine fare ile gelindiğinde görülen bağlantı adresi farklıdır ve sahte ama zararsız bir sayfaya yönlendiren bu bağlantının adresi kullanılan mail takip programından dolayı oldukça uzun görünmektedir. Bu bağlantıya tıklayanlar araştırmayla ilgili bilgilendirici bir görselin olduğu zararsız bir sayfaya yönlendirilmektedirler (Şekil 3.4).



Şekil 3.3. Oltalama e-postası örneği



Şekil 3.4. Oltalama e-postasındaki sahte bağlantının yönlendirdiği sayfa

Oltalama e-postasının mobil cihazlarda görünümü Şekil 3.5'te görülmektedir. Mobil cihazlarda göndericinin e-posta adresi ile sahte bağlantının adresi görülmemektedir.



Şekil 3.5. Oltalama e-postasının mobil cihazlarda görünümü

Çizelge 3.1'de MEBBİS Hizmetiçi Eğitim Modülün'nden yararlanarak öğretmenlerin branşlarına en uygun hizmetiçi eğitimler belirlenmiş ve bunlara göre oltalama e-posta içerikleri oluşturulmuştur.

Çizelge 3.1. Oltalama e-postası için öğretmenlerin branşlarına göre belirlenen hizmetiçi eğitimler

Öğretmen Branşı	Hizmetiçi Kurs Bilgisi
• Sınıf • Teknoloji ve Tasarım	Kaynaştırma Öğrencilerine Yönelik Öğretim Yöntem ve Teknikleri Kursu
• Türk Dili ve Edebiyatı	Türkçe, Türk Dili ve Edebiyatı ile Yabancı Dil Derslerinin Uygulama Sınavlarında Ölçme Değerlendirme Yöntemleri Eğitici Eğitimi Kursu
• Tarih	Türk Düşünce Tarihi Öğretim Programı Eğitici Eğitimi Kursu
• Bilişim Teknolojileri	Bilgisayar Programlama (C++) Eğitimi Kursu
• Sınıf	Özel Yetenekli Bireylerin Belirlenmesi Yöntem ve Teknikleri Kursu
• Matematik	Matematik Öğretmenleri İçin Eğitici Eğitimi Kursu

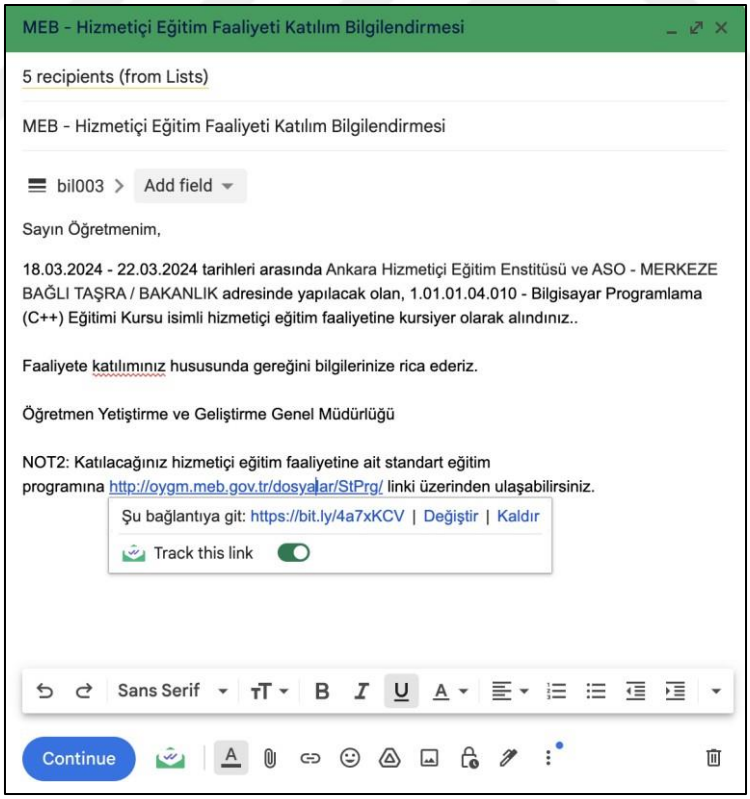
• Muhasebe ve Finansman	Muhasebe Paket Programı (LUCA) Kullanım Kursu
• Din Kültürü ve Ahlak Bilgisi	Öğretim Yöntem ve Teknikleri (Din Kültürü ve Ahlak Bilgisi) Kursu
• Fen Bilimleri	Fen Bilimleri Öğretmenleri İçin Eğitici Eğitimi Kursu
• Coğrafya	Sürdürülebilir Tarım ve Gıda Güvenliği Öğretim Programı Eğitici Eğitimi Kursu
• Meslek Dersleri • Moda Tasarım • Matbaa Teknolojisi • Elektronik • Elektrik • Hayvan Yetiştiriciliği ve Sağlığı Öğretmeni	Mesleki Eğitimde Araştırma Sorgulama Temelli Uygulamalar Mesleki Gelişim Topluluğu Eğitim Programı
• Sağlık Hizmetleri • Biyoloji • Büro Yönetimi	İlk Yardım Eğitici Eğitimi Kursu
• Fizik • Kimya	Fen Bilimleri (Fizik-Kimya-Biyoloji) Öğretmenleri İçin Eğitici Eğitimi Kursu
• Bilgisayar Destekli Makine Ressamlığı	Fusion 360 ile Üretken Şekil Tasarımı Kursu
• Beden Eğitimi	Spor Eğitimi ve Spor Programı Uygulamaları Öğretmen Hareketlilik Programı
• Psikolojik Danışmanlık ve Rehberlik	Davranışsal Bağımlılığa Yönelik Grupla Psikolojik Danışma Programı Uygulayıcı Eğitimi Kursu
• Özel Eğitim	Öğrenme Güçlüğü Testi Uygulayıcı Eğitimi Kursu

3.3.2. Gönderilen oltalama e-postaların takibi

Kurumsal firmalar, üniversiteler ve bazı kamu kurumları, çalışanlarının oltalama saldırılarına karşı farkındalığını artırmak için düzenli aralıklarla oltalama simülasyonları gerçekleştirmektedir. Bu simülasyonlar, ya kurumların kendi geliştirdikleri ya da satın aldıkları uygulamalar aracılığıyla yapılmakta, çalışanların sahte e-postalara verdikleri tepkiler izlenmektedir. Süreç sonunda, çalışanlara yönelik eğitimler düzenlenerek oltalama saldırılarına karşı daha etkin koruma sağlanmaktadır. Kuruluşlar kendi e-posta sunucularını kullandıkları için bu simülasyonların uygulanması ve takip edilmesi oldukça kolaydır. Kuruluşlar, kendi e-posta sunucularını kullanarak simülasyonları kolayca uygular ve izler. Çalışanlar, iş bilgisayarlarında sadece kurumsal e-posta hesaplarını kullanmaları yönünde teşvik edilirken, Türkiye'deki öğretmenler genellikle kurumsal e-posta hesaplarına sahip olmadıkları için hem kişisel cihazlarında hem de kurumlarındaki

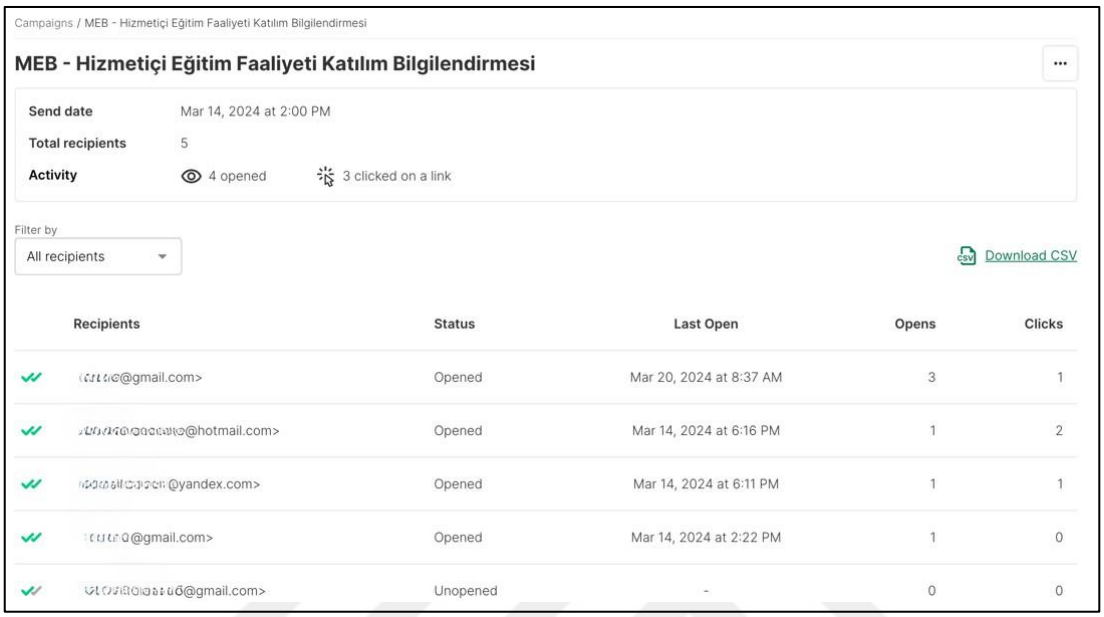
bilgisayarlarda farklı servis sağlayıcılarından (Gmail, Hotmail, Outlook, vs.) edindikleri kişisel e-postalarını kullanmaktadırlar.

Araştırma kapsamında katılımcı öğretmenlerden toplanan e-posta adresleri farklı e-posta hizmet sağlayıcılardan alındığından gönderilecek oltalama postalarını takip etmek için herhangi bir oltalama simülasyon uygulaması uygun olmamıştır. Çünkü bu tür uygulamalar sadece kurumsal hesapları takip etmek için geliştirilmiştir. Bu yüzden, yapılan araştırmalar neticesinde *Mailsuite* [89] isimli e-posta takip uygulaması kullanılmıştır. Ancak bu uygulama gönderilen oltalama e-postasının gelen kutusuna mı yoksa spam kutusuna mı düştüğünü göstermemektedir. Bu uygulama ile araştırma için tasarlanan oltalama e-posta ile kampanya şablonu oluşturulmuş ve beşerli e-posta adresleriyle oluşturulmuş gruplara bu kampanya postaları gönderilmiştir (Şekil 3.5). Bu kampanya postalarında alıcılar diğer alıcıların adreslerini görmemekte, e-postanın sadece kendilerine gönderilmiş gibi olduğunu görmektedirler.



Şekil 3.6. Oltalama çalışması için oluşturulmuş kampanya e-posta örneği

Mailsuite uygulaması sayesinde gönderilen e-postaların açılıp açılmadığı, en son açılma zamanı, açıldıysa kaç kere açıldığı, eğer içinde bağlantı varsa bağlantıya tıklanıp tıklanmadığı, tıklandıysa kaç kere tıklandığı gibi sayısal verilere ulaşılmaktadır (Şekil 3.6).



