T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Serhat TAŞ

KÜLTÜREL BAĞLAMDA OTORİTE TEMELLİ SOSYAL MÜHENDİSLİK SALDIRILARININ ETKİNLİĞİ: TÜRKİYE VE KATAR ÖRNEĞİ

DANIŞMAN
Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Haziran 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK PROGRAMI

Serhat TAŞ

(23SIBE5001)

KÜLTÜREL BAĞLAMDA OTORİTE TEMELLİ SOSYAL MÜHENDİSLİK SALDIRILARININ ETKİNLİĞİ: TÜRKİYE VE KATAR ÖRNEĞİ

DANIŞMAN

Dr. Öğr. Üyesi Barış ÇELİKTAŞ

İSTANBUL, Haziran 2025

T.C.
IŞIK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
SİBER GÜVENLİK PROGRAMI

Serhat TAŞ
(23SIBE5001)

KÜLTÜREL BAĞLAMDA OTORİTE TEMELLİ SOSYAL MÜHENDİSLİK SALDIRILARININ ETKİNLİĞİ: TÜRKİYE VE KATAR ÖRNEĞİ

Tezin Savunulduğu Tarih: 30.06.2025

Tez Danışmanı: Dr. Öğr. Üyesi Barış ÇELİKTAŞ / Işık Üniversitesi

Diğer Jüri Üyeleri: Dr. Öğr. Üyesi Emine EKİN / Işık Üniversitesi

Dr. Öğr. Üyesi Fatih UYSAL / Kafkas Üniversitesi

İSTANBUL, Haziran 2025

ÖZET

KÜLTÜREL BAĞLAMDA OTORİTE TEMELLİ SOSYAL MÜHENDİSLİK SALDIRILARININ ETKİNLİĞİ: TÜRKİYE VE KATAR ÖRNEĞİ

Bu çalışmada otorite figürlerinin sosyal mühendislik saldırılarındaki etkinliği kültürel bir bağlamda incelenmektedir. Türkiye ve Katar'daki elektrik dağıtım şirketlerinde çalışan 900 katılımcının yer aldığı deneysel bir tasarım kullanılmıştır. Analizde, bireysel ve kurumsal otorite figürlerine göre farklılaştırılmış genel oltalama ve hedefli oltalama saldırılarının başarı oranları karşılaştırılmıştır. Sonuçlar, hedefli oltalama saldırılarının genel oltalama saldırılarına kıyasla önemli ölçüde daha yüksek başarı oranlarına ulaştığını göstermiştir. Otorite türünün etkisi kültürel bağlamlar arasında farklılık göstermiştir. Türkiye'de bireysel otorite figürlerine dayalı saldırılar daha başarılı olurken; Katar'da kurumsal otorite figürlerini kullanan saldırılar daha etkili olmuştur. Ayrıca, ülke ile otorite türü arasındaki anlamlı etkileşim, otorite temelli saldırıların etkinliğinin büyük ölçüde uygulandıkları ülkeye ve otoritenin biçimine bağlı olduğunu ortaya koymaktadır. Çalışma ayrıca, oltalamanın gerçekleşeceği web bağlantısına tıklama etkileşimi ile müteakip veri gönderimi arasında güçlü bir ardışık ilişki olduğunu ortaya koyarak, ilk güvenlik açığı ortaya çıktıktan sonra artan davranışsal kırılganlığı göstermektedir. Bulgular, sosyal mühendislik saldırılarına karşı savunma stratejileri tasarlanırken kültürel faktörlerin dikkatle değerlendirilmesi gerektiğini ve bilgi güvenliği politikaları geliştirilirken sosyokültürel kodların dikkate alınması gerektiğini ortaya koymaktadır. Özellikle, yüksek güç mesafeli kültürler otorite taleplerini sorgulamaya odaklanan eğitimler gerektirebilirken, düşük güç mesafeli kültürler otonom karar verme sürecini güçlendirmeyi amaçlayan müdahalelerden faydalanabilir. Kuruluşlara, güvenlik farkındalığı programlarını hedef kitlelerinin otorite dinamiklerine ve kültürel özelliklerine göre uyarlanmalıdır.

Anahtar Kelimeler: Siber Güvenlik, Sosyal Mühendislik, Hedefli Oltalama, Otorite Figürleri, Kültürel Faktörler

ABSTRACT

EFFECTIVENESS OF AUTHORITY-BASED SOCIAL ENGINEERING ATTACKS IN A CULTURAL CONTEXT: CASE OF TURKEY AND QATAR

This study examines the effectiveness of authority figures in social engineering attacks in a cultural context. An experimental design was employed involving 900 participants working in electricity distribution companies in Turkey and Qatar. The analysis compared the success rates of generic phishing and spear phishing attacks, differentiated by individual and institutional authority figures. The results demonstrated that spear phishing attacks achieved significantly higher success rates compared to generic phishing attacks. The impact of authority type varied across cultural contexts. In Turkey, attacks based on individual authority figures were more successful, whereas in Qatar, attacks leveraging institutional authority figures proved more effective. Furthermore, a significant interaction effect between country and authority type was observed, indicating that the effectiveness of authority-based attacks is highly contextdependent. The study also revealed a strong sequential relationship between phishing link engagement and subsequent data submission, highlighting escalating behavioral vulnerability once initial compromise occurs. The findings suggest that cultural factors must be carefully considered when designing defense strategies against social engineering attacks. In particular, high power distance cultures may require enhanced training focused on questioning authority requests, whereas low power distance cultures may benefit from interventions aimed at strengthening autonomous decision-making. Organizations are advised to tailor their security awareness programs according to the authority dynamics and cultural characteristics of their target populations.
Keywords: Cybersecurity, Social Engineering, Spear Phishing, Authority Figures, Cultural Factors

TEŞEKKÜR

Bu yüksek lisans tezinin hazırlanmasında bilgi, deneyim ve rehberlikleriyle katkı sağlayan tez danışmanım Dr. Öğr. Üyesi Barış ÇELİKTAŞ'a en içten teşekkürlerimi sunarım. Akademik bakış açısı ve yapıcı yönlendirmeleri, çalışmamın her aşamasında yol gösterici olmuştur.

Gerçek zamanlı oltalama ve hedefli oltalama deneylerinin gerçekleştirilmesinde kullanılan Phishing platformunu ve gerekli teknik altyapıyı sağlayarak çalışmaya önemli katkıda bulunan Beam Security firmasına teşekkür ederim.

Ayrıca, Beam Security firmasının aracılığıyla ulaşarak bu çalışmanın tamamen akademik amaçlarla ve kâr amacı gütmeden yürütüldüğü bilgisinin iletilmesiyle, araştırmanın ihtiyaç duyduğu kontrol ve deney gruplarının oluşturulmasına gönüllü katılım sağlayarak verdikleri kıymetli destek ve iş birlikleri için Türkiye ve Katar'daki enerji sektörü şirketlerine ve çalışanlarına içten teşekkür ederim.

Siber güvenlik sektörüne ilk adımımı atmamı sağlayan ve bu alanda gelişmem için bana fırsat sunan Barikat Siber Güvenlik firmasına, hem mesleki hem de akademik yolculuğumda bana sağladıkları destek için teşekkür ederim.

Son olarak tezli yüksek lisans programına başvurmam için beni cesaretlendiren değerli dostum Burak KOÇAK'a ve akademik yolculuğum boyunca beni koşulsuz şartsız destekleyen aileme en içten teşekkürlerimi sunarım.

Serhat TAŞ

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

BEC : Business Email Compromise (İş E-postası Ele Geçirme)

BT : Bilgi Teknolojileri

EPDK : Enerji Piyasası Düzenleme Kurumu

IEC : International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)

ISO : International Organization for Standardization (Uluslararası Standardizasyon Örgütü)

KVKK : Kişisel Verilerin Korunması Kanunu

PDPL : Personal Data Protection Law (Kişisel Verilerin Korunması Kanunu)

QCB : Qatar Central Bank (Katar Merkez Bankası)

QR : Quick Response (Hızlı Yanıt)

SMS : Short Message Service (Kısa Mesaj Hizmeti)

SPSS : Statistical Package for the Social Sciences (Sosyal Bilimler için İstatistik Paketi)

BÖLÜM 1

1. GİRİŞ

Günümüzde dijital dönüşümün hızla ilerlemesiyle birlikte, siber güvenlik tehditleri de çeşitlenmekte ve artmaktadır. Teknik güvenlik önlemlerinin etkinliğinin artmasıyla, saldırganlar güvenlik zincirinin en zayıf halkası olarak kabul edilen insan faktörünü hedef alan yöntemlere yönelmektedir (Krombholz vd., 2015). Sosyal mühendislik, insan psikolojisini manipüle ederek teknik güvenlik önlemlerini aşma sanatı olarak tanımlanmakta ve daha az teknik beceri gerektirmesi nedeniyle siber saldırganlar tarafından sıklıkla tercih edilmektedir (Wang vd., 2021; Darwish vd., 2013).

Sosyal mühendislik saldırıları çeşitli türlere ayrılmakta olup, oltalama (phishing) ve hedefli oltalama (spear phishing) en yaygın olanlarıdır (Kwak vd., 2020). Bu saldırıların etkinliğini artıran önemli faktörlerden biri, Cialdini'nin ikna prensiplerinin (otorite, beğenme, kıtlık, tutarlılık, sosyal kanıt ve karşılıklılık) kullanılmasıdır (Cialdini, 2009). Bullée vd. (2018), başarılı sosyal mühendislik saldırılarında otorite prensibinin diğer prensiplere göre önemli ölçüde daha fazla kullanıldığını göstermiştir.

Sosyal mühendislik saldırılarının başarısını etkileyen bir diğer önemli faktör kültürel bağlamdır. Hofstede'nin kültürel boyutlar teorisinde tanımlanan güç mesafesi ve belirsizlikten kaçınma boyutları, özellikle otorite algısı ve otoriteye itaat açısından önem taşımaktadır (Yasin vd., 2019). Yüksek güç mesafesine sahip kültürlerde, hiyerarşik yapıların daha belirgin ve otoriteye saygının daha önemli olması, bu külterlerdeki bireyleri otorite temelli sosyal mühendislik saldırılarına karşı daha savunmasız hale getirebilmektedir.

Literatür incelendiğinde, otorite figürlerinin kültürel bağlamda sosyal mühendislik saldırıları üzerindeki etkisinin yeterince araştırılmadığını görülmektedir. Özellikle farklı kültürlerde otorite figürlerinin karşılaştırmalı

etkileri ve bu figürlerin türlerine göre etkinliklerindeki farklılıklar, literatürde önemli bir boşluk oluşturmaktadır.

Bu çalışma, otorite temelli sosyal mühendislik saldırılarının kültürel bağlamda etkinliğini incelemeyi amaçlamaktadır. Araştırma, Türkiye ve Katar'daki elektrik dağıtım şirketlerinde çalışan 900 katılımcı üzerinde gerçekleştirilen deneysel bir tasarım kullanarak, farklı otorite figürlerine (bireysel ve kurumsal) dayalı sosyal mühendislik saldırılarına verilen tepkileri karşılaştırmaktadır.

Türkiye (66) ve Katar (93) arasındaki güç mesafesi değerlerindeki önemli fark, otorite figürlerine karşı tutumları karşılaştırmak ve otorite temelli sosyal mühendislik saldırılarının etkinliğini incelemek için uygun bir zemin oluşturmaktadır. Bu çerçevede araştırma, farklı kültürel bağlamlarda otorite figürlerinin sosyal mühendislik saldırılarının başarısı üzerindeki etkisini ortaya koyarak, kuruluşların kültürel özelliklere göre uyarlanmış savunma stratejileri geliştirmelerine katkı sağlamayı hedeflemektedir.