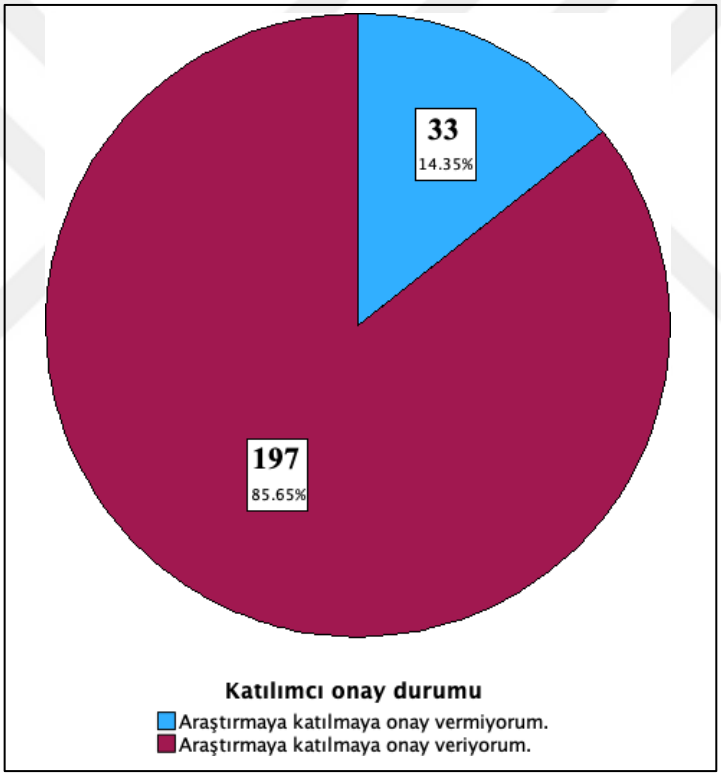
Şekil 3.7. Gönderilen kampanya postalarının sayısal takibi

3.4. Verilerin Analizi

Google Forms üzerinden gönüllü katılımcılardan toplanan katılımcının branşı, görev yaptığı okul düzeyi ile e-posta adresleri MS Excel üzerinde tabloya aktarılmış, oltalama simülasyonu sonrasında Mailsuite uygulaması ile elde edilen sayısal bilgiler bu tabloya eklenmiştir. Bu verileri analiz etmek için IBM SPSS Version 29.0.1.0 programı, istatistiksel yöntem olarak betimleyici istatistiksel yöntemler kullanılmıştır.

4. BULGULAR VE YORUM

Bu bölümde araştırmanın ana amaçlarına ve alt problemlerine ilişkin yapılan istatistiksel çözümler ve bunlara ait yorumlar yer almaktadır. Araştırmayı gerçekleştirmek için öğretmenlere Katılımcılar İçin Bilgilendirilmiş Gönüllü Olur Formu iletilmiştir. Bu form üzerinden öğretmenlere bu araştırmaya katılmaya onay verip vermedikleri sorulmuş ve bu soruya 233 kişi cevap vermiştir. 233 kişiden 33 kişi (%14,35) araştırmaya katılmaya onay vermemişler, 197 kişi (%85,65) araştırmaya katılmaya onay vermişlerdir. Araştırma, onay veren 197 kişi üzerinden gerçekleşmiş ve bu kişilerden elde edilen sayısal veriler ile analiz edilmiştir.



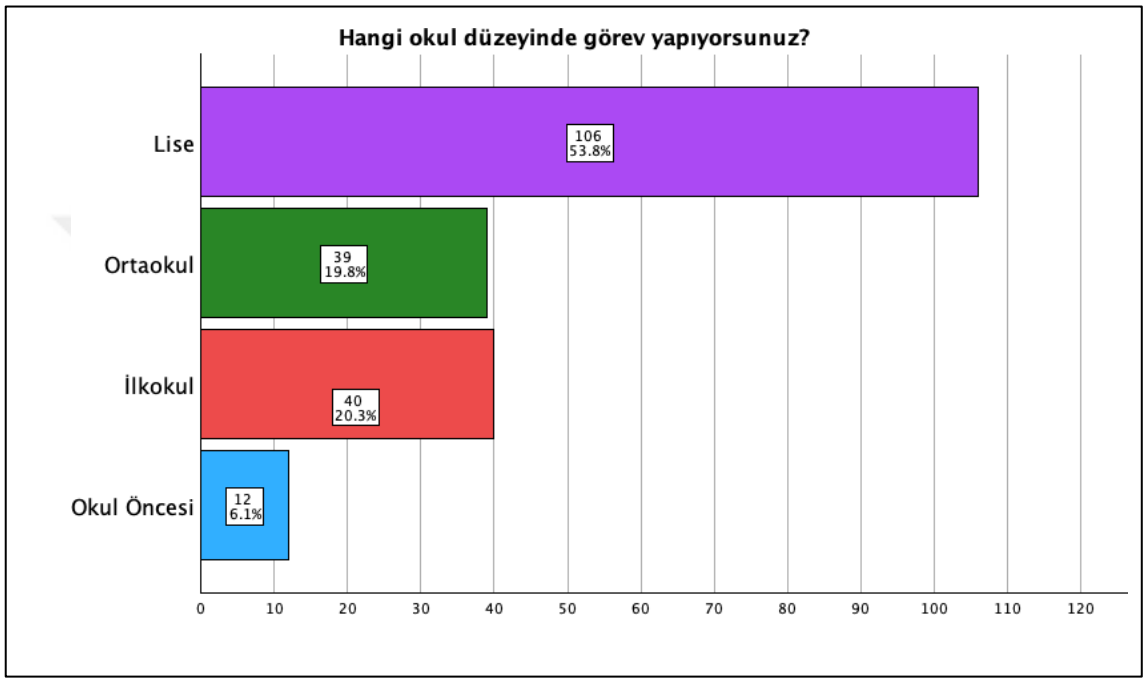
Şekil 4.1. Araştırmaya katılım onay durumu

4.1. Demografik Bulgular

Araştırmaya onay veren 197 katılımcı öğretmen, "Hangi okul düzeyinde görev yapıyorsunuz?" sorusunu yanıtlamışlar 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 (Çizelge 4.1). Bu bilgilere dayanarak ve Şekil 4.2'de görüldüğü gibi araştırmaya en fazla liseden görev yapan öğretmenler katılmışlardır.

Çizelge 4.1. Katılımcı öğretmenlerin görev yaptığı okul düzeylerine ilişkin bilgiler

Okul Düzeyi	Kişi Sayısı	Yüzde
Okul Öncesi	12	6,1
İlkokul	40	20,3
Ortaokul	39	19,8
Lise	106	53,8
Toplam	***197***	***100,0***



Şekil 4.2. Katılımcı öğretmenlerin görev yaptığı okul düzeylerinin grafiksel dağılımı

"Branşınız nedir?" sorusuna verilen yanıtlar incelendiğinde araştırmaya katılan öğretmenlerin branş dağılımı çeşitlilik göstermektedir ve 32 farklı branştan öğretmenin araştırmaya katıldığı görülmektedir. Çizelge 4.2 incelendiğinde en fazla temsil edilen branşlar %25,9 ile Bilişim Teknolojileri, %14,7 ile Sınıf, %7,1 ile Matematik ve %6,1 ile İngilizce branşlarıdır. Ayrıca Okul Öncesi ile Muhasebe ve Finansman branşlarından katılımcılar da %6,1 ve %3,6 oranlarında bulunmaktadır. Diğer branşlardan katılımcı sayıları oldukça düşük, çoğu %2'nin altında kalmaktadır.

Çizelge 4.2. Katılımcı öğretmenlerin branşlarına ilişkin bilgiler

Branşlar	Kişi Sayısı	Yüzde
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
Psikolojik Danışmanlık ve 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
Toplam	***197***	***100,0***

Bazı branş öğretmenleri farklı okul düzeylerinde görev yapmaktadırlar. Çizelge 4.3'e göre farklı okul düzeylerinde görev yapan öğretmenlerin dağılımı şöyledir: Bilişim Teknolojileri öğretmenlerinin 13'ü ortaokulda, 38'i lisede; İngilizce öğretmenlerinin 4'ü ilkokulda, 3'ü ortaokulda, 5'i lisede; Matematik öğretmenlerinin 5'i ortaokulda, 9'u lisede; Psikolojik Danışmanlık ve Rehberlik öğretmenlerinin ise 4'ü ilkokulda, 1'i ortaokulda, 4'ü lisede görev yapmaktadır.

Çizelge 4.3. Farklı okul düzeylerinde branşların dağılım bilgileri

		Hangi okul düzeyinde görev yapıyorsunuz?				
		Okul Öncesi	İlkokul	Ortaokul	Lise	***Toplam***
Branşınız nedir?	Almanca	0	0	0	2	***2***
	Beden Eğitimi	0	0	1	3	***4***
	Bilg. Des. Mak. Ressamlığı	0	0	0	1	***1***
	Bilişim Teknolojileri	0	0	13	38	***51***
	Biyoloji	0	0	0	1	***1***
	Büro Yönetimi	0	0	0	1	***1***
	Coğrafya	0	0	0	1	***1***
	Din Kültürü ve Ahlak Bilgisi	0	1	2	0	***3***
	Elektrik	0	0	0	1	***1***
	Elektronik	0	0	0	2	***2***
	Felsefe	0	0	0	3	***3***
	Fen Bilimleri	0	0	3	0	***3***
	Fizik	0	0	0	5	***5***
	Görsel Sanatlar	0	0	0	4	***4***
	Hayvan Yetiş. ve Sağlığı	0	0	0	1	***1***
	İngilizce	0	4	3	5	***12***
	Kimya	0	0	0	1	***1***
	Matbaa Teknolojisi	0	0	0	1	***1***
	Matematik	0	0	5	9	***14***
	Meslek Dersleri	0	0	0	1	***1***
	Moda Tasarım	0	0	0	1	***1***
	Muhasebe ve Finansman	0	0	0	7	***7***
	Okul Öncesi	12	0	0	0	***12***
	Özel Eğitim	0	2	0	1	***3***
	Psik. Danış. ve Rehberlik	0	4	1	4	***9***
	Sağlık Hizmetleri	0	0	0	1	***1***
	Sınıf	0	29	0	0	***29***
	Sosyal Bilgiler	0	0	2	0	***2***
	Tarih	0	0	0	7	***7***
	Teknoloji ve Tasarım	0	0	4	0	***4***
	Türk Dili ve Edebiyatı	0	0	0	5	***5***
	Türkçe	0	0	5	0	***5***
Toplam		***12***	***40***	***39***	***106***	***197***

4.2. Oltalama E-Postaları ile İlgili Bulgular

Araştırmaya onay veren 197 katılımcıdan toplanan e-posta adreslerine tasarlanan oltalama e-postası gönderilmiş ve Mailsuite uygulaması üzerinden e-postanın gönderilip gönderilmediği tespit edilmiştir. Çizelge 4.4'e göre 196 katılımcıya e-posta ulaşmış; ancak

1 katılımcıya ulaşmamıştır. Dolayısıyla bundan sonraki analizle bu 196 katılımcı üzerinden gerçekleşmiştir.

Çizelge 4.4. Oltalama e-postasının katılımcıya gönderilme durumu

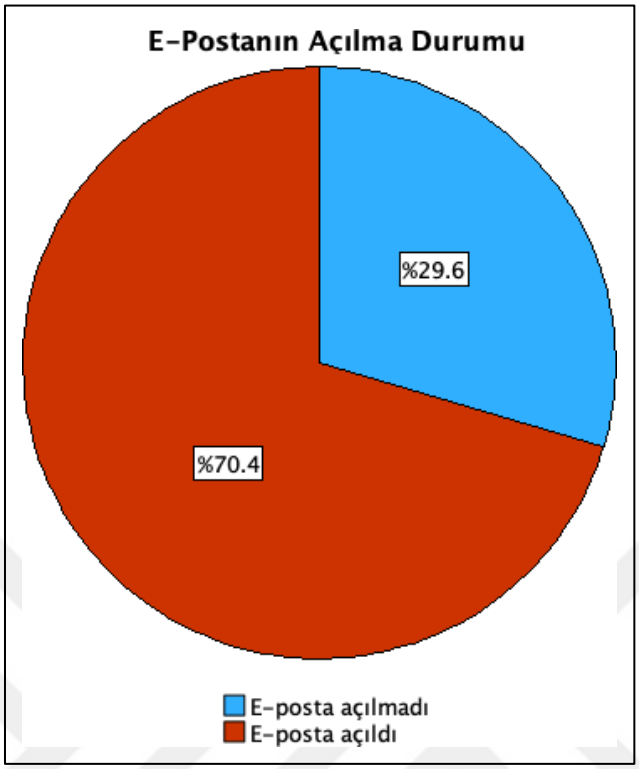
E-postanın gönderilme durumu	Kişi Sayısı	Yüzde
E-posta gönderilmedi	1	0,5
E-posta gönderildi	196	99,5
Toplam	***197***	***100,0***

Bu bulgular, e-posta gönderiminin %99,5 oranında başarılı olduğunu ve sadece %0,5 oranında başarısızlık yaşandığını göstermektedir. Bu, araştırmanın geçerliliği açısından oldukça olumlu bir durumdur. Gönderilen e-postaların büyük çoğunluğunun katılımcılara ulaşması, elde edilen verilerin kapsamlı ve güvenilir bir şekilde analiz edilmesini mümkün kılmaktadır. E-postaların sadece 1 kişiye ulaşmaması, teknik bir sorun veya yanlış e-posta adresi gibi nedenlerden kaynaklanabilir. Ancak genel olarak, e-posta gönderim sürecinin başarılı bir şekilde yönetildiği ve araştırma kapsamındaki katılımcıların büyük bir çoğunluğunun verilerine ulaşılabildiği söylenebilir.

Oltalama e-postası ulaşan 196 katılımcının gönderilen e-postayı açıp açmadıkları incelendiğinde Çizelge 4.5'e göre 58 katılımcı e-postayı açmamış, 138 katılımcı e-postayı açmıştır.

Çizelge 4.5. Gönderilen oltalama e-postasının açılıp açılmama durumu

Gönderilen e-postanın açılma durumu	Kişi Sayısı	Yüzde
E-posta açılmadı	58	29,6
E-posta açıldı	138	70,4
Toplam	***196***	***100,0***



Şekil 4.3. Gönderilen oltalama e-postasının açılıp açılmama durumu

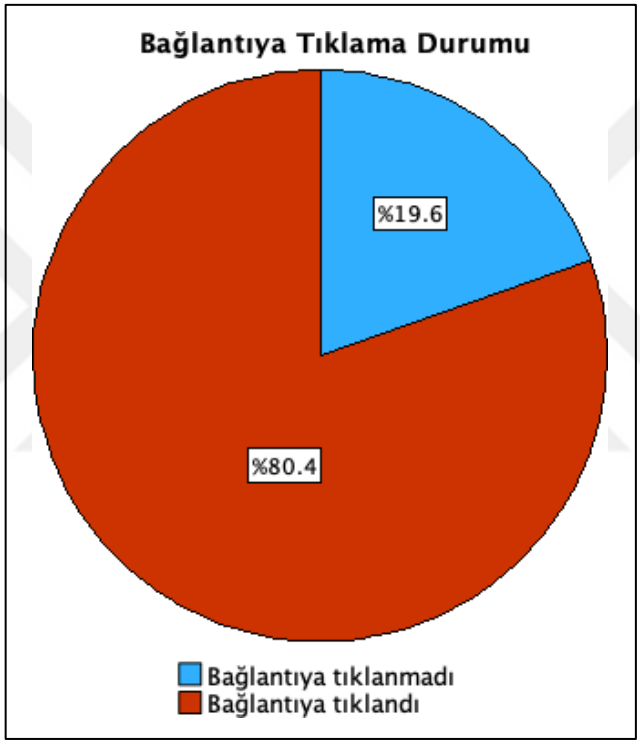
Elde edilen bu sonuçlar, e-posta açılma oranının yüksek olduğunu ve katılımcıların %70,4'ünün gönderilen e-postaları açtığını göstermektedir (Şekil 4.3). Bu durum, katılımcıların e-posta iletişimine dikkat ettiğini ve gönderilen mesajları incelediğini göstermektedir. Ayrıca, mobil cihazlardan alınan anlık bildirimler, gönderilen e-postaların fark edilmesini kolaylaştırmaktadır. Bu nedenle, e-postaların açılma oranının yüksek olması, katılımcıların mobil cihazlar üzerinden gelen bildirimleri dikkate aldığını da göstermektedir. Mobil cihaz kullanımının yaygınlığı ve anlık bildirimlerin etkisi, e- postaların daha hızlı ve etkin bir şekilde fark edilmesini sağlamaktadır.

Ancak, %29,6 oranında e-postanın açılmaması, bazı katılımcıların e-postaları fark etmemiş olabileceğini veya bu e-postaları açmamış olabileceğini göstermektedir. Bu durumun nedenlerinden biri, bazı e-postaların katılımcıların spam/junk klasörlerine düşmüş olması olabilir. E-posta takip uygulaması olan Mailsuite uygulaması, e-postanın spam klasörüne düşüp düşmediğini takip edememektedir. Bu durum, e-postaların tüm katılımcılar tarafından fark edilip edilmediğini tam olarak belirlemeyi zorlaştırmaktadır. Diğer bir neden ise, katılımcıların bir kısmının e-posta güvenliği konusundaki farkındalıklarının ve bilgi düzeylerinin yeterli düzeyde olduğu gösterilebilir.

Oltalama e-postasını açan 138 kişinin bu e-posta içerisinde yer alan oltalama bağlantısına tıklayıp tıklamadıkları Çizelge 4.6'da görülmektedir. E-postayı açan 27 katılımcı bağlantıya tıklamamış, 111 katılımcı ise bu bağlantıya tıklamışlardır.

Çizelge 4.6. Gönderilen oltalama e-postasındaki bağlantıya tıklanıp tıklanmama durumu

Gönderilen e-postadaki bağlantıya tıklama durumu	Kişi Sayısı	Yüzde
Bağlantıya tıklanmadı	27	19.6
Bağlantıya tıklandı	111	80.4
Toplam	***138***	***100.0***



Şekil 4.4. Gönderilen oltalama e-postasındaki bağlantıya tıklanma durumu

Oltalama e-postasını açan katılımcıların %80,4 gibi büyük bir çoğunluğu e-posta içindeki bağlantıya tıklamışlar, %19,6'sı tıklamamışlardır (Şekil 4.4). Bağlantıya tıklama oranının yüksek olması, katılımcıların oltalama e-postalarının içerdiği tuzaklara karşı daha savunmasız olduklarını ve bu tür e-postaların tehlikelerini yeterince bilmediklerini işaret edebilir. Ayrıca gönderilen oltalama e-postasındaki gönderenin posta adresine bakmadıkları ve bağlantıdaki yönlendirilen bağlantıyı incelemeden tıkladıkları da söylenebilir. %19,6 oranında katılımcının bağlantıya tıklamaması, bu kişilerin oltalama e- postalarına karşı daha dikkatli olduklarını, bu tür bağlantılara tıklamadan önce daha fazla düşündüklerini veya resmi hesaplarına bakıp gelen e-posta içeriğinin resmi hesaplarında da

olup olmadığını kontrol ettiklerini göstermektedir. Bu grup, oltalama saldırılarına karşı daha yüksek farkındalık seviyesine sahip olabilir.

Çizelge 4.7'de çapraz tablo analizi yapılarak katılımcıların branşlarına göre gönderilen oltalama e-postasını açma dağılımları görülmektedir. 32 ayrı branştan araştırmaya katılınmış ve sadece 4 branştaki katılımcılardan gönderilen oltalama e-postasını açmadıkları görülmüştür. Bu 4 branşın her birinden sadece 1 öğretmen araştırmaya katılmıştır. Dağılım incelendiğinde en dikkat çekici bulgu, Bilişim Teknolojileri branşında görev yapan öğretmenlerin yüksek katılımı ve e-postaları açma oranlarının yüksek olmasıdır. Bu branştan 51 öğretmenden 37'si e-postayı açmıştır. Matematik branşı da benzer bir trend göstermekte; 14 öğretmenden 11'i e-postayı açmıştır. Diğer branşlarda ise e-posta açma sayıları daha düşük veya sıfıra yakın. Bu veriler, belirli branşlardaki öğretmenlerin e-posta iletişimine olan duyarlılıklarını ve belki de bilgi teknolojileri konusundaki yeterliliklerini yansıtıyor olabilir. Aynı şekilde araştırmaya katılan 28 sınıf öğretmeninden 16'sı e-postayı açmıştır. Diğer branşlardan katılım düşük olmasına rağmen e-postayı açma oranları yüksektir.

Çizelge 4.7. Branşlara göre oltalama e-postasının açılma durumunun dağılımı

		E-Postanın Açılma Durumu		
		E-posta açılmadı	E-posta açıldı	***Toplam***
Branşınız nedir?	Almanca	0	2	***2***
	Beden Eğitimi	0	4	***4***
	Bilg. Des. Mak. Ressamlığı	0	1	***1***
	Bilişim Teknolojileri	14	37	***51***
	Biyoloji	1	0	***1***
	Büro Yönetimi	0	1	***1***
	Coğrafya	0	1	***1***
	Din Kültürü ve Ahlak Bilgisi	1	2	***3***
	Elektrik	0	1	***1***
	Elektronik	2	0	***2***
	Felsefe	2	1	***3***
	Fen Bilimleri	1	2	***3***
	Fizik	1	4	***5***
	Görsel Sanatlar	3	1	***4***
	Hayvan Yetiş. ve Sağlığı	1	0	***1***
	İngilizce	1	11	***12***
	Kimya	0	1	***1***
	Matbaa Teknolojisi	1	0	***1***
	Matematik	3	11	***14***

	Meslek Dersleri	0	1	***1***
	Moda Tasarım	0	1	***1***
	Muhasebe ve Finansman	4	3	***7***
	Okul Öncesi	3	9	***12***
	Özel Eğitim	2	1	***3***
	Psik. Danış. ve Rehberlik	0	9	***9***
	Sağlık Hizmetleri	1	0	***1***
	Sınıf	12	16	***28***
	Sosyal Bilgiler	1	1	***2***
	Tarih	2	5	***7***
	Teknoloji ve Tasarım	1	3	***4***
	Türk Dili ve Edebiyatı	1	4	***5***
	Türkçe	0	5	***5***
Toplam		***58***	***138***	***196***

Çapraz tablo analizinde kullanılan Ki-kare testi ile öğretmenlerin branşları ile oltalama e-postalarının açılma durumları arasındaki ilişkiyi incelenmiştir (Çizelge 4.8) ve "Katılımcıların e-posta açma davranışları branşlara göre anlamlı bir farklılık göstermekte midir?" sorusu yanıtlanmıştır. Pearson Ki-Kare (Pearson Chi-Square) testi için hesaplanan değer 42.666 olup, serbestlik derecesi 31'dir ve elde edilen p-değeri yani olasılık değeri 0.079'dur. Bu sonuçlara göre ilişki, 0,05 anlamlılık düzeyine göre istatistiksel olarak anlamlı değildir yani öğretmenlerin branşları ile gönderilen e-postanın açma davranışları arasında anlamlı bir ilişki yoktur. Ancak analiz sonucunda, analizde kullanılan veri setinde bazı kategorilerin düşük frekanslara sahip olduğu ve bu durumun test sonuçları üzerinde etkili olabileceği görülmektedir.

Çizelge 4.8. Branşlara göre oltalama e-postasının açılma durumunun ki-kare testi analizi

	Değer	**Serbestlik Derecisi**	**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.			

Çizelge 4.9'da farklı okul düzeylerinde görev yapan öğretmenlerin oltalama e-postası açma davranışları çapraz olarak incelenmiştir. E-posta açılmama ve açılma durumu, okul öncesi, ilkokul, ortaokul ve lise düzeylerinde ayrı ayrı gösterilmiştir. Sonuçlara göre, lise düzeyinde en yüksek e-posta açılma sayısı (74) gözlenirken ilkokul düzeyinde en düşük e- posta açılmama sayısı (13) gözlemlenmiş; ancak katılımcı sayısına göre oransal olarak bakıldığında gönderilen oltalama e-postasını açma oranları okul öncesi düzeyinde %75,

ilkokul düzeyinde %66,67, ortaokul düzeyinde %74,36 ve lise düzeyinde %69,81 olarak hesaplanmıştır.