BÖLÜM 2

2. LİTERATÜR

2.1 SOSYAL MÜHENDİSLİK SALDIRILARI

2.1.1 Sosyal Mühendislik Kavramı ve Tanımı

Sosyal mühendislik, siber güvenlik bağlamında, teknik güvenlik önlemlerini aşmak için insan psikolojisini manipüle etme sanatı olarak tanımlanmaktadır (Conteh ve Schmick, 2016). Sosyal mühendislik kavramı, bilgisayar ve siber güvenlik alanında, saldırganın insan zaafiyetlerini etkileme, ikna, kandırma, korkutma, manipülasyon ve yönlendirme gibi yöntemlerle istismar ederek, gizli bilgilere erişim sağlamak, bilgisayar sistemlerini ve ağlarını ele geçirmek, kısıtlı alanlara yetkisiz erişim elde etmek veya siber uzayın güvenlik hedeflerini (gizlilik, bütünlük, erişilebilirlik, kontrol edilebilirlik ve denetlenebilirlik) ihlal etmek amacıyla gerçekleştirdiği bir saldırı türü olarak açıklanmaktadır (Wang vd., 2021). Özet olarak, sosyal mühendislik, saldırganın siber güvenliği ihlal etmek için sosyal etkileşim yoluyla insan zaafiyetlerini istismar ettiği bir saldırı türüdür (Wang vd., 2020).

Sosyal mühendislik kavramının kökeni, politik ve ekonomik yönetim alanındaki kullanımına dayanmaktadır. Tarihsel olarak, bu terim ilk kez 1842'de İngiliz ekonomist John Gray tarafından kullanılmıştır ve daha sonra Thorstein Veblen, Jane Addams gibi düşünürler tarafından da benimsenmiştir (Hatfield, 2017). Ancak siber güvenlik bağlamında sosyal mühendislik terimi, 1980'lerin başında hacker topluluğu içerisinde kullanılmaya başlanmıştır. 1984 yılında "2600: The Hacker's Quarterly" dergisinde yayımlanan makalelerde, sosyal mühendislik terimi, operatörleri daha fazla bilgi vermeye ikna etmek için kullanılan bir süreç olarak tanımlanmıştır (Wang vd., 2020).

Sosyal mühendislik saldırıları, teknik saldırılara kıyasla daha az teknik beceri gerektirmesi ve daha düşük maliyetli olması nedeniyle siber saldırganlar

için cazip bir seçenek haline gelmektedir. Sosyal mühendislik saldırıları, insanların bilişsel önyargılarını ve karar verme süreçlerindeki zafiyetlerini istismar ederek başarıya ulaşmaktadır. İnsanlar, tüm bilgileri işlemek için yeterli bilişsel kapasiteye sahip olmadıklarından, karar verme süreçlerinde kısayollar (sezgisel yöntemler) kullanmaktadırlar. Zihinsel kısayollar çoğu durumda işe yarasa da, bir sezgisel yöntem hatalı olduğunda bilişsel bir önyargı ortaya çıkmakta ve sosyal mühendisler, hedeflerini istenen davranışları sergilemeye yönlendirmek için bu bilişsel önyargıları manipüle etmektedirler (Birthriya vd., 2025).

Lastdrager (2014), sosyal mühendislik tanımları üzerine kapsamlı bir çalışma yürütmüş ve sosyal mühendisliği ortak tanımını; bir hedeften bilgi edinmek için kimlik taklidi kullanılan, ölçeklenebilir bir aldatma eylemi olarak ifade etmiştir. Saldırgan, kurbanı doğrudan bir dolandırıcılık yoluyla kandırmak veya dolaylı yoldan zararlı yazılım göndermek için çeşitli kanallar kullanarak, kurbanın kişisel veya gizli bilgilerini elde etmeyi amaçlamaktadır (Chiew vd., 2018).

Sosyal mühendislik saldırıları, teknik güvenlik önlemlerinin etkinliğinin artmasıyla birlikte, güvenlik zincirinin en zayıf halkası olarak kabul edilen insan faktörünü hedefleyen yöntemlere yönelmektedir. Sosyal mühendislik saldırıları, özellikle hedefli olduklarında (örneğin, spear phishing), Sony Pictures Entertainment'ın hacklenmesinden Hillary Clinton'ın başkanlık kampanyasını sarsan Demokratik Ulusal Komite sunucularının hacklenmesine kadar çeşitli ihlallerden sorumlu tutulmaktadır (Birthriya vd., 2025).

Sosyal mühendislik saldırıları, insan faktörünün kaçınılmaz olarak güvenlik sistemlerinin bir parçası olması nedeniyle evrensel bir tehdit oluşturmaktadır. Güvenlik önlemleri ne kadar iyi tasarlanmış ve uygulanmış olursa olsun, her bilgisayar sistemi bir şekilde insanlara bağımlıdır ve insan unsurları sadece savunmasız değil, aynı zamanda diğer güvenlik önlemlerini gölgede bırakacak kadar savunmasızdır. Bu güvenlik zafiyeti evrenseldir ve platform, yazılım, ağ veya ekipman yaşından bağımsızdır (Wang vd., 2020).

2.1.2 Sosyal Mühendislik Saldırılarının Türleri

Sosyal mühendislik saldırıları, çeşitli türlere ayrılmaktadır ve bu türler arasında oltalama (phishing) saldırıları en yaygın olanlarından biridir. Oltalama, dolandırıcıların kurbanı sahte bir web sitesine yönlendiren bir e-posta göndererek özel bilgileri elde etmeye çalıştığı bir sosyal mühendislik saldırısı biçimi olarak tanımlanmaktadır (Darwish vd., 2013). Oltalama saldırıları, günümüzde siber güvenlik tehditleri arasında önemli bir yer tutmakta ve kuruluşlar için ciddi riskler oluşturmaktadır (Krombholz vd., 2015).

Hedefli oltalama (spear phishing), güvenilir kaynaklardan geliyormuş gibi görünen ve belirli bireyleri veya kuruluşlar içindeki belirli departmanları hedefleyen e-postaları içeren daha sofistike bir saldırı türüdür (Kwak vd., 2020). Hedefli oltalama saldırılarında, saldırganlar hedef hakkında topladıkları kişisel bilgileri kullanarak bağlamsal olarak anlamlı kimlik taklitleri ve anlatılar oluşturmaktadır. Xu vd. (2023) tarafından yapılan bir çalışmada, hedefler hakkındaki kişisel bilgilere daha fazla erişimin, saldırılarda bağlamsal olarak anlamlı kimlik taklidi ve anlatılar oluşturulmasıyla sonuçlanabileceği belirtilmiştir.

Balina avcılığı (whaling), üst düzey yöneticileri hedefleyen hedefli oltalama saldırılarını ifade etmektedir (Khadka vd., 2023). Burrell (2024), balina avcılığı saldırılarının teknik önlemlerden ziyade psikolojik manipülasyona dayandığını ve özellikle üniversiteler gibi hiyerarşik yapıların bulunduğu ortamlarda etkili olduğunu belirtmektedir.

Sesli oltalama (vishing), telefon üzerinden gerçekleştirilen sesli oltalama saldırılarını ifade etmektedir (Longtchi vd., 2024). Sesli oltalama saldırılarında, dolandırıcılar kendilerini güvenilir bir kuruluşun temsilcisi olarak tanıtarak hedeflerinden hassas bilgiler talep etmektedir. Sesli oltalama saldırıları, özellikle yaşlı bireyler gibi teknolojik açıdan daha az bilgili kişileri hedef almakta ve genellikle kimlik doğrulama bilgilerini elde etmeye odaklanmaktadır (Ashfaq vd., 2023).

SMS oltalama (smishing), SMS üzerinden gerçekleştirilen oltalama saldırılarını ifade etmektedir. SMS oltalama saldırılarında, dolandırıcılar kurbanlarını kötü amaçlı bağlantılara tıklamaya veya hassas bilgilerini paylaşmaya ikna etmek için aciliyet veya korku gibi duygusal manipülasyonlar kullanmaktadır. SMS oltalama saldırıları, mobil cihazlardan bilgi elde etmeyi ve bağlantılara tıklanmasını sağlamayı amaçlamaktadır (Desetty vd., 2020).

Klon oltalama (clone phishing), daha önce alınan gerçek bir e-postayı kopyalayıp kötü amaçlı içerikle yeniden göndermeyi ifade etmektedir. Bu saldırı türünde, saldırganlar daha önce alıcı tarafından alınan meşru bir e-postayı kopyalayarak güven algısını istismar etmektedir. Kopyalanan e-postadaki bağlantılar veya ekler, kötü amaçlı olanlarla değiştirilmekte ve güven algısını istismar ederek veri elde etmeyi amaçlamaktadır (Jari, 2022).

İş e-postası ele geçirme (Business Email Compromise - BEC), gerçek bir çalışanın e-posta hesabını taklit ederek kuruluş içindeki diğer kişilere saldırmayı ifade etmektedir. BEC saldırılarında, saldırganlar genellikle finans departmanı çalışanlarını veya üst düzey yöneticileri hedef alarak para transferi talimatları vermektedir. BEC saldırıları, finansal talimatlar vermeyi ve para transferi yapmayı amaçlamakta ve özellikle finansal kayıplara neden olması bakımından kuruluşlar için ciddi bir tehdit oluşturmaktadır (Papathanasiou vd., 2023).

Sosyal medya oltalama (angler phishing), sosyal medya hesaplarını taklit ederek kullanıcılarla etkileşime geçmeyi ifade etmektedir. Sosyal medya oltalama saldırılarında, saldırganlar popüler markaların veya hizmet sağlayıcıların sosyal medya hesaplarını taklit ederek müşteri hizmetleri sorunlarını çözme bahanesiyle kullanıcılardan hassas bilgiler talep etmektedir. Güven kazandıktan sonra veri veya para talep etmeyi amaçlayan bu saldırılar, sosyal medya platformlarının yaygınlaşmasıyla birlikte artış göstermiştir (Jain vd., 2025).

QR oltalama (quishing), QR kodlar aracılığıyla sahte web sitelerine yönlendirerek bilgi hırsızlığı yapmayı ifade etmektedir. Nispeten yeni olan bu saldırı türünde, saldırganlar meşru görünen ancak kötü amaçlı web sitelerine yönlendiren QR kodlar oluşturmaktadır. COVID-19 pandemisi sırasında

temassız işlemlerin artmasıyla birlikte QR oltalama saldırıları da artış göstermiş ve oltalama, kötü amaçlı yazılım yükleme gibi amaçlarla kullanılmaktadır (Galadima vd., 2024).

Pretexting (bahanelendirme), saldırganın kurbanın güvenini kazanmak için sahte bir senaryo veya kimlik oluşturduğu bir sosyal mühendislik tekniğidir. Bu teknikte, saldırgan genellikle kendisini otorite figürü (örneğin, BT destek personeli, üst düzey yönetici veya dış denetçi) olarak tanıtarak hedeften hassas bilgiler talep etmektedir. Pretexting, özellikle kurumsal ortamlarda etkili olmakta ve genellikle telefon veya e-posta yoluyla gerçekleştirilmektedir (Birthriya vd, 2025).

Watering hole (su kaynağı) saldırıları, saldırganın hedef kitlenin sıklıkla ziyaret ettiği web sitelerini tespit edip bu siteleri kötü amaçlı yazılımlarla enfekte ettiği bir saldırı türüdür. Bu saldırı türünde, saldırgan doğrudan hedefi değil, hedefin güvendiği ve düzenli olarak ziyaret ettiği web sitelerini hedef almaktadır. Watering hole saldırıları, özellikle belirli bir sektör veya kuruluşu hedefleyen hedefli saldırılarda kullanılmakta ve genellikle ileri düzey tehdit aktörleri tarafından gerçekleştirilmektedir (Malik, 2020).

2.1.3 Sosyal Mühendislik Saldırılarının Aşamaları

Sosyal mühendislik saldırıları, sistematik bir yaklaşımla gerçekleştirilen ve belirli aşamalardan oluşan süreçlerdir. Literatürde bu aşamalar farklı şekillerde sınıflandırılsa da, genel olarak kabul gören bir süreç modeline göre sosyal mühendislik saldırıları; bilgi toplama, ilişki geliştirme, manipülasyon/sömürü, bilgiyi kullanma ve çıkış stratejisi olmak üzere genellikle beş temel aşamada gerçekleştirilmektedir (Mouton vd., 2016).

Sosyal mühendislik saldırılarının ilk aşaması, hedef hakkında bilgi toplama ve keşif olarak tanımlanmaktadır. İlk aşamada saldırgan, potansiyel kurbanlar ve hedef organizasyon hakkında detaylı bilgiler toplamaktadır. Açık kaynak istihbaratı (OSINT) teknikleri kullanılarak sosyal medya profilleri, kurumsal web siteleri, çevrimiçi forumlar ve diğer kamuya açık kaynaklardan bilgi edinilmektedir. Toplanan bilgiler, hedefin zayıf noktalarını tespit etmek ve

sonraki aşamalarda kullanılacak saldırı vektörlerini belirlemek için analiz edilmektedir (Krombholz vd., 2015).