Çizelge 4.9. Okul düzeyine göre oltalama e-postasının açılma durumunun dağılımı

		E-Postanın Açılma Durumu		
		E-posta açılmadı	E-posta açıldı	***Toplam***
Hangi okul düzeyinde görev yapıyorsunuz?	Okul Öncesi	3	9	***12***
	İlkokul	13	26	***39***
	Ortaokul	10	29	***39***
	Lise	32	74	***106***
Toplam		***58***	***138***	***196***

Farklı okul düzeyinde görev yapan öğretmenlerin e-postaları açma davranışları arasında istatistiksel olarak anlamlı bir fark olup olmadığını değerlendirmek için çapraz tablo analizinden sonra ki-kare testi yapılmıştır. 31 serbestlik derecesinde Pearson Ki-Kare hesaplanan değeri 0.694, bu testin olasılık değeri (p-değeri) 0.875 hesaplanmıştır. Bu değer, 0,05 anlamlılık düzeyinin üzerinde olduğu için, katılımcıların e-posta açma davranışları okul düzeylerine göre anlamlı bir farklılık göstermemektedir yani katılımcıların okul düzeylerinin oltalama e-postalarını açma davranışları üzerinde bir etkisi yoktur. Ancak, bir kategorideki değer beklenen değerden düşük olduğu için bazı kategorilerdeki örneklem büyüklüğünün yeterli olmadığı dikkate alınmalıdır. Bu durum, sonuçların güvenirliği üzerinde etkili olabilir. Daha büyük ve dengeli örneklemlerle yapılacak gelecekteki çalışmalar, bu tür analizlerde daha sağlıklı sonuçlar verebilir.

Çizelge 4.10. Okul düzeyine göre oltalama e-postasının açılma durumunun ki-kare testi analizi

	Değer	**Serbestlik Derecisi**	**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.			

Oltalama e-postasını açan 138 katılımcının branşlarına göre e-postadaki bağlantıya tıklama davranışları çapraz tablo analizi ile incelenmiş ve Çizelge 4.11'deki sonuçlar elde edilmiştir. Bu analize göre 27 farklı branştaki katılımcı öğretmenlerden Büro Yönetimi, Görsel Sanatlar, Moda Tasarım, Sosyal Bilgiler branşlarındakilerin (her birinde 1 katılımcı) açtıkları oltalama e-postasındaki bağlantıya tıklamadıkları görülmüştür. Bilişim Teknolojileri branşında 37 öğretmenden 31'i bağlantıya tıklarken; Sınıf öğretmenleri

branşında 16 öğretmenden 11'i bağlantıya tıklamıştır. Matematik ve İngilizce branşlarında da e-postayı açan 11 katılımcının 10'unun bağlantıya tıkladığı görülmüştür.

Çizelge 4.11. Branşlara göre oltalama e-postasındaki bağlantıya tıklama durumunun dağılımı

		Bağlantıya Tıklama Durumu		
		Bağlantıya tıklanmadı	Bağlantıya tıklandı	***Toplam***
Branşınız nedir?	Almanca	1	1	***2***
	Beden Eğitimi	0	4	***4***
	Bilg. Des. Mak. Ressamlığı	0	1	***1***
	Bilişim Teknolojileri	6	31	***37***
	Büro Yönetimi	1	0	***1***
	Coğrafya	0	1	***1***
	Din Kültürü ve Ahlak Bilgisi	1	1	***2***
	Elektrik	0	1	***1***
	Felsefe	0	1	***1***
	Fen Bilimleri	0	2	***2***
	Fizik	1	3	***4***
	Görsel Sanatlar	1	0	***1***
	İngilizce	1	10	***11***
	Kimya	0	1	***1***
	Matematik	1	10	***11***
	Meslek Dersleri	0	1	***1***
	Moda Tasarım	1	0	***1***
	Muhasebe ve Finansman	2	1	***3***
	Okul Öncesi	0	9	***9***
	Özel Eğitim	0	1	***1***
	Psik. Danış. ve Rehberlik	2	7	***9***
	Sınıf	5	11	***16***
	Sosyal Bilgiler	1	0	***1***
	Tarih	0	5	***5***
	Teknoloji ve Tasarım	1	2	***3***
	Türk Dili ve Edebiyatı	1	3	***4***
	Türkçe	1	4	***5***
Toplam		***27***	***111***	***138***

Ki-kare testi ile öğretmenlerin branşları ile oltalama e-postalarındaki bağlantıya tıklama davranışları arasındaki ilişki incelenmiş (Çizelge 4.12) ve "Katılımcıların e-postadaki bağlantıya tıklama davranışları branşlara göre anlamlı bir farklılık göstermekte midir?" sorusuna yanıt aranmıştır. Analiz sonucunda Pearson Ki-Kare hesaplanan değeri 33,33 bulunmuş, 0,05 anlam düzeyinde 26 serbestlik derecesi ve 0,153 olasılık değeri (p-değeri) ile katılımcıların branşı ile oltalama e-postasındaki bağlantıya tıklama davranışları arasında

anlamlı bir ilişki olmadığı görülmüştür. Ancak, analiz sonucunda bazı kategorilerde düşük frekansların bulunması, test sonuçları üzerinde etkili olabilecektir. Daha büyük ve dengeli örneklemlerle yapılacak gelecekteki çalışmalar, bu tür analizlerde daha sağlıklı sonuçlar verebilir.

Çizelge 4.12. Branşlara göre oltalama e-postasındaki bağlantıya tıklama durumunun ki-kare testi analizi

	Değer	**Serbestlik Derecisi**	**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.			

Oltalama e-postasını açan 138 katılımcının görev yaptıkları okul düzeyi ile e-postadaki bağlantıya tıklama durumları Çizelge 4.13 ile incelenmiştir. Çizelgedeki veriler oransal olarak incelendiğinde sırasıyla; okul öncesi düzeyindeki katılımcıların hepsi yani %100'ünün, en fazla katılımın olduğu lise düzeyindeki katılımcıların %83,78'inin, ilkokul düzeyinde görev yapanların %76,92'sinin, ortaokul düzeyindeki katılımcıların ise %68,97'sinin bağlantıya tıklamış oldukları görülmektedir.

Çizelge 4.13. Okul düzeylerine göre oltalama e-postasındaki bağlantıya tıklama durumunun dağılımı

		Bağlantıya Tıklama Durumu		
		Bağlantıya tıklanmadı	Bağlantıya tıklandı	***Toplam***
Hangi okul düzeyinde görev yapıyorsunuz?	Okul Öncesi	0	9	***9***
	İlkokul	6	20	***26***
	Ortaokul	9	20	***29***
	Lise	12	62	***74***
Toplam		***27***	***111***	***138***

Çizelge 4.14'te katılımcıların görev yaptığı okul düzeyleri ile oltalama e-postasındaki bağlantıya tıklama davranışları arasındaki anlamsal ilişki Pearson ki-Kare testi ile incelenmiş ve bu iki durum arasında 0,05 anlam düzeyinde 0,148 olasılık değeri (p-değeri) ile anlamsal bir ilişki olmadığı görülmüştür yani farklı okul düzeylerinde görev yapan öğretmenlerin oltalama e-postalarındaki bağlantılara tıklama olasılıklarının benzerdir. Ancak, bazı kategorilerde düşük frekansların bulunması, test sonuçları üzerinde etkili olabilir.

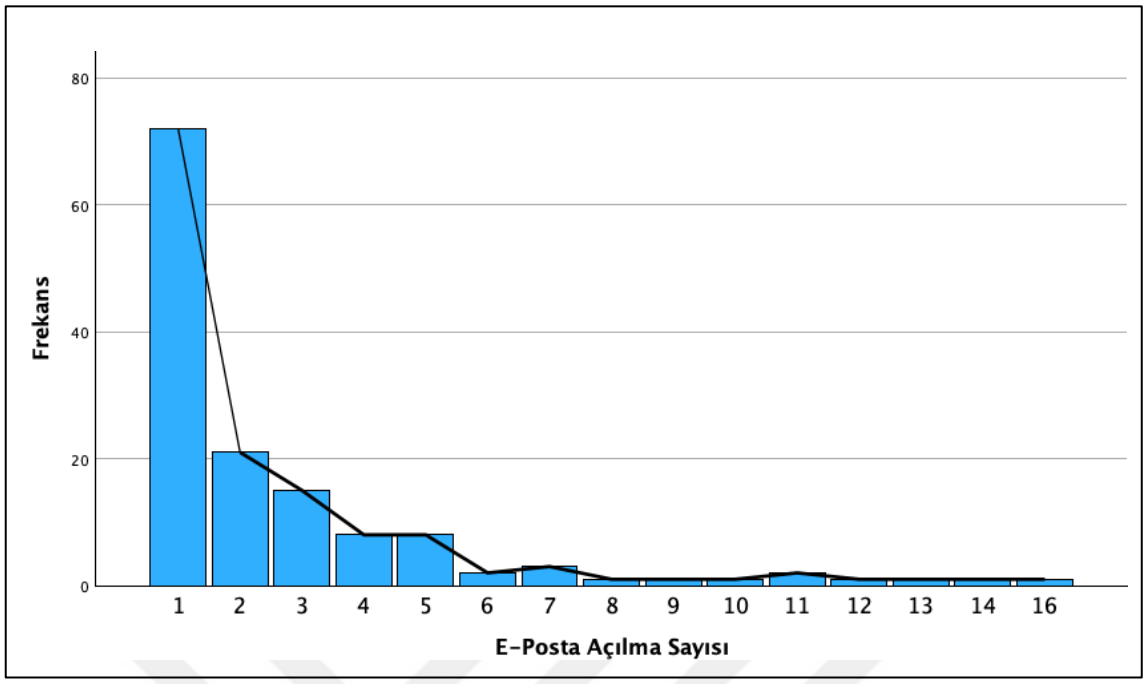
Çizelge 4.14. Okul düzeylerine göre oltalama e-postasındaki bağlantıya tıklama durumunun ki-kare analizi

	Değer	Serbestlik Derecisi	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.			

Çalışma kapsamında kullanılan e-posta takip uygulaması ile katılımcıların e-postayı kaç kere açtıkları ve e-postadaki bağlantıya tıkladılarsa kaç kere tıkladıkları verileri elde edilmiştir. Araştırmaya katılan 138 kişinin gönderilen oltalama e-postasını kaç kere açtıkları ile ilgili bulgular Çizelge 4.15'te görülmektedir. Katılımcıların mail açma sayısının ortalaması 2,67, medyan ve medyan değerleri 1 olarak belirlenmiştir. Standart sapma 2,845 olup, bu da mail açma sayılarının ortalamadan önemli ölçüde sapma gösterdiğini göstermektedir. Mail açma sayısının minimum değeri 1, maksimum değeri ise 16'dır. Çarpıklık değeri 2,509 olup, bu dağılımın pozitif çarpıklık gösterdiğini, mail açma sayılarının çoğunlukla düşük değerlerde yoğunlaştığını ve dağılımın sağa çarpık olduğunu göstermektedir (Şekil 4.5). Basıklık değeri 6,735 olup, bu da dağılımın sivri bir tepe noktasına sahip olduğunu ve değerlerin uçlarda yoğunlaştığını göstermektedir (Şekil 4.5). Bu bulgular, katılımcıların mail açma davranışlarının oldukça değişken olduğunu ve çoğunlukla düşük açılma sayılarında yoğunlaştığını ortaya koymaktadır. Ancak, bazı katılımcılar e-postayı defalarca açarak ortalama değeri artırmıştır. E-postaların birçok kez açılması, katılımcıların dikkatli olup, içeriği birden fazla kez gözden geçirdiğini ya da resmi hesaplarını kontrol ederek e-posta içeriğinin doğru olup olmadığını belirlemek için tekrar tekrar ziyaret ettiklerini işaret edebilir.

Çizelge 4.15. Gönderilen oltalama e-postasının açılma sayısı ile ilgili istatistiki bilgiler

Ortalama	2,67
Medyan	1,00
Mod	1
Standart Sapma	2,845
Çarpıklık	2,509
Çarpıklığın Std. Hatası	0,206
Basıklık	6,735
Basıklığın Std. Hatası	0,410
Minimum	1
Maksimum	16

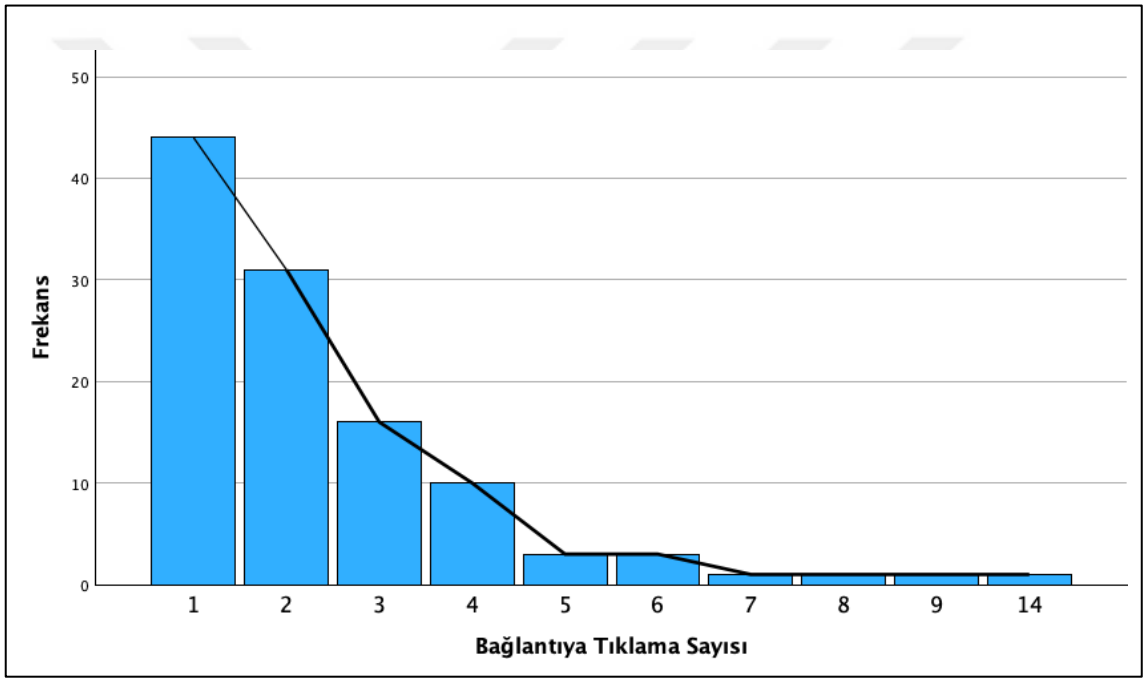


Şekil 4.5. Gönderilen oltalama e-postasının açılma sayısının grafiği

Gönderilen oltalama e-postasındaki bağlantıya tıklayan 111 kişiden bazıları bu bağlantıya birden fazla tıklamışlardır. Çizelge 4.15'e göre; katılımcıların bağlantıya tıklama sayısının ortalaması 2,39 olup, medyan değeri 2 ve mod değeri 1 olarak hesaplanmıştır. Standart sapma 1,936 olup, bu da tıklama sayılarının ortalamadan önemli ölçüde sapma gösterdiğini ortaya koymaktadır. Tıklama sayılarının minimum değeri 1, maksimum değeri ise 14'tür. Çarpıklık değeri 2,872 olup, bu dağılımın pozitif çarpıklık gösterdiğini ve tıklama sayılarının çoğunlukla düşük değerlerde yoğunlaştığını ifade eder. Bu durum, grafiğin sağa çarpık olduğunu göstermektedir (Şekil 4.6). Basıklık değeri ise 12,239 olup, dağılımın sivri bir tepe noktasına sahip olduğunu ve değerlerin uçlarda yoğunlaştığını göstermektedir (Şekil 4.6). Bu bulgulara göre katılımcıların çoğunluğu bağlantıya bir veya iki kez tıklamış, ancak bazı katılımcılar bağlantıya daha fazla sayıda tıklamışlardır. Bu bulgular, katılımcıların bağlantıya tıklama davranışlarının oldukça değişken olduğunu ve çoğunlukla düşük tıklama sayılarında yoğunlaştığını göstermektedir. Bu tür tıklama davranışları, oltalama e-postalarının ne kadar etkili olduğunu ve katılımcıların bu tür e-postalara karşı ne kadar savunmasız olduklarını ortaya koymaktadır.

Çizelge 4.16. Gönderilen oltalama e-postasındaki bağlantıya tıklanma sayısı ile ilgili istatistiki bilgiler

Ortalama	2,39
Medyan	2,00
Mod	1
Standart Sapma	1,936
Çarpıklık	2,872
Çarpıklığın Std. Hatası	0,229
Basıklık	12,239
Basıklığın Std. Hatası	0,455
Minimum	1
Maksimum	14



Şekil 4.6. Gönderilen oltalama e-postasındaki bağlantıya tıklanma sayısının grafiği

5. SONUÇ, TARTIŞMA VE ÖNERİLER

Bu araştırmanın amacı, Türkiye'de resmi kurumlarda görev yapan öğretmenlerin siber güvenlik farkındalıklarını simüle edilmiş oltalama e-postaları yoluyla ölçmek ve analiz etmektir. Gerçekçi oltalama tehditlerini tanıma ve bu tehditlere uygun tepkiler verme becerilerini değerlendirmeyi hedefleyen bu çalışma, öğretmenlerin siber saldırılara karşı reaksiyonlarını belirlemeye yardımcı olmuştur. Elde edilen bulgular, eğitim kurumlarının siber güvenlik önlemlerini güçlendirmesi gerektiğini vurgulamakta ve öğretmenlerin bu konudaki bilinç ve becerilerini geliştirmek için öneriler sunmaktadır. Bu bölümde, araştırmanın sonuçları ve bu sonuçların eğitim sektörü için taşıdığı önemin yanı sıra siber güvenlik farkındalığının artırılması için stratejik öneriler sunulacaktır.

5.1. Sonuç ve Tartışma

Üniversite etik kurulundan alınan onay ile hazırlanan Katılımcılar İçin Bilgilendirilmiş Gönüllü Olur Formu, Google Forms üzerinde Türkiye genelinde ulaşılan öğretmenlere gönderilmiş, öğretmenlere araştırmaya katılıp katılmayacakları sorulmuş ve araştırmaya katılmaya onay veren öğretmenlerden oltalama e-postalarının gönderileceği e-posta adreslerinin yanı sıra branş ve okul düzeyi bilgileri de toplanmıştır. Bu formu dolduran 233 öğretmenden 197'si araştırmaya katılmaya onay vermişlerdir.

Araştırmanın hassas bir konu olmasından kaynaklı hedeflenen sayıya ulaşmak zor olmuştur. Ancak araştırmaya katılmaya onay veren 197 katılımcı, farklı okul düzeylerinde görev yapan 32 farklı branştan öğretmendir. En fazla katılım %53,8 ile lise düzeyinde gerçekleşmiştir. Branş olarak incelendiğinde, en fazla katılım %25,9 ile Bilişim Teknolojileri, %14,7 ile Sınıf öğretmenleri yer almaktadır. Branş dağılımı fazla olduğu için bazı branşlarda katılım 1 ile sınırlı kalmıştır.

Oltalama simülasyonu 13.05.2024-15.05.2024 tarihleri arasında gerçekleştirilmiştir. Kurumsal firmalarda kullanılan uygulamaların uygunluğu ve sadece kurumsal hesaplara yönelik gerçekleştirildiği için bu simülasyonlar sık sık ve kolay bir şekilde uygulanmaktadır. Ancak öğretmenler farklı e-posta hizmet sağlayıcılardan edindikleri e- posta hesaplarını kullandıkları için oltalama simülasyonu gerçekleştirmek kolay olmamıştır. Öğretmenlerin ilgisini çekecek meslekleri ve branşlarına uygun tasarlanan oltalama e-postası toplanan e-posta adreslerine gönderilmiş ve bu e-postaların takibi

Mailsuite isimli uygulama ile sağlanmıştır. Gönderilen oltalama e-postalardan sadece 1 tanesi, e-posta adresinin yanlış yazılması ya da teknik nedenler gibi olası nedenlerden dolayı adrese ulaşmamıştır ve bu yüzden araştırmanın analizi 196 katılımcı üzerinden yürütülmüştür.

Oltalama e-postası gönderilen 196 katılımcıdan 138'i e-postayı açmış, 58'i e-postayı açmamıştır. E-postayı açma oranı %70,4 ile oldukça yüksek bir orandır. Bu durum katılımcıların gönderilen e-postayı inceledikleri, e-posta iletişimine dikkat ettiklerini göstermektedir. %29,6'lık oranla 58 kişinin e-postayı açmama nedeni bilinmemektedir. Araştırmanın sınırlılıklarından biri olana bu durum kullanılan e-posta takip uygulamasının gönderilen e-postanın spam kutusuna mı yoksa gelen kutusuna mı düştüğünü tespit edememektedir. 58 kişinin e-postayı açmama olasılıkları arasında bilgi güvenliği farkındalıklarının yüksek olmasından dolayı oltalama e-postasını tanımaları, e-postanın spam kutusuna düşmesi, paylaşılan e-posta adresinin çok kullanılan bir e-posta hesabı olmamasından kaynaklı e-postayı fark etmemeleri olabilir.

E-postayı açan 138 katılımcıdan 111'i e-posta içindeki bağlantıya tıklamıştır ki bu durum %80,4 ile oldukça yüksek bir orandır. %19,6'lık bir oranı kapsayan 27 kişi ise bağlantıya tıklamamıştır. Bu kişilerin oltalama farkındalıklarının yüksek olduğu söylenebilir. Bağlantıya tıklayanların ise farkındalıklarının yüksek olmadığı, e-postayı gönderenin posta hesabı ile bağlantının adresini kontrol etmedikleri söylenebilir. Her ne kadar bağlantı herhangi bir zararlı web sitesine yönlendirmese, kötü amaçlı bir yazılım yüklemese ya da başka herhangi bir siber saldırıya maruz bırakmasa da bağlantıya tıklayanlar için oldukça riskli bir durumdur. Gerçek bir oltalama e-postası olsaydı katılımcılar kişisel hesap ve cihazlarını kullandıkları için ciddi bir siber saldırıya maruz kalabilirdi.

Katılımcıların e-posta açma davranışları ile branşları ve okul düzeyleri arasında anlamlı bir ilişki olup olmadığı ayrı ayrı incelenmiş ve ne branşları ne de okul düzeyleri arasında anlamlı bir ilişki olmadığı bulunmuştur. Benzer şekilde katılımcıları gönderilen e- postadaki bağlantıya tıklama davranışları ile branşları ve okul düzeyleri arasında anlamlı bir ilişki olup olmadığı da ayrı ayrı incelenmiş ve yine anlamsal bir ilişki olmadığı tespit edilmiştir. Kısaca katılımcılarının branşları ile görev yaptıkları okul düzeylerinin e-posta açma davranışları veya e-postadaki bağlantıya tıklama davranışları üzerinde bir etkisi yoktur. Ancak bu araştırmada, bazı kategorilerde gözlenen değerler beklenenin altında

kalmıştır, bu da bazı kategorilerde örneklem büyüklüklerinin yetersiz olduğunu göstermektedir. Bu durum, elde edilen sonuçların genel geçerliliği ve güvenilirliği üzerinde etkileyici olabilir.