İkinci aşama, ilişki kurma ve güven oluşturma sürecidir. Bu aşamada saldırgan, hedef kişi veya kurumla bir temas noktası oluşturmakta ve güven inşa etmeye çalışmaktadır. Güven oluşturma, sosyal mühendislik saldırılarının en önemli bileşenlerinden biri olarak kabul edilmektedir. Saldırgan, ilk aşamada topladığı bilgileri kullanarak hedefle ortak noktalar bulmakta, sahte kimlikler oluşturmakta ve çeşitli senaryolar geliştirmektedir. Bu süreçte pretexting (senaryo oluşturma) tekniği sıklıkla kullanılmakta ve hedefin güvenini kazanmak için özel olarak tasarlanmış hikâyeler kurgulanmaktadır (Birthriya vd, 2025).

Üçüncü aşama, manipülasyon ve sömürü aşamasıdır. Bu aşamada saldırgan, kurduğu güven ilişkisini kullanarak hedefini manipüle etmekte ve istediği bilgileri elde etmeye çalışmaktadır. Psikolojik manipülasyon teknikleri, duygusal tetikleyiciler ve ikna prensipleri bu aşamada yoğun olarak kullanılmaktadır. Hedef kişinin korku, aciliyet, merak gibi duygusal durumları tetiklenerek mantıklı düşünme yeteneği zayıflatılmakta ve bilgi güvenliği politikalarını ihlal etmesi sağlanmaktadır. Bu aşamada saldırgan, hedeften doğrudan bilgi talep edebileceği gibi, zararlı yazılımları çalıştırmasını veya güvenlik prosedürlerini atlamasını da sağlayabilmektedir (Hadnagy, 2018).

Dördüncü aşama, elde edilen bilgi ve erişimin kullanılması olarak tanımlanmaktadır. Saldırgan, önceki aşamalarda edindiği bilgileri ve erişim haklarını kullanarak asıl hedefine ulaşmaya çalışmaktadır. Bu aşamada, hedef sistemlere erişim sağlanmakta, hassas veriler elde edilmekte veya ilerleyen saldırılar için zemin hazırlanmaktadır. Saldırganın nihai amacına bağlı olarak, finansal kazanç sağlama, bilgi sızdırma, sistemlere zarar verme veya itibar zedeleme gibi farklı sonuçlar ortaya çıkabilmektedir (Conteh ve Schmick, 2016).

Beşinci ve son aşama ise, izlerin silinmesi ve çıkış stratejisidir. Son aşamada saldırgan, saldırı sürecinde bıraktığı dijital ve fiziksel izleri ortadan kaldırmaya çalışmaktadır. Log kayıtlarının silinmesi, sahte kimliklerin ortadan kaldırılması ve saldırının tespit edilmesini zorlaştıracak önlemlerin alınması bu

aşamada gerçekleştirilmektedir. Bazı durumlarda saldırgan, gelecekte tekrar kullanabilmek için kurbanla olan ilişkisini sürdürmeyi tercih edebilmektedir (Ivaturi ve Janczewski, 2011).

Sosyal mühendislik saldırılarının aşamaları, doğrusal bir süreç olarak gerçekleşebileceği gibi, döngüsel ve tekrarlayan bir yapıda da gerçekleşebilmektedir. Saldırgan, başarısız olduğu durumlarda farklı stratejiler geliştirerek süreci tekrarlayabilmekte veya aşamalar arasında geri dönüşler yapabilmektedir. Modern sosyal mühendislik saldırılarında, bu aşamaların birbirine entegre edildiği ve sınırların belirsizleştiği yapılar da gözlemlenmektedir (Aldawood ve Skinner, 2019).

2.1.4 Sosyal Mühendislik Saldırılarının Psikolojik Temelleri

Sosyal mühendislik saldırılarının başarısı, büyük ölçüde insan psikolojisinin anlaşılması ve manipüle edilmesi yeteneğine dayanmaktadır. Sosyal mühendislik saldırıları, teknik güvenlik önlemlerini aşmak yerine, güvenlik zincirinin en zayıf halkası olarak kabul edilen insan faktörünü hedef almaktadır. Sosyal mühendislik saldırılarının psikolojik temelleri, bireylerin bilişsel süreçlerindeki açıkları, karar verme mekanizmalarındaki zayıflıkları ve duygusal tepkilerini istismar etme prensiplerine dayanmaktadır (Krombholz vd., 2015).

İnsan bilişsel kapasitesinin tüm bilgileri işlemeye yeterli olmaması nedeniyle, bireyler karar verme süreçlerinde kısayollar (sezgisel yöntemler) kullanmaktadır. Zihinsel kısayollar çoğu durumda iyi çalışsa da, bir sezgisel yöntem yanlış gittiğinde bilişsel bir yanlılık ortaya çıkmakta ve sosyal mühendisler, hedeflerini istenen davranışları sergilemeye yönlendirmek için bu bilişsel yanlılıkları manipüle etmektedir (Bullée vd., 2018).

Psikolojik faktörler, sosyal mühendislik saldırılarının başarısını etkileyen insan psikolojik özellikleri veya niteliklerini ifade ederken, psikolojik teknikler, sosyal mühendislik saldırganlarının bireyleri saldırılara uymaya teşvik etmek için belirli psikolojik faktörleri istismar etmek amacıyla kullandıkları stratejileri içermektedir. Bu bağlamda, sosyal mühendislik saldırılarının başarısını artıran

en önemli psikolojik faktörler arasında otorite, güven, ihmal, bilişsel cimrilik, korku ve açgözlülük yer almaktadır (Longtchi vd., 2024).

Sosyal mühendislik saldırılarının altında yatan unsurlardan biri, insanların karar verme süreçlerini etkileyen psikolojik mekanizmalardır (Khadka vd., 2023). Greenspan (2008) tarafından geliştirilen saflık teorisi, ikna edilebilirliğe yatkınlığı açıklamakta ve güvenilirliğin bir uzantısı olarak hizmet etmektedir. İnanılırlık, makul bir kanıt olmadan birine veya bir şeye inanma istekliliğini ifade ederken, saflık buna somut bir eylem eklemekte ve olumsuz bir sonuca yol açmaktadır (Bullée vd., 2015).

İyimser yanlılık teorisi, insanların olumlu olayların başkalarına göre kendilerine daha fazla, olumsuz olayların ise başkalarına kendilerinden daha fazla olacağına inanma eğiliminde olduklarını öne sürmektedir. Weinstein (1980) tarafından geliştirilen teori, insanların genel olarak, onu azaltmak için çok sayıda girişimde bulunulsa bile, iyimser yanlılığı sürdürdüklerini göstermektedir. İyimser yanlılık ve saflık birlikte incelendiğinde, insanların sosyal mühendislik saldırılarının hedefi olmayacaklarını, olsalar bile başkalarından daha dirençli olacaklarını düşündükleri sonucuna varılabilir (Bullée vd., 2015).

Sosyal mühendislik saldırılarının başarısında önemli bir faktör, kurbanların genellikle kendilerini aldatılmaya karşı iyi donanımlı olarak görmesidir. Ancak araştırmalar, insanların yalanları ve aldatmacaları tespit etmede zayıf performans gösterdiğini ortaya koymaktadır (Krombholz vd., 2015).

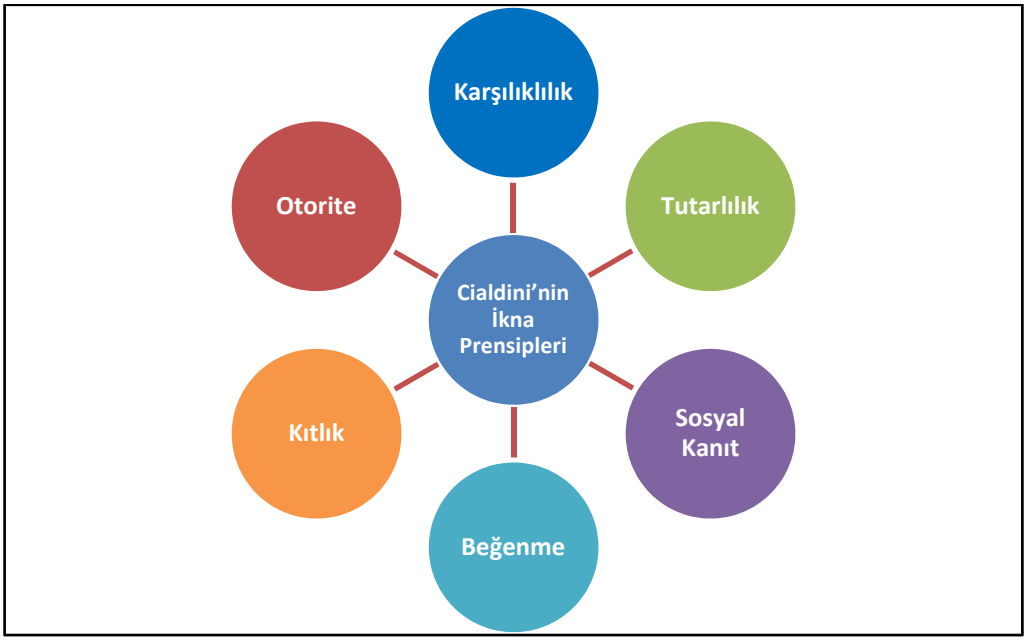
Sosyal mühendislik saldırılarının altında yatan bir diğer unsur, ikna prensiplerinin stratejik kullanımıdır. Cialdini (2009) tarafından geliştirilen altı ikna prensibi, sosyal mühendislerin hedeflerini manipüle etmek için sıklıkla kullandıkları psikolojik mekanizmaları açıklamaktadır. Bu altı ikna prensibi; karşılık verme, uyum, beğenme, kıtlık, bağlılık ve otoritedir. Cialdini'nin ikna prensipleri arasında otorite, sosyal mühendislik saldırılarında özellikle etkili bir araç olarak öne çıkmaktadır (Bullée vd., 2015).

2.2 İKNA PRENSİPLERİ, OTORİTE VE SOSYAL MÜHENDİSLİK

2.2.1 Cialdini'nin İkna Prensipleri

İkna ve etkileme süreçlerinin psikolojik temellerini inceleyen Robert B. Cialdini tarafından, insanların karar verme mekanizmalarını etkileyen prensipler ortaya konulmuştur (Cialdini, 2009). Cialdini'nin ikna prensipleri, bireylerin "Tıkla-Vınla" (Click-Whirr) şeklinde adlandırılan otomatik davranış kalıplarına dayanmaktadır. Bu prensipler, bilimsel deneysel çalışmalar ve bilhassa pazarlama ve satış alanlarındaki etki uygulayıcılarının dünyasında gerçekleştirilen saha araştırmaları neticesinde belirlenmiştir. Söz konusu prensiplerin varlığının bilinmesine karşın, bunların meşru olmayan kullanımlarını tespit etmek her durumda mümkün olamamaktadır. Zira bu prensiplerin tetiklediği davranışlar, sosyal uyum için önemli kaynak teşkil etmekte ve genellikle olumlu ve toplumsal açıdan arzu edilen davranışlar olarak değerlendirilmektedir (Schumacher, 2011). Cialdini'nin ikna prensipleri; karşılıklılık, tutarlılık, sosyal kanıt, beğenme, kıtlık ve otorite olarak sıralanmaktadır.

Karşılıkta bulunma (reciprocation) prensibi, bireylerin kendilerine sunulanı geri ödeme zorunluluğu hissetmesine dayanan güçlü bir sosyal norm niteliğindedir. Bu prensip, toplumun temelini oluşturmakta ve insanlık tarihinde sürekli ilişkilerin ve mal ve hizmet alışverişinin gelişimini sağlamaktadır (Cialdini ve Goldstein, 2004). Karşılıkta bulunma prensibi, sosyal mühendislik saldırılarında, saldırı öncesinde ücretsiz hediyeler veya iyilikler sunularak, yükümlülük hissi sebebiyle uyum olasılığının artırılması amacıyla kullanılmaktadır (CSO Online, 2013).