Araştırmaya en fazla Bilişim Teknolojileri branşından öğretmenler katılmışlardır. Bu branştaki öğretmenlerin bu tür saldırılara karşı farkındalıklarının yüksek olduğu düşünülse de katılan 51 öğretmenden %72,55'lik bir oranda 37 öğretmen gönderilen oltalama e-postasını açmış, e-postayı açan 31 (%83,78) öğretmen de bağlantıya tıklamışlardır. Dolayısıyla bu örnekte de görüldüğü gibi siber güvenlik alanında en bilgili kişilerin bile farkındalıklarının düşük olduğu ve oltalama e-postasını açma ve e-postadaki bağlantıya tıklama davranışı üzerinde branşların etkisinin olmadığı görülmektedir.

Gönderilen oltalama e-postasını bazı katılımcıların birden fazla kere açtığı gözlemlenmiştir. E-postaların defalarca açılmasının nedenleri arasında katılımcıların dikkatli olup içeriği birden fazla kez kontrol ettikleri ya da katılımcıların MEBBİS üzerinden gerekli kontrollerini yapıp e-posta içeriğinin doğru olup olmadığını kontrol etmelerinden kaynaklı olabilir. Aynı şekilde bazı katılımcıların da birden fazla kere e- posta üzerinde yer alan bağlantıya tıkladıkları gözlemlenmiştir. Bu tür tıklama davranışları, oltalama epostalarının ne kadar etkili olduğunu, katılımcıların bu tür e-postalara karşı ne kadar savunmasız olduklarını ve bağlantıya tıklandığında bunun bir oltalama simülasyonu olduğunu belirten bir uyarı görseli gelmesine rağmen emin olmak için birden fazla bağlantıya tıkladıklarını göstermektedir.

Bu araştırma, öğretmenlerin oltalama saldırılarına karşı farkındalığın tespiti amacıyla gerçekleştirilmiş ve birçok önemli bulgu elde edilmiştir. Bu bulgular arasında özellikle, e-posta açma ve bağlantılara tıklama davranışlarının yüksek oranda olması, öğretmenlerin bu tür tehditleri yeterince tanımadıklarını ve dolayısıyla savunmasız olduklarını göstermektedir. Eğitim sektöründeki bu güvenlik açıklarının kapatılması için öğretmenlere yönelik kapsamlı siber güvenlik eğitimlerine ve farkındalık programlarına ihtiyaç duyulduğunu ortaya koymaktadır. Araştırmanın, katılımcı örneklem büyüklüğünün ve demografik çeşitliliğinin yetersiz olması gibi sınırlılıklar göz önünde bulundurulduğunda, elde edilen sonuçların belli bir dikkatle değerlendirilmesi gerektiği anlaşılmaktadır. Daha büyük ve dengeli örneklemlerle yapılacak gelecekteki çalışmalar, bu tür analizlerde daha sağlıklı ve güvenilir sonuçlar sağlayabilir. Ancak bu sınırlılıklara rağmen elde edilen

bulgular, eğitim sektöründe siber güvenlik farkındalığının artırılması gerektiğini vurgulamaktadır. Genel olarak, öğretmenlerin siber tehditlere karşı daha dirençli hale gelmeleri için sistemli bir eğitim yaklaşımının benimsenmesi zorunluluk taşımaktadır. Bu bağlamda, eğitim politikalarının güncellenmesi ve öğretmenlerin siber güvenlik konusunda daha bilinçli hale getirilmesi, hem bireysel hem de kurumsal güvenlik için kritik öneme sahiptir.

5.2. Öneriler

Elde edilen bu sonuçlar neticesinde Türkiye'deki öğretmenlerin oltalama saldırıları farkındalığını artırmak için etkili çalışmalar yapılmalıdır. Bu çalışmalar için 8 ayrı başlıkta şu öneriler sunulabilir:

1. Eğitim programlarının yaygınlaştırılması ve zenginleştirilmesi:
    a. Öğretmenlerin siber güvenlik ve oltalama saldırıları hakkında bilinçlendirilmesi için düzenli ve zorunlu eğitim programları düzenlenmelidir. Bu eğitimler, sadece Bilişim Teknolojileri öğretmenleri ile sınırlı kalmamalı, tüm branşlardaki öğretmenleri kapsamalıdır.
    b. Eğitimlerin içeriği, gerçekçi oltalama senaryoları, simülasyonlar ve interaktif oturumlarla zenginleştirilmelidir.
    c. Millî Eğitim Bakanlığı, bu eğitimleri hem yüz yüze hem de çevrimiçi platformlar aracılığıyla sunarak erişilebilirliği artırmalıdır.
2. Sürekli farkındalık kampanyaları:
    a. Türkiye genelinde tüm okullarda sürekli farkındalık kampanyaları düzenlenmelidir.
    b. Bu kampanyalar kapsamında, öğretmenlere ve öğrencilere yönelik afişler, broşürler, e-posta bültenleri ve bilgilendirici videolar hazırlanmalıdır.
    c. Siber güvenlik bilincini artırmak amacıyla düzenli olarak seminerler ve atölye çalışmaları yapılmalıdır.
3. Pratik simülasyon ve tatbikatlar:
    a. Öğretmenlerin siber saldırılara karşı tepkilerini ölçmek için düzenli olarak oltalama simülasyonları yapılmalıdır.
    b. Bu simülasyonlar, öğretmenlerin güvenlik açıklarını fark etmelerini ve doğru tepkiler vermelerini sağlayacak şekilde tasarlanmalıdır.
    c. Simülasyon sonuçları değerlendirilerek öğretmenlere geri bildirim verilmelidir.

4. Dijital okuryazarlık dersleri:
    a. Siber güvenlik konuları, öğretmenlerin meslek içi gelişim programlarına entegre edilmelidir.
    b. Öğretmenlerin dijital okuryazarlık düzeylerini artırmak için kapsamlı dersler verilmelidir.
    c. Bu derslerde, güvenli internet kullanımı, güçlü şifre oluşturma, veri koruma ve oltalama saldırılarını tanıma gibi konular işlenmelidir.
5. İşbirlikleri ve kaynak paylaşımı:
    a. Millî Eğitim Bakanlığı, siber güvenlik alanında uzman kurumlar ve üniversitelerle işbirliği yaparak öğretmenlere yönelik eğitim materyalleri ve kaynaklar sağlamalıdır.
    b. Özel sektör ve sivil toplum kuruluşları ile ortak projeler geliştirilmeli ve öğretmenlere yönelik destek programları oluşturulmalıdır.
6. Teknolojik altyapının güçlendirilmesi:
    a. Okullarda kullanılan bilgisayar sistemleri ve ağ altyapıları, siber saldırılara karşı daha dirençli hale getirilmelidir.
    b. Güncel antivirüs programları ve güvenlik yazılımları kullanılmalı, düzenli olarak güncellemeler yapılmalıdır.
    c. Öğretmenlerin ve öğrencilerin güvenli internet erişimini sağlamak amacıyla güvenlik duvarları ve filtreleme sistemleri güçlendirilmelidir.
7. Kurum içi iletişim ve e-posta kullanım politikaları:
    a. Öğretmenlerin, kurum içi iletişimlerinde ve işlerinde kişisel e-posta hesaplarını kullanmaları yerine, Millî Eğitim Bakanlığı tarafından sağlanan kurumsal e-posta adreslerini kullanmaları zorunlu hale getirilmelidir.
    b. Kurumsal e-posta kullanımının yaygınlaştırılması ile düzenli aralıklarla oltalama simülasyonları gerçekleştirilebilir ve sonuçlarına göre zorunlu eğitimler düzenlenebilir.
    c. Bu e-posta politikası, öğretmenlerin siber saldırılara karşı daha iyi korunmasını sağlar ve kurumsal veri güvenliğini artırır.
8. Geri bildirim ve iyileştirme:
    a. Düzenli olarak yapılan eğitimler ve simülasyonların etkinliği değerlendirilerek iyileştirme çalışmalarına gidilmelidir.
    b. Öğretmenlerin siber güvenlik konusundaki geri bildirimleri toplanmalı ve eğitim programları bu doğrultuda güncellenmelidir.

KAYNAKLAR

1. İnternet: Charles Duell. (2006). *Vikisöz.* URL: https://tr.wikiquote.org/wiki/Charles_Duell, Son Erişim Tarihi: 13.12.2023.

2. Chatchalermpun, S., & Daengsi, T. (2021). Improving cybersecurity awareness using phishing attack simulation. *IOP Conference Series: Materials Science and Engineering,* 1088(1), 012015.

3. İnternet: Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2023. (2023, Ağustos). *Türkiye İstatistik Kurumu (TÜİK).* URL: https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2023-49407, Son Erişim Tarihi: 15.03.2023.

4. İnternet: Digital 2024 Global Overview Report. (2023). *We Are Social & MeltWater.* URL: https://wearesocial.com/uk/blog/2024/01/digital-2024/, Son Erişim Tarihi: 23.02.2024.

5. İnternet: DBIR 2023 Data Breach Investigations Report. (2023). *Verizon.* URL: https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf, Son Erişim Tarihi: 15.01.2024.

6. İnternet: Global Risks Report 2022. (2022). *World Economic Forum.* URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf, Son Erişim Tarihi: 15.01.2024.

7. Farrell, C. (2020). *Phishing in the Financial Sector* (Yüksek Lisans tezi - Order No. 28092202). ProQuest Dissertations & Theses Global.(2451165180).

8. Brı˙dgers, G., Hausman, C., Tomeo, A. & Umapathy, G. V. (2023). The evolving phishing landscape., J. Bı˙ngham ve T. Martı˙n (Editörler). *Phishing for dummies.* John Wı˙ley & Sons, Inc., s. 11-16.

9. İnternet: Q3 2023 Phishing and Malware Report. (2023). *Vade Secure.* URL: https://www.vadesecure.com/hubfs/Ressource%20Marketing%20Website/Report/Q3%202023%20Phishing%20and%20Malware%20Report-EN.pdf, Son Erişim Tarihi: 19.01.2024.

10. İnternet: The State of Phishing 2023. (2023). *SlashNext Security.* URL: https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf, Son Erişim Tarihi: 19.01.2024.

11. 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

12. İnternet: Phishing By Industry Benchmarking Report 2023. (2023). *KnowBe4, Inc.* URL: https://www.knowbe4.com/hubfs/2023-Phishing-by-Industry-Benchmarking-Report-Research-EN_US.pdf, Son Erişim Tarihi: 01.02.2024.

13. Kahriman, Y. (2022). *Türkiye'de siber güvenlik alanında yapılan tezlerin incelenmesi: Bibliyografik bir çalışma,* Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Konya.

14. Çakır, H., & 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.

15. İnternet: Yıllık Hizmetiçi Eğitim Planı. (2023). *MEB Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü*. URL: http://oygm.meb.gov.tr/dosyalar/planlar/2023_Plan.pdf, Son Erişim Tarihi: 25.02.2024.

16. Hadnagy, C. (2018). *Social engineering: The art of human hacking* (Second Edition). Kanada: John Wiley & Sons, s.1-16

17. Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security*, 136, 103558.

18. İnternet: History of Phishing. *Phishing.org.* URL: https://www.phishing.org/history-of-phishing, Son Erişim Tarihi: 27.02.2024.

19. 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.

20. İnternet: Ollman, G. (2007). The Phishing Guide Understanding & Preventing Phishing Attacks. *IBM Corporation.* URL: https://nsi.org/ReferenceLibrary/630.pdf, Son Erişim Tarihi: 27.02.2024.

21. İnternet: What is phishing? Find definitions, Examples & Solutions. *Vade Secure.* URL: https://www.vadesecure.com/en/phishing#phishing-definition, Son Erişim Tarihi: 22.02.2024.

22. İnternet: Phishing Activity Trends Report, 4th Quarter 2023. (2023). *The APWG.* URL: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf, Son Erişim Tarihi: 25.02.2024.

23. İnternet: What Is Phishing? (2024). *Cisco.* URL: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html, Son Erişim Tarihi: 22.02.2024.