Şekil 2.1 Cialdini'nin İkna Prensipleri (Cialdini, 2009)

Bağlılık ve tutarlılık (commitment and consistency) prensibi, kişinin kim olduğunu ve ne yaptığını belirten bir eylem olan bağlılık ile kişinin bağlılıklarına, inançlarına ve kendine atfedilen özelliklere göre tutarlı davranmasını sağlayan tutarlılık arasındaki ilişkiyi ifade etmektedir (Cialdini ve Goldstein, 2004). Söz konusu prensip, Festinger ve Carlsmith'in bilişsel uyumsuzluk kuramına dayanmakta ve bireylerin tutumları ile davranışları arasındaki uyumu sürdürmeye yönelik motivasyonlarını öne sürmektedir (Festinger ve Carlsmith, 1959). Sosyal mühendislikte bu prensip, hedefin öncelikle küçük bir isteğe uymasının sağlanması ve ardından sunulan gerçek ve genellikle daha büyük isteğe uyum gösterme olasılığının artırılması amacıyla kullanılabilmektedir.

Sosyal kanıt (social proof) prensibi, özellikle belirsiz durumlarda ve diğer kişiler bireye benziyorsa, çevredeki diğer insanların davranışlarını veya inançlarını benimseme eğilimini ifade etmektedir. Bu prensip, bireylerin kendilerine benzeyen kişilere, örneğin arkadaşlarına ve onların kararlarına ve eylemlerine güven duyduğunu da ima etmektedir (Workman, 2008).

Beğenme (liking) prensibi, "İnsanları sevdiğinizi açıkça belirtirseniz, onların da sizi sevmemesi güçtür" şeklinde özetlenebilmektedir (Bujold, 2002). Bireyler tanıdıkları ve sevdikleri kişilerden gelen isteklere uyma eğilimi göstermektedirler. Bunun nedeni, insanların başkalarıyla sosyal ilişkiler kurma ve sürdürme temel güdüsüdür. Uyumun artırılması için algılanan benzerlik dahi yeterli olabilmektedir, zira benzerlikler potansiyel bir arkadaşlık işareti olarak değerlendirilmektedir (Cialdini ve Goldstein, 2004). Sosyal mühendisler, kendilerine karşı beğeni oluşturmak amacıyla genellikle mizahı araç olarak kullanmaktadırlar. Ayrıca çalışanların yardımsever olma arzusundan da faydalanmaktadırlar (CSO Online, 2013).

Kıtlık (scarcity) prensibi, daha az erişilebilir olan fırsatlara daha yüksek değer atfedilmesini ifade etmektedir. Bu durum, erişilebilirlikten kaliteye uzanan bir bilişsel kısayol nedeniyle gerçekleşmektedir. Ayrıca, bir şey daha kısıtlı hale geldiğinde, özgürlükler kaybedilmektedir. Tepkisellik Kuramı, bu özgürlük kaybına, giderek daha nadir hale gelen unsuru öncekinden daha fazla arzulamakla yanıt verildiğini öne sürmektedir (Brehm, 1966).

Otorite (authority) prensibi, en belirgin prensip olarak kabul edilmektedir çünkü çoğu birey yaşamları boyunca otoritelere uyma deneyimine sahiptir. Otorite konusundaki en tanınmış bilimsel araştırmalar Milgram Deneyleridir (Milgram, 1965). Miligram deneyleri, otorite kullanımının bireylerin inançlarına ve etik anlayışlarına aykırı davranmalarına dahi neden olabileceğini göstermektedir. Bu durum, genellikle üniformalar, rozetler, kimlik kartları ve unvanlar gibi otorite sembolleri için de geçerlilik taşımaktadır. Otorite kolaylıkla taklit edilebilmekte ve sorgulanması güç olmaktadır (Workman, 2008).

2.2.2 Otorite Prensibinin Sosyal Mühendislik Saldırılarındaki Rolü

Otorite prensibi, sosyal mühendislik saldırılarında en yaygın ve etkili biçimde kullanılan ikna tekniği olarak kabul edilmektedir. Cialdini'nin altı ikna prensibinden biri olan otorite, bireylerin otorite figürlerine karşı gösterdikleri doğal itaat eğilimini istismar etmektedir (Bullée vd., 2018). Otoriteye itaat etme eğilimi, insan davranışının temel bir özelliğidir ve bu eğilim, Stanley Milgram'ın

klasik otorite itaat deneyinde açıkça görülmüştür. Miligram'ın ünlü deneyinde, laboratuvar önlüğü giyen bir kişinin talimatı üzerine katılımcıların %66'sı test deneklerine 450 V dozunda elektrik verme konusunda tereddüt etmemiştir (Milgram, 1963). Tekrar çalışmaları ve meta-analizler benzer sonuçlar bulmuş ve bulgular otoritenin önemli bir davranışsal fenomen olduğunu doğrulamıştır (Burger, 2009; Packer, 2008).

Sosyal mühendislik bağlamında otorite prensibi, saldırganların kendilerini güvenilir ve yetkili bir kaynak olarak göstererek, hedeflerini belirli eylemleri gerçekleştirmeye veya hassas bilgileri paylaşmaya ikna etme sürecini ifade etmektedir (Bullée vd., 2018).

Sosyal mühendislik saldırılarının anatomisi incelendiğinde, otorite prensibinin diğer ikna tekniklerine kıyasla daha sık kullanıldığı görülmektedir. Bullée vd. (2018)'nin gerçekleştirdiği literatür analizi çalışması, başarılı sosyal mühendislik saldırılarında otorite prensibinin %32,8 oranında kullanıldığını ve bu oranın diğer ikna prensiplerine göre önemli ölçüde yüksek olduğunu ortaya koymaktadır.

Otorite temelli sosyal mühendislik saldırılarının etkinliği, insanların otoriteye karşı geliştirdikleri psikolojik tepkilerle yakından ilişkilidir. Nurse (2018), bireylerin otorite figürlerine karşı gösterdikleri itaat eğiliminin, sosyal mühendislerin istismar ettiği temel psikolojik zayıflıklardan biri olduğunu belirtmektedir. Özellikle hiyerarşik yapıların belirgin olduğu organizasyonlarda, çalışanların üst düzey yöneticilerin veya teknik uzmanların taleplerine sorgulamadan uyma eğilimi, otorite temelli saldırıların başarı oranını artırmaktadır.

Otorite prensibinin sosyal mühendislik saldırılarındaki uygulamaları çeşitlilik göstermektedir. Saldırganlar genellikle üst düzey yöneticileri, bilgi teknolojileri uzmanlarını, hukuk danışmanlarını veya güvenlik personelini taklit ederek hedeflerini manipüle etmeye çalışmaktadır (Siddiqi vd., 2022). Bu bağlamda, otorite figürünün kimliğini benimseme, saldırganın güvenilirliğini artırmak için kullanılan temel stratejilerden biridir. Örneğin, bir saldırgan

kendisini şirketin bilgi teknolojileri departmanından bir çalışan olarak tanıtarak, hedefinden parola sıfırlama işlemi için kimlik bilgilerini talep edebilmektedir.

Otorite temelli sosyal mühendislik saldırılarının önemli bir özelliği, saldırganların kullandıkları dil ve iletişim tarzıdır. Khadka vd. (2023) tarafından gerçekleştirilen araştırmada, otorite figürlerini taklit eden saldırganların genellikle resmi bir dil kullandıkları, teknik terimler ve jargonlardan yararlandıkları ve emir kipi içeren ifadeler tercih ettikleri belirtilmektedir. İzlenen iletişim stratejisi, hedeflerin saldırganın otorite konumunu sorgulamadan kabul etmesini sağlamaktadır.

Tiwari (2020), otorite temelli sosyal mühendislik saldırılarının etkinliğini artıran faktörlerden birinin de aciliyet unsuru olduğunu ifade etmektedir. Otorite figürleri tarafından iletilen acil talepler, hedeflerin eleştirel düşünme süreçlerini bypass etmelerine ve hızlı kararlar almalarına neden olmaktadır. Örneğin, üst düzey bir yöneticiden geldiği izlenimi verilen ve aciliyet içeren bir e-posta, çalışanların normal güvenlik prosedürlerini göz ardı etmelerine ve talep edilen eylemi gerçekleştirmelerine yol açabilmektedir.

Otorite prensibinin sosyal mühendislik saldırılarındaki rolü, hedef kitlenin kişilik özellikleriyle de yakından ilişkilidir. Uebelacker ve Quiel (2014) tarafından geliştirilen Sosyal Mühendislik Kişilik Çerçevesi (SEPF), otorite prensibinin özellikle sorumluluk sahibi (conscientious) ve uyumlu (agreeable) kişilik özelliklerine sahip bireylerde daha etkili olduğunu öne sürmektedir. Sorumluluk sahibi bireyler, otorite figürlerinin taleplerine uymayı bir görev olarak algılarken; uyumlu bireyler ise çatışmadan kaçınma eğiliminde olduklarından, otorite figürlerinin isteklerini reddetmekte zorlanmaktadır.

Muscanell vd. (2014), otorite temelli sosyal mühendislik saldırılarının başarısında, saldırganların kullandıkları sembollerin ve göstergelerin önemli bir rol oynadığını belirtmektedir. Araştırmacılar, otoritenin insanları etkilemede güçlü bir sosyal etki prensibi olduğunu ve bireylerin otorite figürlerini güvenilir, uzman ve doğrudan güç sahibi kişiler olarak algıladıklarını ifade etmektedir. Kurumsal logolar, profesyonel e-posta imzaları, resmi unvanlar ve pozisyonlar, teknik terminoloji ve jargon kullanımı gibi unsurlar, saldırganların otorite

algısını güçlendirmekte ve hedeflerin güvenini kazanmalarını sağlamaktadır. Örneğin, araştırmacılar 2012 yılında ABD Savunma Bakanlığı personelini hedef alan bir oltalama saldırısını incelemişler ve saldırganların ".mil" uzantılı resmi askeri e-posta adreslerini kullanarak başarılı olmaları üzerinde durmuşlardır. Araştırmacılara göre bu tür otorite göstergelerinin etkisi o kadar güçlüdür ki, bireyler genellikle bu sembolleri gördüklerinde, isteğin gerçekten yetkili bir kaynaktan gelip gelmediğini sorgulamadan otomatik olarak uyum gösterme eğiliminde olmaktadırlar.

2.2.3 Bireysel ve Kurumsal Otorite Figürleri

Sosyal mühendislik saldırılarında hedef kişilerin güven ve itaat eğilimlerini istismar etmek için kullanılan önemli araçlar olan otorite figürleri, genel olarak bireysel ve kurumsal olmak üzere iki ana kategoride incelenebilir.

Bireysel otorite figürleri, genellikle hedef kişinin doğrudan üstü, üst düzey yönetici veya BT personeli gibi kurum içindeki belirli bir kişiyi taklit etmeyi içerir. Bu tür saldırılar, hedefin belirli bir kişiye olan güven ve saygısını istismar eder ve genellikle aciliyet hissi yaratarak veya kişisel bir bağlantı kurarak etkinliklerini artırır (Krombholz vd., 2015). Bireysel otorite figürlerinin başarısı, büyük ölçüde hedefin bu figürlerle olan kişisel ilişkisine ve onlara gösterdiği saygı düzeyine bağlıdır. Özellikle hedefin profesyonel gelişimi veya performans değerlendirmesi gibi önemli faktörler üzerinde kontrolü olan doğrudan ilişkili otorite figürleri büyük bir güce sahiptir (Eftimie vd., 2022). Bu durumlarda, hedef kişi, talimatları yerine getirmemenin olası olumsuz sonuçlarından kaçınmak için otorite figürünün talimatlarını izleme eğilimindedir (Wang vd., 2021).

Kurumsal otorite figürleri ise bir organizasyonu veya bilinen bir kurumu temsil etme şeklinde ortaya çıkar. Bu saldırılar, kurum tarafından halihazırda oluşturulmuş itibar ve güvenilirliği kullanır ve genellikle otoriter görünen iletişimlerden faydalanır. Kurumsal otoritenin gücü, özellikle iyi bilinen ve tanınan kuruluşları içerdiğinde güçlü bir ikna aracıdır, çünkü insanlar genellikle bu tür kuruluşlar tarafından verilen taleplere güvenme ve uyma eğilimindedir

(Bose ve Leung, 2007). Kurumsal otorite figürlerinin sosyal mühendislik saldırılarındaki etkinliği, büyük ölçüde kurumun algılanan meşruiyetine ve güvenilirliğine bağlıdır. Kurumsal otorite figürleri, özellikle hedef kişi kurum için çalıştığında veya kurumla yakından ilişkili olduğunda etkilidir (Bullée vd., 2018). Bu durumlarda, hedef kişi, uymaması durumunda kurumsal yaptırımlardan kaçınmak için kurumsal otorite figürünün talimatlarına uyma eğilimindedir (Wang vd., 2021).