24. İnternet: Phishing. (2023). *CISA.* URL: https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf, Son Erişim Tarihi: 22.02.2024.

25. Ahamid, I., Abawajy, J., & Kim, T.-H. (2013). Using feature selection and classification scheme for automating phishing email detection. *Studies in Informatics and Control,* 22(1):61–70.

26. Baker, E. M., Tedesco, J. C., & Baker, W. H. (2006). Consumer Privacy and Trust Online: An Experimental Analysis of Anti-Phishing Promotional Effects. *Journal of Website Promotion*, 2(1-2):89–113.

27. Yearwood, J., Webb, D., Ma, L., Vamplew, P., Ofoghi, B., & Kelarev, A. (2009). Applying clustering and ensemble clustering approaches to phishing profiling. *In Proceedings of the Eighth Australasian Data Mining Conference*, 25–34.

28. Shyni, C. E. & Swamynathan, S. (2013). Protecting the Online User's Information Against Phishing Attacks Using Dynamic Encryption Techniques. *Journal of Computer Science*, 9(4), 526-533..

29. Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions. *IEEE Access*, 10, 36429–36463.

30. Goel, D., & Jain, A.K. (2017). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Comput. Secur.*, 73, 519-544.

31. İnternet: List of phishing incidents. *Wikipedia.* URL: https://en.wikipedia.org/wiki/List_of_phishing_incidents, Son Erişim Tarihi: 25.02.2024.

32. İnternet: Phishing Attacks: Everything You Need to Know. (2021). *Airo Software*. URL: https://www.airosoftware.com/phishing-attacks-all-you-need-to-know/ , Son Erişim Tarihi: 25.02.2024.

33. İnternet: Cost of a data breach report 2023. (2023). *IBM Corporation.* URL: https://www.ibm.com/downloads/cas/E3G5JMBP, Son Erişim Tarihi: 25.02.2024.

34. İnternet: Cyber kill chain. *Lockheed Martin.* URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, Erişim Tarihi: 26.02.2024.

35. Jakobsson, M. & Myers, S. (2007). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. New Jersey: John Wiley&Sons, Inc. s.5-23.

36. 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.

37. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, 17, 1–24.

38. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3.

39. 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.

40. Kaur, A., & Mian, S. M. (2023). A Review on Phishing Technique: Classification, Lifecycle and Detection Approaches. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE).*

41. Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., & Guizani, M. (2017). Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection. *IEEE Communications Surveys & Tutorials*, 19(4), 2797–2819.

42. İnternet: Global Phishing Activity. *OpenPhish.* URL: https://openphish.com/phishing_activity.html, Son Erişim Tarihi: 02.05.2024.

43. İnternet: Crisc, J. (2023, 19 Nisan). The History of Phishing: A Deep Dive into its Global Impact and High Profile Incidents. *Linkedln.* URL: https://www.linkedin.com/pulse/history-phishing-deep-dive-its-global-impact-high-dr-jason/, Son Erişim Tarihi: 28.02.2024.

44. İnternet: Phishing: number of affected brands 2009-2023. (2024). *Statista.* URL: https://www.statista.com/statistics/266156/number-of-brands-hijacked-by-phishing-attacks/, Son Erişim Tarihi: 28.02.2024.

45. İnternet: State of the Phish 2024. (2024). *Proofprint.* URL: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf, Son Erişim Tarihi: 28.02.2024.

46. İnternet: Outcomes of successful phishing attacks in companies worldwide 2021-2023. (2024). *Statista.* URL: https://www.statista.com/statistics/1350723/consequences-phishing-attacks/, Son Erişim Tarihi: 20.02.2024.

47. Chanti, S. & Chithralekha, S. (2022). A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, 9(89).

48. Heartfield, R., & Loukas, G. (2015). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, 48(3), 37:1-37:39.

49. Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems With Applications*, 106, 1–20.

50. İnternet: Kyle, C. (2024, 18 Ocak). 19 most common types of phishing attacks in 2024. *Upguard.* URL: https://www.upguard.com/blog/types-of-phishing-attacks, Son Erişim Tarihi: 20.03.2024.

51. Valecha, R., Mandaokar, P., & Rao, H. R. (2021). Phishing email detection using persuasion cues. *IEEE Transactions on Dependable and Secure Computing*, 19(2), 747-756.

52. İnternet: Polatsek, M. (2022, 5 Ağustos). Phishing emails. *CybeReady*. URL: https://cybeready.com/awareness-training/black-friday-phishing-email-examples, Son Erişim Tarihi: 20.03.2024.

53. İnternet: Phishing Examples. *Phishing.org.* URL: https://www.phishing.org/phishing-examples, Son Erişim Tarihi: 20.03.2024.

54. Basit, A., Zafar, M., Javed, A. R., & Jalil, Z. (2020). A novel ensemble machine learning method to detect phishing attack [Conference presentation]. *2020 IEEE 23rd International Multitopic Conference (INMIC),* Bahawalpur, Pakistan, 1-5.

55. İnternet: Phishers' favorites 2023 year-in-review. (2024). *Vade Secure*. URL: https://www.vadesecure.com/hubfs/Ressource%20Marketing%20Website/eBooks/Phishers%20Favorites%202023%20Year%20in%20Review/Vade-Phishers%20Favorites%202023-EN.pdf, Son Erişim Tarihi: 20.03.2024.

56. İnternet: Zscaler ThreatLabz 2024 Phishing Report. (2024). *Zscaler, Inc.* URL: https://www.zscaler.com/resources/industry-reports/threatlabz-phishing-report-2024.pdf, Son Erişim Tarihi: 20.03.2024.

57. İnternet: Spear-phishing email: Most favored APT attack bait. (2012). T*rend Micro, Inc.* URL: https://documents.trendmicro.com/assets/wp/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf, Son Erişim Tarihi: 20.03.2024.

58. İnternet: Yıldırım, S. (2016, 24 Kasım). Spear phishing nedir? https://serkanyildirim.me/spear-phishing-nedir/, Son Erişim Tarihi: 20.03. 2024.

59. İnternet: Recent phishing attacks: How they were executed and what we can learn. (2024). *LivingSecurity.* URL: https://www.livingsecurity.com/blog/recent-phishing-attacks-and-lessons, Son Erişim Tarihi: 20.03.2024.

60. İnternet: Petrosyan, A. (2023, 18 Ağustos). Impact of spear-phishing attacks in global companies 2022. *Statista.* URL: https://www.statista.com/statistics/1406109/companies-worldwide-impact-spear-phishing/#statisticContainer, Son Erişim Tarihi: 20.03.2023.

61. İnternet: Tunggal, A.,T. (2023, 2 Mayıs). What is a whaling attack?. *Upguard.* URL: https://www.upguard.com/blog/whaling-attack , Son Erişim Tarihi: 20.03.2024.

62. Mishra, S., & Soni, D. (2019). SMS Phishing and Mitigation Approaches. *2019 Twelfth International Conference on Contemporary Computing* (IC3), 1–5.

63. İnternet: İstanbul Büyükşehir Belediyesi. (2024, 2 Ocak). ÖNEMLİ DUYURU Bazı vatandaşlarımızın telefonlarına Mezarlıklar Daire Başkanlığımızdan gelmiş gibi görünen bu mesajın ulaştığı tespit edilmiştir. Söz konusu mesajla ilgili vatandaşlarımızın hiçbir işlem yapmamasını önemle rica ederiz. [Tweet]. *Twitter*. URL: https://x.com/istanbulbld/status/1742237048503722356, Son Erişim Tarihi: 20.03.2024.

64. İnternet: Yüksel, C. (2023, 30 Kasım). Dolandırıcıların yeni yöntemine dikkat! Sakın linke tıklamayın! *Yenigün Gazetesi.* URL: https://www.gazeteyenigun.com.tr/haber/18041182/dolandiricilarin-yeni-yonteminedikkat-sakin-linke-tiklamayin, Son Erişim Tarihi: 20.03.2024.

65. Saud Al-Musib, N., Mohammad Al-Serhani, F., Humayun, M., & Jhanjhi, N. (2023). Business email compromise (BEC) attacks. *Materials Today: Proceedings*, 81, 497–503.

66. İnternet: 2023 Internet Crime Report. (2024). *FBI Internet Crime Complaint Center FBI I3*. URL: https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf, Son Erişim Tarihi: 21.03.2024.

67. İnternet: Britton, M. (2024, 7 Mart). Key takeaways from the 2023 FBI IC3 report: business email compromise losses jump to nearly $3 billion. *Abnormal Security*. URL: https://abnormalsecurity.com/blog/2023-fbi-ic3-report-takeaways, Son Erişim Tarihi: 21.03.2024.

68. İnternet: Baron, C. H. (2023, 28 Nisan). 11 most costly BEC attack examples of the past 10 years. *Abnormal Security*. URL: https://abnormalsecurity.com/blog/most-costly-bec-attack-examples, Son Erişim Tarihi: 21.03.2024.

69. İnternet Phishing Frenzy: C-Suite Receives 42x More QR Code Attacks Than Average Employee - H1 2024 Email Threat Report. (2024). *Abnormal Security*. URL: https://cdn2.assets-servd.host/gifted-zorilla/production/files/Phishing-Frenzy- C-Suite-Receives-42x-More-QR-Code-Attacks.pdf, Son Erişim Tarihi: 21.02.2024.

70. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023, September). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132, 103387.

71. 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.

72. 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.

73. bin Othman Mustafa, M. S., Nomani Kabir, M., 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.

74. 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.

75. 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.

76. ARSLAN, Y. (2021). Phishing Attacks Awareness Exercise Example. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi,* 9(3), 348–358.

77. Aljumah, Y., & Ahmed, S. S. (2021). A Novel Approach to Get Awareness in Saudi Arabia Regarding Phishing Attacks. *2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE),* 1-5.

78. Lain, D., Kostiainen, K., & Čapkun, S. (2022). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. *2022 IEEE Symposium on Security and Privacy (SP),* 842-859.

79. 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.

80. 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.

81. 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.

82. Carroll, F., Adejobi, J. A., & Montasari, R. (2022). How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. *SN Computer Science,* 3(2).

83. Aslan, M. (2022). *Maintaining Cybersecurity Awareness In Large-Scale Organizations: A Pilot Study In A Public Institution*. Yüksek Lisans Tezi, Çankaya Üniversitesi, Bilgisayar Mühendisliği, Ankara.

84. Drummonds, A. O., Henry, J., & Mirpuri, K. (2022). An Analysis of Website Phishing Awareness in Jamaica. *SoutheastCon* 2022, 368-373.

85. Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security,* 132, 103364.

86. Kenneth, A., Hayashi, B. B., Lionardi, J., Richie, S., Achmad, S., Junior, F. A., & Nadia. (2023). Phishing Attack Awareness Among College Students. *2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS).*

87. İnternet: Abreu, G. (2023, 27 Temmuz). Kartopu örneklemesi: Güçlü bir araştırma aracının sırlarını açığa çıkarma. *Mind the GRAPH*. URL: https://mindthegraph.com/blog/tr/kartopu-ornekleme/, Son Erişim Tarihi: 10.04.2024.

88. İnternet: Millî Eğitim Bakanlığı Bilişim Sistemleri Hizmetiçi Eğitim Modülü. *MEBBİS.* URL: https://mebbis.meb.gov.tr/HizmetIci/hie04001.aspx, Son Erişim Tarihi: 10.04.2024.

89. İnternet: Email tracking. *Mailsuite*. URL: https://mailsuite.com/en/dashboard/, Son Erişim Tarihi: 10.05.2024.