Sosyal mühendislik saldırılarında bireysel ve kurumsal otorite figürlerinin etkisini artıran önemli bir faktör, bu figürlerin kullandığı dil ve iletişim tarzıdır. Otorite figürleri genellikle resmi bir dil kullanır ve aciliyet hissi yaratır. Örneğin, "derhal harekete geçmeniz gerekiyor", "bu talimatları izlememeniz durumunda hesabınız askıya alınacaktır" veya "bu bir güvenlik denetimidir" gibi ifadeler, hedef kişinin kritik düşünme süreçlerini bypass etmesine ve otomatik olarak talimatlara uymasına neden olabilir (Longtchi vd., 2024). Bu tür dil kullanımı, özellikle belirsizlikten kaçınma düzeyi yüksek olan kültürlerde etkili olabilir, çünkü bu kültürlerde bireyler belirsizlik ve muğlaklıktan rahatsız olur ve bu nedenle net yönergeler ve talimatlar arar (Krombholz vd., 2015). Öte yandan, bilgi güvenliği konusunda eğitim almış kişiler, otorite figürlerinin taleplerini sorgulamaya ve doğrulamaya yatkın olabilir. Bununla birlikte, yüksek güç mesafesine sahip kültürlerde, bilgi güvenliği eğitimi almış olsa bile, bireyler otorite figürlerinin taleplerine uymaya devam edebilir (Rocha Flores vd., 2015). Bu çerçevede, kültürel bağlamın sosyal mühendislik saldırılarında etkili olduğu söylenebilir.

2.3 KÜLTÜREL FAKTÖRLER VE SOSYAL MÜHENDİSLİK

2.3.1 Hofstede'nin Kültürel Boyutlar Teorisi

Kültür, toplumların davranış kalıplarını, değerlerini ve normlarını şekillendiren temel bir unsur olarak kabul edilmektedir. Hofstede (2001) kültürü, bir grubu veya insan kategorisini diğerinden ayıran zihnin kolektif programlaması olarak tanımlamıştır. Kültürel farklılıkların sistematik olarak

incelenmesi ve ölçülmesi amacıyla geliştirilen en kapsamlı çalışmalardan biri Geert Hofstede'nin kültürel boyutlar teorisidir. Teori, ilk olarak 1980 yılında Hofstede'nin IBM şirketinin farklı ülkelerdeki çalışanları üzerinde yaptığı araştırmaya dayanmaktadır (Tukur ve Adam, 2017). Başlangıçta dört boyuttan oluşan teori, daha sonraki çalışmalarla genişletilmiş ve boyutların sayısı altıya yükseltilmiştir (Choo, 2021).

Hofstede'nin kültürel boyutlar teorisinin boyutları şunlardır: Güç Mesafesi (Power Distance), Belirsizlikten Kaçınma (Uncertainty Avoidance), Bireycilik-Toplulukçuluk (Individualism-Collectivism), Erillik-Dişilik (Masculinity-Femininity), Uzun Vadeli-Kısa Vadeli Yönelim (Long-term versus Short-term Orientation) ve Hoşgörü-Kısıtlama (Indulgence-Restraint) (Darmawati vd., 2019).

Güç Mesafesi boyutu, bir toplumdaki bireylerin güç dağılımındaki eşitsizliği ne ölçüde kabul ettiğini ve beklediğini ifade etmektedir. Yüksek güç mesafesine sahip toplumlarda, hiyerarşik yapılar daha belirgindir ve otorite figürlerine itaat daha fazla vurgulanmaktadır (Choo, 2021). Bu toplumlarda, kurumsal ve örgütsel gücün eşitsiz dağılımı normal karşılanmakta ve güç sahiplerinin kararlarının sorgulanmadan kabul edilmesi beklenmektedir (Lustig ve Koester, 2010). Düşük güç mesafesine sahip toplumlarda ise, eşitlik ideali daha ön plandadır ve sosyal sınıflar arasındaki geçiş daha kolaydır (Abzari ve Safari, 2011; Tukur ve Adam, 2017).

Belirsizlikten Kaçınma boyutu, bir toplumun belirsiz durumlara karşı toleransını ve bu durumlarla başa çıkma biçimini ifade etmektedir. Yüksek belirsizlikten kaçınma eğilimi gösteren toplumlarda, kurallar ve prosedürler daha fazla önemsenmekte ve risk almaktan kaçınılmaktadır (Tukur ve Adam, 2017). Bu toplumlarda, bireyler belirsizlik ve muğlaklık karşısında tehdit altında hissetmekte ve bu durumlardan kaçınmak için daha yapılandırılmış sistemler oluşturmaya çalışmaktadırlar. Düşük belirsizlikten kaçınma eğilimi gösteren toplumlarda ise, bireyler değişime daha açıktır ve belirsizlikle daha kolay başa çıkabilmektedirler (Lustig ve Koester, 2010; Darmawati vd., 2019).

Bireycilik-Toplulukçuluk boyutu, bir toplumun bireylerin kendi çıkarlarını mı yoksa grup çıkarlarını mı önceleğini ifade etmektedir. Bireyci toplumlarda, kişisel değerler ve hedefler davranışın temel belirleyicisidir ve bireysel özerklik önem taşımaktadır (Abzari ve Safari, 2011; Tukur ve Adam, 2017). Toplulukçu toplumlarda ise, grup değerleri ve hedefleri ön plandadır ve bireyler kendilerini öncelikle bir grubun üyesi olarak tanımlamaktadırlar (Darmawati vd., 2019).

Erillik-Dişilik boyutu, bir toplumun cinsiyet rollerini nasıl tanımladığını ve bu rollere ne kadar önem verdiğini ifade etmektedir. Eril kültürler genellikle hırs, bireycilik, kararlılık ve maddi başarı ile ilişkilendirilirken; dişil kültürler daha çok başkalarına karşı duyarlılık, bakım ve yaşam kalitesini önemseme ile karakterize edilmektedir (Lustig ve Koester, 2010; Darmawati vd., 2019).

Uzun Vadeli-Kısa Vadeli Yönelim boyutu, bir toplumun zaman perspektifini ve yaşam ile iş konusundaki referans noktasını ifade etmektedir. Uzun vadeli yönelime sahip kültürler, azim, tutumluluk ve alçakgönüllülük gibi değerleri teşvik ederken; kısa vadeli yönelime sahip kültürler, eylemlerin ardından hızlı sonuçlar beklemektedirler (Lustig ve Koester, 2010; Darmawati vd., 2019).

Hoşgörü-Kısıtlama boyutu, toplumun hayattan zevk alma ve doğal insan dürtülerinin tatmini konusundaki yaklaşımını ifade etmektedir. Hoşgörülü toplumlarda yaşamdan keyif alma ve özgürlük değerleri ön plandayken; kısıtlayıcı toplumlarda sosyal normlar ve kurallar aracılığıyla dürtülerin kontrolü öne çıkmaktadır (Darmawati vd., 2019).

2.3.2 Güç Mesafesi ve Otoriteye İtaat İlişkisi

Güç mesafesi, bir toplumun kurumlarında ve organizasyonlarında gücün eşit olmayan bir şekilde dağılımının ne ölçüde kabul edildiğini ve beklendiğini ifade eden kültürel bir boyuttur. Güç mesafesi kavramı, toplumsal hiyerarşilerin yapılandırılma biçimini ve bireylerin otorite figürlerine karşı tutumlarını şekillendirmektedir. Güç mesafesinin yüksek olduğu toplumlarda, otoriteye itaat etme eğilimi daha belirgin olarak gözlemlenmektedir (Hofstede, 2001).

Otoriteye itaat mekanizmasının bilişsel ve psikolojik temelleri incelendiğinde, bireylerin otorite figürlerine karşı geliştirdikleri tutumların; meşruiyet algısı, uzmanlık varsayımı ve sorumluluğun dışsallaştırılması olmak üzere üç temel unsurdan etkilendiği görülmektedir (Tyler, 2006). Meşruiyet algısı, otorite figürünün talimat verme hakkına sahip olduğuna dair inanç; uzmanlık varsayımı, otorite figürünün üstün bilgiye sahip olduğu düşüncesi; sorumluluğun dışsallaştırılması ise, bireyin kendi eylemlerinden doğan sonuçların sorumluluğunu otorite figürüne atfetme eğilimini ifade etmektedir. Söz konusu unsurlar, özellikle güç mesafesi yüksek kültürlerde, bireylerin otoriteye itaat etme davranışını güçlendirmektedir.

Güç mesafesi ile otoriteye itaat arasındaki ilişki, kültürlerarası araştırmalarla desteklenmektedir. Smith ve Bond (1998) tarafından yürütülen çalışmada, güç mesafesi yüksek olan toplumlarda, bireylerin otorite figürlerinin talimatlarını sorgulamadan kabul etme olasılığının daha yüksek olduğu tespit edilmiştir. Benzer şekilde, Brewer ve Venaik (2011) güç mesafesinin yüksek olduğu toplumlarda, hiyerarşik ilişkilerin daha belirgin olduğunu ve alt kademelerde bulunanların üstlerine karşı daha itaatkâr davrandıklarını ortaya koymuştur. Bilgi güvenliği perspektifinden değerlendirildiğinde, yüksek güç mesafesine sahip kültürlerde, otorite figürü olarak algılanan kişilerden gelen taleplerin sorgulanmadan yerine getirilmesi eğilimi, saldırganların otorite figürlerini taklit ederek hassas bilgilere erişim sağlamasını kolaylaştırmaktadır (Workman, 2008).

2.3.3 Türkiye ve Katar'ın Kültürel Boyutlar Açısından Karşılaştırılması

Hofstede Insights tarafından yayınlanan ve 2023 yılında güncellenen "Country Comparison Tool" veri tabanından alınan Türkiye ve Katar'ın kültürel boyutlarına ait değerler Tablo 2.1’de sunulmuştur (Hofstede Insights, 2023).

Tablo 2.1 Türkiye ve Katar'ın Karşılaştırmalı Değerleri

Kültürel Boyutlar	Türkiye	Katar
Güç Mesafesi	66	93
Bireycilik - Toplulukçuluk	46	18
Erillik - Dişillik	45	55
Belirsizlikten Kaçınma	85	80
Uzun Vadeli - Kısa Vadeli Oryantasyon	35	14
Hoşgörü - Kısıtlama	49	34

Türkiye ve Katar arasındaki en belirgin kültürel farklılık güç mesafesi boyutunda gözlemlenmektedir. Türkiye orta-yüksek düzeyde bir güç mesafesi değerine (66) sahipken, Katar çok yüksek bir güç mesafesi değerine (93) sahiptir. Bu önemli fark, iki ülkedeki bireylerin otorite figürlerine karşı tutumlarını ve dolayısıyla otorite temelli sosyal mühendislik saldırılarının etkinliğini doğrudan etkilemektedir. Yüksek güç mesafesi değerine sahip toplumlarda, hiyerarşik yapılar daha belirgindir ve otorite figürlerine saygı daha önemlidir. Bu tür kültürlerde yaşayan bireylerin otorite figürlerinin taleplerine sorgulamadan uyma eğiliminde olmaları, onları otorite temelli sosyal mühendislik saldırılarına karşı daha savunmasız hale getirebilir (Krombholz vd., 2015).

Bireycilik-toplulukçuluk boyutunda da önemli bir farklılık bulunmaktadır. Katar (18), Türkiye'ye (46) göre çok daha toplulukçu bir yapıya sahiptir. Bu durum, Katar'daki yüksek güç mesafesinin toplulukçu değerlerle birleşerek, otorite figürlerinin grup normları üzerindeki etkisini güçlendirdiğini düşündürmektedir. Toplulukçu kültürlerde, bireyler meslektaşlarının ve akranlarının görüşlerine önem verirken, bireyci kültürlerde, bireyler akranlarının görüşlerine daha az önem verebilir ve eylemleri konusunda daha iyimser

olabilirler (Rocha Flores vd., 2015). Bu bağlamda, Katar'daki toplulukçu yapı, grup uyumuna ve otoriteye uyma eğilimini artırarak, sosyal mühendislik saldırılarına karşı daha fazla zafiyet oluşturabilir.

Uzun vadeli-kısa vadeli oryantasyon boyutunda da belirgin bir fark görülmektedir. Katar'ın (14), Türkiye'ye (35) göre daha geleneksel ve kısa vadeli bir düşünce yapısına sahip olması, Katar'da geleneksel değerlere ve otoriteye bağlılığın daha güçlü olabileceğini, Türkiye'nin ise nispeten daha pragmatik bir yaklaşım benimsediğini göstermektedir. Kısa vadeli oryantasyona sahip toplumlar, geleneklere saygı gösterme, sosyal yükümlülükleri yerine getirme ve otoriteye itaat etme eğilimindedir (Yasin vd., 2019). Bu nedenle, Katar'daki kısa vadeli oryantasyon, kurumsal otorite figürlerine daha fazla saygı duyulmasını ve bu figürlerin taleplerine uyulmasını teşvik edebilir.

Belirsizlikten kaçınma boyutunda her iki ülke de yüksek değerlere sahip olması (Türkiye: 85, Katar: 80), her iki toplumda da belirsizliği azaltmak için resmi kuralların ve yapıların ihtiyacının yüksek olduğunu göstermektedir. Yüksek belirsizlikten kaçınma değerine sahip kültürlerde, bireyler belirsizlik ve muğlaklık karşısında rahatsızlık duyarlar ve bu nedenle net yönergeler ve talimatlar ararlar. Yüksek düzeyde belirsizlikten kaçınma, otorite figürleri tarafından verilen talimatlara uyma eğilimini artırabilir ve sosyal mühendislik saldırılarının başarı şansını yükseltebilir (Krombholz vd., 2015). Ülkeler arasında belirsizlikten kaçınma boyutunda gözlemlenen benzerlik, otorite temelli sosyal mühendislik saldırılarında kullanılan "kurallara uyma" ve "prosedürleri takip etme" gibi taktiklerin her iki kültürde de etkili olabileceğini düşündürmektedir.

Erillik-dişillik boyutunda, Katar (55) Türkiye'ye (45) göre daha eril bir kültüre sahiptir. Eril kültürlerde rekabet, başarı ve güç daha ön plandayken, dişil kültürlerde işbirliği, mütevazılık ve yaşam kalitesi daha önemlidir. Katar'ın daha eril yapısı, hiyerarşik ilişkilere ve güç odaklı otorite figürlerine daha fazla önem verilmesine yol açarak, kurumsal otorite figürlerinin sosyal mühendislik saldırılarında daha etkili olmasını sağlayabilir.

Hoşgörü-kısıtlama boyutunda, Türkiye (49) Katar'a (34) göre daha hoşgörülü bir toplum yapısına sahiptir. Kısıtlayıcı toplumlar, sosyal normların ve kuralların daha katı bir şekilde uygulandığı kültürlerdir. Katar'ın daha kısıtlayıcı yapısı, kurumsal otoritelerin ve resmi kuralların daha fazla benimsendiği bir ortam oluşturarak, kurumsal otorite figürlerinin sosyal mühendislik saldırılarında daha etkili olmasına katkıda bulunabilir.

Türkiye ve Katar arasındaki kültürel farklılıklar, otorite temelli sosyal mühendislik saldırılarının etkinliğini önemli ölçüde etkileyebilir. Özellikle güç mesafesi boyutundaki belirgin fark, otorite figürlerinin algılanma biçimini ve bu figürlere itaat etme eğilimini şekillendirebilir. Türkiye'nin orta-yüksek güç mesafesi ve nispeten düşük kurumsal güven düzeyi, bireysel ilişkilere ve kişisel bağlantılara daha fazla önem verilmesine yol açabilir. Bu nedenle, Türkiye'de bireysel otorite figürlerine dayalı sosyal mühendislik saldırıları daha etkili olabilir. Katar'da ise yüksek güç mesafesi ve güçlü kurumsal güven, kurumsal otorite figürlerine dayalı saldırıların daha başarılı olmasını sağlayabilir.

2.4 İLGİLİ ÇALIŞMALAR

Burrell (2024), üniversite ortamında balina avcılığı (whaling) ve hedefli oltalama (spear phishing) saldırılarının etkinliğini incelediği çalışmasında, siber psikoloji ve suç psikolojisi perspektiflerini birleştirerek bu saldırıların başarısının altında yatan faktörleri araştırmıştır. XXO Üniversitesi'nde gerçekleşen ve üst düzey yöneticileri taklit eden e-postaların gönderildiği bir vaka üzerinden yapılan kök neden analizi (RCA), bu tür saldırıların teknik karmaşıklıktan ziyade psikolojik manipülasyona dayandığını ortaya koymuştur. Çalışma, özellikle hiyerarşik yapılarda otorite yanlılığının ve kurumsal güven manipülasyonunun etkisini öne çıkarmaktadır. Araştırma sonuçları, üniversite gibi hiyerarşik yapıların olduğu kurumlarda çalışanların otoriteye itaat etme eğiliminin, bu tür saldırılara karşı önemli bir zafiyet oluşturduğunu göstermektedir. Burrell, geleneksel siber güvenlik önlemlerinin teknik savunmalara odaklandığını, ancak psikolojik savunmasızlıkları ele almada

yetersiz kaldığını öne sürerek, davranışsal içgörüleri entegre eden bir siber güvenlik çerçevesinin gerekliliğini savunmaktadır.

Xu vd. (2023), hedefli oltalama (spear phishing) saldırılarında kişisel bilgi kullanımının etkisini inceledikleri çalışmalarında, saldırganların hedef kişiler hakkında sahip oldukları bilgi miktarının, kullanıcı savunmasızlığı üzerindeki etkisini araştırmışlardır. Araştırmacılar, SpearSim adlı bir simülasyon ortamı geliştirerek laboratuvar ortamında kontrollü bir deney gerçekleştirmişlerdir. Deney tasarımında katılımcılar, saldırgan ve son kullanıcı rollerini üstlenmiş; saldırganlar, hedefleri hakkında düşük veya yüksek miktarda bilgiye sahip olacak şekilde iki gruba ayrılmıştır. Çalışmanın sonuçları, hedef hakkında daha fazla kişisel bilgiye sahip olan saldırganların, bağlamsal olarak anlamlı kimlik taklidi ve anlatılar içeren daha ikna edici saldırılar oluşturabildiklerini göstermiştir. Yüksek bilgi kullanılabilirliği koşulundaki son kullanıcıların, düşük bilgi kullanılabilirliği koşulundakilere kıyasla hedefli oltalama saldırılarına 2,97 kat daha fazla savunmasız oldukları tespit edilmiştir. Ayrıca, iş arkadaşı veya arkadaş kimliğini taklit eden saldırıların, ticari marka taklidi yapan saldırılara göre çok daha etkili olduğu bulunmuştur.

Rizzoni vd. (2022), büyük bir İtalyan hastanesinde gerçekleştirdikleri oltalama simülasyon çalışmasında, genel ve kişiselleştirilmiş oltalama e-postalarına karşı personelin tepkilerini karşılaştırmayı amaçlamışlardır. Yaklaşık 6000 sağlık çalışanının katıldığı bu vaka çalışmasında, üç farklı kampanya yaklaşık 4 aylık aralıklarla yürütülmüştür. Araştırma yöntemi olarak, personel rastgele iki gruba ayrılmış ve bir gruba genel oltalama e-postaları, diğer gruba ise hastane bağlamına özel hazırlanmış kişiselleştirilmiş e-postalar gönderilmiştir. Bulgular, kişiselleştirilmiş oltalama e-postalarının çok daha etkili olduğunu göstermiştir. İlk kampanyada, personelin %64'ü genel oltalama e-postasını açmazken, kişiselleştirilmiş e-postayı açmayanların oranı sadece %38 olmuştur. Ayrıca, kişiselleştirilmiş e-postalardaki bağlantılara tıklama oranı (%55), genel e-postalardakine (%7) göre anlamlı derecede daha yüksek bulunmuştur. Çalışmada, oltalama simülasyonlarının faydalı olduğu ancak etik sorunlar ve organizasyonel zorluklar içerdiği ifade edilmiştir. Araştırmacılar,

başarılı ve etik oltalama simülasyonlarının, organizasyon genelinde koordinasyon, doğru zamanlama ve personelin farkındalığının olmamasını gerektirdiğini belirtmişlerdir.

Eftimie vd. (2022), hedefli oltalama (spear phishing) saldırılarına karşı kişilik özelliklerinin etkisini inceledikleri çalışmalarında, Büyük Beşli kişilik modelinin (Big Five) oltalama saldırılarına karşı savunmasızlıkla ilişkisini araştırmışlardır. Araştırmacılar, bir yazılım geliştirme şirketinde çalışan 235 katılımcı üzerinde dört hafta boyunca dört farklı hedefli oltalama kampanyası gerçekleştirmişlerdir. Katılımcılar önce Büyük Beşli kişilik testine tabi tutulmuş, ardından belirli kişilik özelliklerini hedef alan oltalama e-postaları almışlardır. İkili lojistik regresyon analizleri sonucunda, düşük açıklık ve sorumluluk ile yüksek dışadönüklük, uyumluluk ve nevrotiklik özelliklerine sahip bireylerin oltalama saldırılarına karşı daha savunmasız oldukları tespit edilmiştir. Özellikle, e-posta açma aşamasında nevrotiklik; bağlantıya tıklama ve hassas veri gönderme aşamalarında ise dışadönüklük, uyumluluk ve nevrotiklik özellikleri istatistiksel olarak anlamlı bulunmuştur. Çalışma ayrıca, siber güvenlik eğitiminin oltalama saldırılarına karşı genel farkındalığı artırdığını, ancak bazı kişilik özelliklerine sahip bireylerin (düşük açıklık, düşük sorumluluk ve yüksek nevrotiklik) eğitim sonrasında da riskli davranışlar sergilemeye devam ettiklerini göstermiştir.

Bayl-Smith vd. (2022), oltalama saldırılarına karşı çalışan tepkilerini ve koruyucu motivasyon faktörlerini inceledikleri çalışmalarında, farklı ikna stratejilerinin etkinliğini bir finans kurumunda gerçekleştirdikleri simüle edilmiş saha deneyi ile araştırmışlardır. Araştırmacılar, PhishMe aracılığıyla çalışanlara beş farklı ikna stratejisi (otorite, sosyal kanıt, kıtlık ve bunların kombinasyonları) kullanan e-postalar göndermişler ve ardından katılımcıların tıklama ve raporlama davranışlarıyla ilişkili koruyucu faktörleri belirlemek için çevrimiçi bir anket uygulamışlardır. Çalışmada, algılanan tehdit şiddeti, tehdit duyarlılığı, yanıt etkinliği ve kişisel yeterlilik değişkenleri incelenmiştir. Bulgular, farklı ikna stratejileri arasında yanıt davranışlarının önemli ölçüde değiştiğini göstermiştir. Tehdit duyarlılığı algısının, tıklama davranışının ötesinde

raporlama davranışı olasılığını artırdığı tespit edilmiştir. Ayrıca, tehdit duyarlılığı ve kurumsal yanıt etkinliği algısı, simüle edilmiş oltalama e-postasına yanıt vermeme olasılığıyla ilişkilendirilmiştir. Çalışma, otorite temelli e-postaların en yüksek raporlama oranına sahip olduğunu ve sosyal kanıt + kıtlık stratejisinin en yüksek tıklama oranını elde ettiğini ortaya koymuştur.

Abroshan vd. (2021), oltalama saldırılarının başarısında insan davranışlarının ve demografik faktörlerin etkisini inceledikleri çalışmalarında, oltalama sürecinin her aşamasında (e-postayı açma, bağlantıya tıklama ve hassas bilgileri girme) kullanıcı davranışlarını etkileyen faktörleri araştırmışlardır. Araştırmacılar, katılımcıların risk alma davranışlarını ölçmek için Balon Analog Risk Testi (BART), alan-spesifik risk alma davranışlarını ölçmek için DOSPERT ölçeği ve karar verme stillerini belirlemek için Genel Karar Verme Stili (GDMS) ölçeğini kullanmışlardır. Ardından, 135 katılımcı üzerinde simüle edilmiş bir oltalama kampanyası yürüterek, kullanıcıların oltalamaya karşı savunmasızlıklarını değerlendirmişlerdir. Bulgular, risk alma davranışının ve cinsiyetin, oltalama sürecinin farklı aşamalarında kullanıcıların savunmasızlığını öngörebildiğini göstermiştir. Özellikle yüksek risk alma eğilimine sahip bireylerin oltalama saldırılarına karşı daha savunmasız oldukları tespit edilmiştir. Araştırma, oltalama sürecinin her aşamasında farklı davranışsal faktörlerin etkili olduğunu ve oltalama önleme çalışmalarının bu faktörleri göz önünde bulundurarak tasarlanması gerektiğini belirtmektedir.