EKLER

EK-1. Etik Kurul Onay Yazısı

Evrak Tarih ve Sayısı: 12.12.2023-E.819251

T.C.
GAZİ ÜNİVERSİTESİ REKTÖRLÜĞÜ
Etik Komisyonu

Sayı : E-77082166-302.08.01-819251 12.12.2023
Konu : Bilimsel ve Eğitim Amaçlı

Dağıtım Yerlerine

Üniversitemiz Bilişim Enstitüsü Elektronik Bilgisayar Eğitimi Ana Bilim Dalı **Yüksek Lisans Öğrencisi Neslihan GENÇ'in, Prof.Dr.Murat YÜCEL'in** danışmanlığında yürüttüğü ***"Öğretmenlerin Oltalama Saldırıları Farkındalığının Araştırılması "*** adlı tez çalışması ile ilgili konu Komisyonumuzun **07.11.2023** tarih ve **19** sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi rica ederim.

Araştırma Kod No: 2023 - 1440

Prof. Dr. İsmail KARAKAYA
Komisyon Başkanı

Ek:1 Liste
DAĞITIM
Gereği:
Sayın Prof. Dr. Murat YÜCEL

Bilgi:
Bilişim Enstitüsü Müdürlüğüne

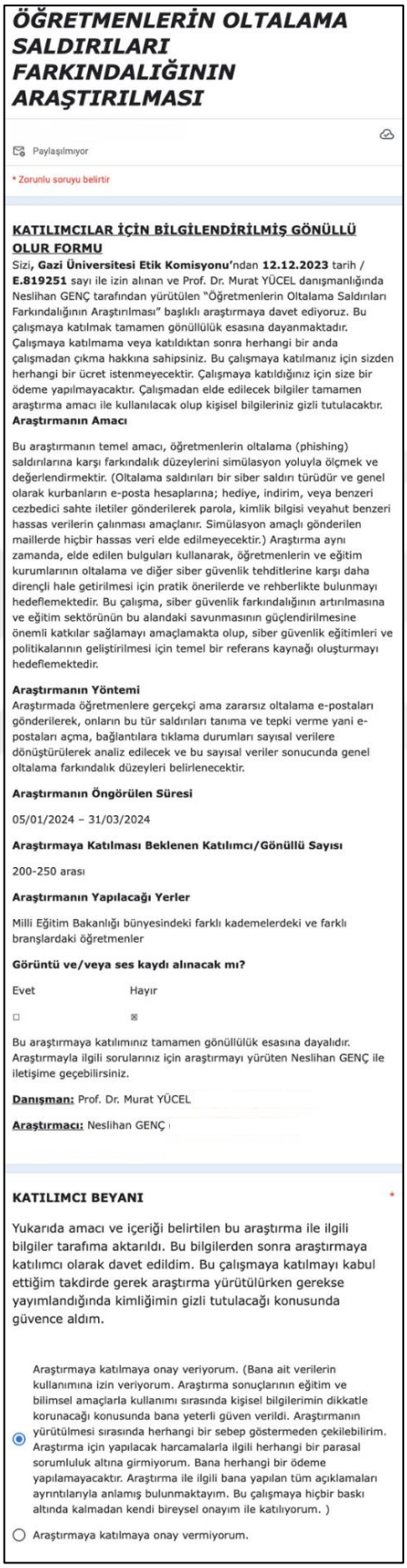
Bu belge, güvenli elektronik imza ile imzalanmıştır.
Belge Doğrulama Kodu :BS4HE3N1H3 Belge Takip Adresi : https://www.turkiye.gov.tr/gazi-universitesi-ebys

Emniyet Mahallesi Bandırma Caddesi No :6/1 06560 Yenimahalle/ANKARA
Tel:0 (312) 202 20 57 - 0 (312) 2... Faks:0 (312) 202 38 76
İnternet Adresi :http://etikkomisyon.gazi.edu.tr/
Kep Adresi: gaziuniversitesi@hs01.kep.tr

Bilgi için :Nurvel Gömer
Genel Evrak Sorumlusu
Telefon No:202 20 57

Bu belge güvenli elektronik imza ile imzalanmıştır.

EK-3. Google Forms Katılımcılar İçin Bilgilendirilmiş Gönüllü Olur Formu



ÖĞRETMENLERİN OLTALAMA SALDIRILARI FARKINDALIĞININ ARAŞTIRILMASI

Paylaşılmıyor

* Zorunlu soruyu belirtir

KATILIMCILAR İÇİN BİLGİLENDİRİLMİŞ GÖNÜLLÜ OLUR FORMU

Sizi, **Gazi Üniversitesi Etik Komisyonu'**ndan **12.12.2023** tarih / **E.819251** sayı ile izin alınan ve Prof. Dr. Murat YÜCEL danışmanlığında Neslihan GENÇ tarafından yürütülen "Öğretmenlerin Oltalama Saldırıları Farkındalığının Araştırılması" başlıklı araştırmaya davet ediyoruz. Bu çalışmaya katılmak tamamen gönüllülük esasına dayanmaktadır. Çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmadan çıkma hakkına sahipsiniz. Bu çalışmaya katılmanız için sizden herhangi bir ücret istenmeyecektir. Çalışmaya katıldığınız için size bir ödeme yapılmayacaktır. Çalışmadan elde edilecek bilgiler tamamen araştırma amacı ile kullanılacak olup kişisel bilgileriniz gizli tutulacaktır.

Araştırmanın Amacı

Bu araştırmanın temel amacı, öğretmenlerin oltalama (phishing) saldırılarına karşı farkındalık düzeylerini simülasyon yoluyla ölçmek ve değerlendirmektir. (Oltalama saldırıları bir siber saldırı türüdür ve genel olarak kurbanların e-posta hesaplarına; hediye, indirim, veya benzeri cezbedici sahte iletiler gönderilerek parola, kimlik bilgisi veyahut benzeri hassas verilerin çalınması amaçlanır. Simülasyon amaçlı gönderilen maillerde hiçbir hassas veri elde edilmeyecektir.) Araştırma aynı zamanda, elde edilen bulguları kullanarak, öğretmenlerin ve eğitim kurumlarının oltalama ve diğer siber güvenlik tehditlerine karşı daha dirençli hale getirilmesi için pratik önerilerde ve rehberlikte bulunmayı hedeflemektedir. Bu çalışma, siber güvenlik farkındalığının artırılmasına ve eğitim sektörünün bu alandaki savunmasının güçlendirilmesine önemli katkılar sağlamayı amaçlamakta olup, siber güvenlik eğitimleri ve politikalarının geliştirilmesi için temel bir referans kaynağı oluşturmayı hedeflemektedir.

Araştırmanın Yöntemi

Araştırmada öğretmenlere gerçekçi ama zararsız oltalama e-postaları gönderilerek, onların bu tür saldırıları tanıma ve tepki verme yani e-postaları açma, bağlantılara tıklama durumları sayısal verilere dönüştürülerek analiz edilecek ve bu sayısal veriler sonucunda genel oltalama farkındalık düzeyleri belirlenecektir.

Araştırmanın Öngörülen Süresi

05/01/2024 – 31/03/2024

Araştırmaya Katılması Beklenen Katılımcı/Gönüllü Sayısı

200-250 arası

Araştırmanın Yapılacağı Yerler

Milli Eğitim Bakanlığı bünyesindeki farklı kademelerdeki ve farklı branşlardaki öğretmenler

Görüntü ve/veya ses kaydı alınacak mı?

Evet	Hayır
☐	☒

Bu araştırmaya katılımınız tamamen gönüllülük esasına dayalıdır. Araştırmayla ilgili sorularınız için araştırmayı yürüten Neslihan GENÇ ile iletişime geçebilirsiniz.

Danışman: Prof. Dr. Murat YÜCEL

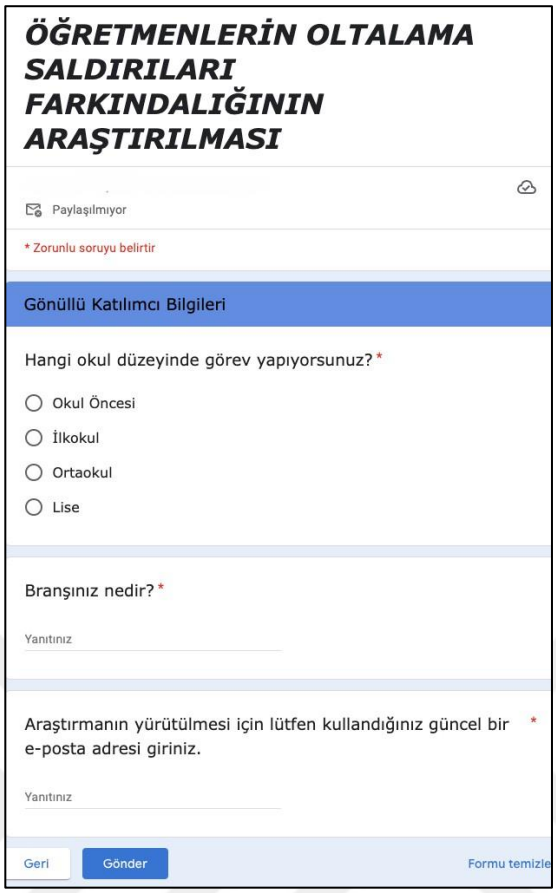
Araştırmacı: Neslihan GENÇ

KATILIMCI BEYANI *

Yukarıda amacı ve içeriği belirtilen bu araştırma ile ilgili bilgiler tarafıma aktarıldı. Bu bilgilerden sonra araştırmaya katılımcı olarak davet edildim. Bu çalışmaya katılmayı kabul ettiğim takdirde gerek araştırma yürütülürken gerekse yayımlandığında kimliğimin gizli tutulacağı konusunda güvence aldım.

◉ Araştırmaya katılmaya onay veriyorum. (Bana ait verilerin kullanımına izin veriyorum. Araştırma sonuçlarının eğitim ve bilimsel amaçlarla kullanımı sırasında kişisel bilgilerimin dikkatle korunacağı konusunda bana yeterli güven verildi. Araştırmanın yürütülmesi sırasında herhangi bir sebep göstermeden çekilebilirim. Araştırma için yapılacak harcamalarla ilgili herhangi bir parasal sorumluluk altına girmiyorum. Bana herhangi bir ödeme yapılamayacaktır. Araştırma ile ilgili bana yapılan tüm açıklamaları ayrıntılarıyla anlamış bulunmaktayım. Bu çalışmaya hiçbir baskı altında kalmadan kendi bireysel onayım ile katılıyorum.)

○ Araştırmaya katılmaya onay vermiyorum.



ÖĞRETMENLERİN OLTALAMA SALDIRILARI FARKINDALIĞININ ARAŞTIRILMASI

Paylaşılmıyor

* Zorunlu soruyu belirtir

Gönüllü Katılımcı Bilgileri

Hangi okul düzeyinde görev yapıyorsunuz? *

- Okul Öncesi
- İlkokul
- Ortaokul
- Lise

Branşınız nedir? *

Yanıtınız

Araştırmanın yürütülmesi için lütfen kullandığınız güncel bir e-posta adresi giriniz. *

Yanıtınız

Geri Gönder Formu temizle

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : GENÇ, Neslihan

Uyruğu : T.C.

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Gazi Üniversitesi / Bilişim Enstitüsü	2024
Yüksek lisans (Tezsiz)	Hoca Ahmet Yesevi Uluslararası Türk Kazak Üniversitesi / Mühendislik Fakültesi	2021
Lisans	Marmara Üniversitesi / İktisat Fakültesi	2024
Lisans	Gazi Üniversitesi / Teknik Eğitim Fakültesi	2007
Lise	Anafartalar Anadolu Ticaret Lisesi	2001

İş Deneyimi

Yıl	Yer	Görev
2023-Halen	Ataşehir Dilek Sabancı MTAL (MEB)	Bilişim Teknolojileri Bölüm Şefi
2010-Halen	Ataşehir Dilek Sabancı MTAL (MEB)	Bilişim Teknolojileri Öğretmeni
2007-2010	Melih İsfendiyar İlköğretim Okulu	Bilişim Teknolojileri Öğretmeni

Yabancı Dil

İngilizce



GAZİLİ OLMAK AYRICALIKTIR.