Greitzer vd. (2021), oltalama saldırılarına karşı teknik ve insani faktörleri inceledikleri deneysel çalışmalarında, George Mason Üniversitesi'nde 6.938 akademik ve idari personeli hedef alan üç haftalık bir oltalama kampanyası yürütmüşlerdir. Araştırmacılar, üç farklı yaşam alanı bağlamında (BT yardım masası, paket teslimatı ve kredi kartı uyarısı) oltalama e-postaları göndererek, demografik faktörleri, çalışma istasyonu/ağ izleme verilerini ve kampanya öncesi ve sonrası anketlerle ölçülen çeşitli davranışsal ve psikolojik faktörleri incelemişlerdir. Bulgular, farklı e-posta bağlamlarına ve daha önce oltalama saldırılarına maruz kalıp kalmamaya bağlı olarak oltalama duyarlılığında önemli farklılıklar olduğunu göstermiştir. Daha önce oltalama saldırılarına maruz kalan

kişilerin, sonraki oltalama e-postalarına daha fazla yanıt verme eğiliminde oldukları tespit edilmiştir. Ayrıca, oltalama bağlantılarına tıklayan katılımcıların, tıklamayanlara göre dürtüsellik puanlarının daha yüksek olduğu bulunmuştur. Çalışma, bağlantıların meşruiyetini kontrol etmek gibi uygun çevrimiçi güvenlik alışkanlıklarına sahip katılımcıların, oltalama saldırılarına karşı daha az savunmasız olduklarını da ortaya koymuştur.

Tiwari (2020), oltalama e-postalarında otorite, aciliyet, risk algısı ve insan faktörlerinin kullanıcı duyarlılığına etkisini araştırdığı çalışmasında, kişilik özellikleri ile ikna prensiplerinin ilişkisini ve bu faktörlerin oltalama saldırılarına karşı savunmasızlık üzerindeki etkilerini incelemiştir. Amazon Mechanical Turk platformu üzerinden katılımcıların toplandığı araştırmada, kişilik özelliklerini ölçmek için Beş Faktör Kişilik Envanteri kullanılmış ve katılımcıların farklı otorite, aciliyet ve risk seviyelerini içeren oltalama e-postalarına karşı tepkileri değerlendirilmiştir. Bulgular, otorite temelli ikna prensiplerinin sorumluluk ve uyumluluk kişilik özellikleriyle, aciliyet temelli ikna prensiplerinin ise dışadönüklük ve açıklık kişilik özellikleriyle ilişkili olduğunu göstermiştir. Ayrıca, daha önce oltalama saldırılarına maruz kalmış kişilerin, otorite, aciliyet ve risk içeren e-postalara karşı daha savunmasız oldukları tespit edilmiştir. Çalışma, otorite ve aciliyet dili içeren e-postaların tıklanma olasılığının daha yüksek olduğunu, ancak daha yüksek risk içeren eylemleri gerektiren e-postaların tıklanma olasılığının daha düşük olduğunu ortaya koymuştur.

Lin vd. (2019), internet kullanıcılarının yaşı ve e-posta içeriğinin (etki silahları ve yaşam alanları) hedefli oltalama saldırılarına karşı duyarlılık üzerindeki etkilerini inceledikleri çalışmalarında, 100 genç ve 58 yaşlı internet kullanıcısına 21 gün boyunca bilgileri dışında günlük simüle edilmiş oltalama e-postaları göndermişlerdir. Araştırmacılar, katılımcıların duyarlılığının bir göstergesi olarak e-postalardaki bağlantılara tıklamalarını kaydeden bir tarayıcı eklentisi kullanmışlardır. Bulgular, katılımcıların %43'ünün simüle edilmiş oltalama e-postalarına düştüğünü ve yaşlı kadınların en yüksek duyarlılığı gösterdiğini ortaya koymuştur. Genç kullanıcıların duyarlılığı çalışma boyunca azalırken, yaşlı kullanıcıların duyarlılığı sabit kalmıştır. Saldırıların göreceli

etkinliği, etki silahları ve yaşam alanlarına göre farklılık göstermiş, özellikle kıtlık ve yasal içerikli e-postalar en yüksek duyarlılığa neden olurken, sosyal kanıt ve finansal içerikli e-postalar en düşük duyarlılığa neden olmuştur. Ayrıca, yaşlı kullanıcılar genç kullanıcılara kıyasla daha düşük duyarlılık farkındalığı bildirmişlerdir.

Rocha Flores vd. (2015), oltalama saldırılarına karşı direnci etkileyen kişisel psikolojik ve demografik faktörleri ve ulusal kültürün bu faktörler üzerindeki etkisini araştırdıkları çalışmalarında, İsveç, ABD ve Hindistan'daki dokuz farklı kuruluştan 2.099 çalışana anket uygulamış ve ardından aynı örnekleme duyurulmamış bir oltalama saldırısı gerçekleştirmişlerdir. Araştırmacılar, sosyal mühendisliğe direnç gösterme niyeti, genel bilgi güvenliği farkındalığı, bilgi sistemleri eğitimi ve bilgisayar deneyimi gibi faktörleri ölçmek için anket kullanmış, ardından katılımcıların oltalama e-postalarına verdikleri tepkileri doğrudan gözlemlemişlerdir. Bulgular, sosyal mühendisliğe direnç gösterme niyeti, genel bilgi güvenliği farkındalığı, resmi bilgi sistemleri eğitimi ve bilgisayar deneyiminin oltalama direnciyle pozitif anlamlı bir korelasyona sahip olduğunu göstermiştir. Ayrıca, çalışma oltalama belirleyicileri ile çalışanların gözlemlenen oltalama davranışı arasındaki korelasyonun İsveçli, ABD'li ve Hintli çalışanlar arasında 15 vakanın 6'sında farklılık gösterdiğini ortaya koymuştur. Çalışmada ulaşılan sonuçlar, kültürel farklılıkların oltalama saldırılarına karşı savunmasızlığı etkileyebileceğini göstermektedir.

BÖLÜM 3

3. YÖNTEM

Bu bölümde çalışmanın metodolojik yaklaşımı açıklanmaktadır. Simülasyon tabanlı çalışmaların aksine, bu araştırma gerçek dünya koşullarında bir saha deneyi kullanmış, oltalama e-postaları kontrollü koşullar altında doğrudan kurumsal ortamlardaki çalışanlara gönderilmiştir. Çalışmada, katılımcı davranışları; e-posta açma, okuma, bağlantıya tıklama, veri gönderme ve oltalama bildirimi şeklinde kayıt edilmiştir. Veriler ikili formda (0 = hayır, 1 = evet) takip edilmiş ve uygun istatistiksel yöntemlerle analiz edilmiştir.

3.1 ARAŞTIRMA SORULARI VE HİPOTEZLER

Önceki bölümlerde belirtilen kültürel ve davranışsal dayanaklar temelinde; çalışmada, gerçek dünya oltalama saldırılarında saldırı tekniği etkinliği, otorite tipi etkisi, kültürel etkileşimler ve davranışsal geçişleri ele alan dört temel hipotez formüle edilmiştir. Saldırının başarısını temsil eden temel bağımlı değişken DataSubmissionStatus'tür (Veri Gönderme Durumu). Çalışmada geliştirilen hipotezler aşağıda sunulmuştur:

Literatürde, hedefli oltalama (spear phishing) saldırılarının genel oltalama (generic phishing) saldırılarından daha etkili olduğu görülmektedir. Rizzoni vd. (2022), hedefli oltalama e-postalarının, genel e-postalara göre daha yüksek tıklama oranlarına sahip olduğunu bulmuşlardır. Benzer şekilde, Xu vd. (2023), hedef hakkında daha fazla kişisel bilgi içeren saldırıların başarı oranını önemli ölçüde artırdığını tespit etmişlerdir. Cialdini'nin ikna prensipleri doğrultusunda, hedefli oltalama saldırıları, otorite prensibi gibi psikolojik manipülasyon tekniklerini daha etkili bir şekilde kullanabilmektedir (Cialdini, 2009). Bullée vd. (2018), başarılı sosyal mühendislik saldırılarının diğer prensiplerden daha fazla otorite prensibini kullandığını bulmuşlardır. Milgram'ın klasik deneyi,

insanların otorite figürlerinin talimatlarına uyma eğiliminin, sosyal mühendislik saldırılarında istismar edilebilecek güçlü bir faktör olduğunu göstermiştir (Milgram, 1963). Bu bağlamda, çalışmada ilk hipotez şu şekilde oluşturulmuştur:

H1 – Saldırı Tekniği Temelli Hipotez

- $H1_0$: Genel oltalama ve hedefli oltalama teknikleri arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark yoktur.
- $H1_1$: Genel oltalama ve hedefli oltalama teknikleri arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark vardır.

H1 hipotezi, genel oltalama e-postaları (Kontrol Grubu) ile hedefli oltalama e-postaları (Deney Grupları A ve B) arasındaki etkinliği test etmektedir. Veri gönderen katılımcıların oranı, temel başarı metriği olarak kullanılmaktadır.

Otorite figürlerinin türü, sosyal mühendislik saldırılarının etkinliğini önemli ölçüde etkilemektedir. Hofstede'nin kültürel boyutlar teorisine göre, otorite figürlerine itaat etme eğilimi, yüksek güç mesafesine sahip kültürlerde daha belirgindir (Hofstede, 2015). Bireysel otorite figürlerinin etkinliği, hedefin bu figürlerle olan kişisel ilişkisine ve gösterdiği saygı düzeyine bağlıdır (Eftimie vd., 2022). Kurumsal otorite figürlerinin etkinliği ise, organizasyonun algılanan meşruiyetine ve güvenilirliğine bağlıdır (Bullée vd., 2018). Türkiye gibi kurumlara duyulan güven endeksinin düşük ve güç mesafesinin orta-yüksek olduğu kültürlerde, bireysel otorite figürlerine dayalı saldırıların daha etkili olabileceği öngörülmektedir. Katar gibi güç mesafesinin yüksek ve kurumlara duyulan güven endeksinin yüksek olduğu kültürlerde ise, kurumsal otorite figürlerine dayalı saldırıların daha başarılı olması beklenmektedir. Bu bağlamda, çalışmanın ikinci hipotezi şu şekilde oluşturulmuştur:

H2 – Ülke İçinde Otorite Tipine Göre Karşılaştırma

- $H2_0$: Tüm katılımcı verileri birleştirildiğinde, bireysel ve kurumsal otorite temelli hedefli oltalama saldırıları arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark yoktur.

- $H2_1$: Türkiye'de, bireysel otorite figürlerini kullanan hedefli oltalama saldırıları, kurumsal otorite figürlerini kullananlardan daha başarılıdır.
- $H2_2$: Katar'da, kurumsal otorite figürlerini kullanan hedefli oltalama saldırıları, bireysel otorite figürlerini kullananlardan daha başarılıdır.

H2 hipotezi, Hofstede'nin Güç Mesafesi İndeksi ve kurumlara duyulan güven endeksi üzerine önceki araştırmalara dayanmaktadır. Türkiye gibi kurumlara duyulan güvenin düşük ve güç mesafesinin orta-yüksek olduğu ülkelerde, kişiselleştirilmiş otorite figürleri daha büyük bir uyum sağlayabilir. Buna karşılık, Katar gibi kurumlara duyulan güvenin daha güçlü olduğu ülkelerde, kurumsal otorite figürlerini kullanan saldırılar daha güvenilir görünebilir ve dolayısıyla daha etkili olabilir.

Kültürel faktörlerin ve otorite tipinin etkileşimi, sosyal mühendislik saldırılarının başarısını önemli ölçüde etkileyebilir. Kültürel değerler ve normlar, bireylerin farklı otorite tiplerine (bireysel veya kurumsal) tepkilerini şekillendirebilir. Yasin vd. (2019), otorite figürlerine karşı tutumların farklı kültürel bağlamlarda değiştiğini ve bu değişkenliğin sosyal mühendislik saldırılarının başarısını etkilediğini bulmuşlardır. Hofstede'nin kültürel boyutlar teorisinde tanımlanan güç mesafesi ve bireycilik-kolektivizm boyutları, bu etkileşimi açıklamada önemli bir rol oynamaktadır. Yüksek güç mesafesine sahip kolektivist kültürlerde, insanlar kurumsal otoritelere daha fazla güvenirken, daha bireyci ve orta düzeyde güç mesafesine sahip kültürlerde, insanlar kişisel ilişkilere dayalı bireysel otorite figürlerine daha fazla güvenmektedirler. Türkiye ve Katar'ın kültürel özelliklerini göz önünde bulundurarak, bu iki ülkedeki bireylerin farklı otorite tiplerine verdikleri tepkilerde önemli farklılıklar olacağı öngörülmektedir. Bu bağlamda, çalışmanın üçüncü hipotezi şu şekilde oluşturulmuştur:

H3 – Ülke ve Otorite Tipi Arasındaki Etkileşim

- $H3_0$: Saldırı başarısı açısından ülke ve otorite türü arasında istatistiksel olarak anlamlı bir etkileşim yoktur.
- $H3_1$: Saldırı başarısı açısından ülke ve otorite türü arasında istatistiksel olarak anlamlı bir etkileşim vardır.

H3 hipotezi, hedefli oltalama saldırılarında bireysel ve kurumsal otorite figürlerinin etkinliğinin kültürel bağlamlara göre değişip değişmediğini incelemektedir. Otorite tiplerinin göreceli başarısının Türkiye ve Katar arasında farklılık gösterip göstermediğini, potansiyel olarak güç mesafesi ve güven algıları gibi faktörlerden etkilenip etkilenmediğini araştırmaktadır. Bu etkileşimlerin belirlenmesi, sosyal mühendislik güvenlik açıklarında kültüre özgü dinamikleri ortaya çıkaracak ve daha hedefli güvenlik farkındalığı stratejilerinin geliştirilmesine ışık tutacaktır.

Oltalama saldırılarında kullanıcı davranışı genellikle aşamalı bir şekilde ilerler ve her bir aşamadaki eylem, bir sonraki eylemi doğrudan etkiler. Bu davranışsal süreklilik, Cialdini'nin tutarlılık prensibi (2009) ile uyumludur. Bu prensip, bireylerin bir kez başlatıldığında taahhütlerini sürdürme olasılıklarının daha yüksek olduğunu öne sürer. Örneğin, bir oltalama bağlantısına tıklamak, kullanıcının başlangıçtaki duyarlılığını gösterir ve kullanıcılar bilişsel uyumsuzluğu azaltmak için eylemlerini rasyonelleştirebileceğinden, daha fazla tehlikeye girme olasılığını artırır. Bu çerçeveye dayanarak, çalışmanın dördüncü hipotezi şu şekilde oluşturulmuştur:

H4 – Davranışsal Geçiş İlişkisi Hipotezi

- $H4_0$: Oltalama bağlantısına tıklama ile veri gönderme davranışı arasında istatistiksel olarak anlamlı bir ilişki yoktur.
- $H4_1$: Oltalama bağlantısına tıklayan çalışanlar, tıklamayanlara göre veri gönderme olasılığı önemli ölçüde daha yüksektir.

H4 hipotezi, bir oltalama saldırısı sırasında kullanıcı davranışının sıralı doğasını, özellikle bir eyleme (bağlantıya tıklama gibi) katılmanın bir sonraki, daha kritik adıma (hassas veri gönderme) ilerleme olasılığını önemli ölçüde artırıp artırmadığını incelemektedir. İlk etkileşimden tam uyuma kadar öngörülebilir bir davranış kalıbının var olup olmadığını ortaya çıkarmayı amaçlamakta ve bu da saldırı zincirinin önemli bir güvenlik ihlali ile sonuçlanmadan önce nerede kesilebileceğine dair değerli bilgiler sunmaktadır. Bu ilişkinin doğrulanması, organizasyonların davranışsal sürekliliği, güvenlik

ihlali ile sonuçlanmadan önce kıran hedefli müdahaleler uygulamasını sağlayabilir.

3.2 ÇALIŞMA TASARIMI

Bu bölümde, gerçek dünya genel ve hedefli oltalama deneylerinin yürütülmesine ilişkin süreç adım adım özetlenmektedir. Çalışma tasarımı, yapay simülasyonlar yerine kontrollü bir saha ortamı kullanarak farklı otorite figürü manipülasyonları ve kültürel bağlamlarda davranışsal tepkileri test etmektedir. Her alt bölümde katılımcı seçiminden saldırı uygulamasına ve veri analizi prosedürlerine kadar deneysel sürecin belirli bir aşaması detaylandırılmaktadır.

3.2.1 Çalışma Grubu

Araştırma için katılımcılar, İstanbul, Türkiye'deki devlet düzenlemesine tabi bir elektrik dağıtım şirketi ve Katar'ın ulusal enerji çerçevesine bağlı devlet mülkiyetindeki bir elektrik ve su hizmetleri işletmesinden seçilmiştir. Her iki kurum da dahili güvenlik protokolleri ve düzenleyici hususlar nedeniyle kamuya açık materyallerde anonimlik talep etmesine rağmen, katılım için resmi yazılı onay verilmiştir. Bu onay, oltalama çalışmaları için teknik yapılandırma izinlerini ve Beam Security adlı bir siber güvenlik çözümleri sağlayıcısının koordinasyonu ve gözetimi altında her kurumun iç etik ve yasal uyum kurullarından alınan onayları içermektedir. Etik uyum, Beam Security'nin Phishing platformundaki yönetişim çerçevesi aracılığıyla sağlanmıştır. Bu çerçeve ISO/IEC 29100 Gizlilik Çerçevesi ve Türkiye'deki KVKK (Türk Kişisel Verilerin Korunması Kanunu - KVKK) ile Katar'daki QCB uyumluluk gereklilikleri dahil olmak üzere geçerli ulusal veri koruma yasalarıyla tam uyum içinde bulunmaktadır.

Nihai örneklem, ülke başına 450 olmak üzere, üç deneysel koşula eşit olarak dağıtılmış toplam 900 katılımcıdan oluşmuştur: genel oltalama e-postaları alan bir kontrol grubu ile bireysel veya kurumsal otorite manipülasyonu içeren hedefli oltalama e-postaları alan iki deney grubu. Katılımcı rolleri ve cinsiyet

dağılımı, tipik işgücü demografisiyle tutarlı tutulmuş ve davranışsal analiz sırasında bağlamsal faktörler olarak hizmet etmiştir. Katılımcıların deneysel koşullar arasındaki ayrıntılı dağılımı Tablo 3.1'de özetlenmiştir.

Tablo 3.1 Katılımcıların Dağılımı

Ülke	Grup	Katılımcı	Toplam
Türkiye	Kontrol Grubu	150	450
	Deney Grubu A (Bireysel Otorite)	150	
	Deney Grubu B (Kurumsal Otorite)	150	
Katar	Kontrol Grubu	150	450
	Deney Grubu A (Bireysel Otorite)	150	
	Deney Grubu B (Kurumsal Otorite)	150	

3.2.2 Hazırlık Aşaması

3.2.2.1 Etik Onaylar ve Kurumsal İşbirliği

Deneysel çalışma, bir siber güvenlik çözümleri sağlayıcısı olan Beam Security aracılığıyla koordine edilmiştir. Beam Security, resmi anlaşmaları, etik onayları, bilgilendirilmiş onam süreçlerini ve hedef kuruluşlarla teknik koordinasyonu kolaylaştırmıştır. Otorite figürü olarak kullanılacak denetleyici, düzenleyici ve regülatör kurumların her ikisi de araştırma amaçları doğrultusunda kurumsal isimlerinin, logolarının, departman başlıklarının kullanılmasına izin vermiştir.

Türkiye ve Katar'da faaliyet gösteren, bu çalışmanın oltalama saldırıları için hedef kitlesini oluşturan elektrik dağıtım şirketleri, Beam Security firmasıyla yapılan protokol kapsamında; kurumsal isimlerinin, logolarının ve

departman başlıklarının doğrudan kullanılmasına izin vermemiş, yalnızca kurumsal kimliklerinin açıkça anlaşılmayacak şekilde anonimleştirilerek kullanılmasını onaylamıştır. Ayrıca aynı protokol çerçevesinde, her iki ülkedeki şirketlerin bilgi güvenliği birimleri; yanıltıcı alan adları üzerinden gönderilecek oltalama e-postalarının standart güvenlik filtrelerini aşarak doğrudan katılımcıların gelen kutularına ulaşabilmesini sağlamak amacıyla, e-posta ağ geçitlerini alan adı tabanlı istisnalar ve gönderici bazlı beyaz listelerle yapılandırmıştır. Bu sayede, kontrol ve deney gruplarına gönderilen oltalama e-postalarının alıcıların gelen kutularına başarıyla ulaştığından emin olunmuştur.

3.2.2.2 Senaryo Geliştirme Adaptasyonu

Araştırmacı tarafından oltalama senaryoları, her ülkenin dili, kültürel bağlamı ve organizasyonel iletişim tarzına göre dikkatle tasarlanmıştır. Türkiye için Türkçe dilinde, Katar için İngilizce dilinde e-posta senaryoları geliştirilmiştir. Senaryolar, parola kullanımı sona erme bildirimleri ve düzenleyici uyum denetimleri dahil olmak üzere tipik organizasyonel iletişim temalarını yansıtmıştır.

- **Kontrol Grubu (Genel Oltalama)**: Genel oltalama senaryolarında, katılımcı kuruluşların otantik kurumsal alan adlarına çok benzeyen typosquatting (yazım hatası içeren) alan adları kullanılmıştır. E-postalar, iç BT departmanlarından geliyormuş gibi görünen Microsoft parola kullanımı süresi sona erme bildirimleri şeklinde tasarlanmış ve alıcıların gömülü bağlantılar aracılığıyla parolalarını yenilemeleri istenmiştir.
- **Deney Grupları (Hedefli Oltalama)**: Hedefli oltalama senaryoları özellikle düzenleyici otoriteyi kullanmıştır. E-postalarda katılımcılara 2024 faaliyet raporlarının ISO 27001 BGYS standartlarına uygun olduğu, ancak faaliyetleri sırasında yapay zeka araçlarının kullanılması durumunda ISO 42001 standardı kapsamında ek uygunluk doğrulaması gerektiği bildirilmiştir. Bu iletişimler, aciliyet ve otantiklik yaratmak amacıyla katı bir uyumluluk son tarihi (14.03.2025) ve uyumsuzluk durumunda cezai yaptırımla karşılacağı uyarıları içermiştir.

Araştırmacı, kimlik avı e-postalarının güvenilirliğini artırmak için LinkedIn gibi sosyal medya kaynaklarından doğrulanan, kamuya açık organizasyon şemaları ve rol unvanlarına dayalı bireysel ve kurumsal otorite figürleri seçmiştir. Çalışma aşamasında gerçek kurumsal ve kişisel tanımlayıcıların kullanımı, yasal ve etik uyumluluğu sağlamak için resmi anlaşmalar aracılığıyla yetkilendirilmiştir.

- **Bireysel Otorite E-postaları**:
  - Türkiye: mahmutmahmut@epdkqov.tr adresinden gönderilmiştir. (Türkiye'nin EPDK'sını taklit etmektedir).
  - Katar: mahmutmahmut@gatarenergy.qa adresinden gönderilmiştir. (QatarEnergy'yi taklit etmektedir).
- **Kurumsal Otorite E-postaları**:
  - Türkiye: denetim@epdkqov.tr adresinden gönderilmiştir.
  - Katar: audit@gatarenergy.qa adresinden gönderilmiştir.

Araştırmanın etik protokolleri kapsamında, deney gruplarına yönelik hedefli oltalama senaryosunda ilgili ülkenin denetleyici, düzenleyici ve regülatör kurumunun araştırma kapsamında kurumsal isimleri, logoları ve departmen başlıklarının kullanımına izin verilmiştir. Ancak, ilgili regülatör kurumlarında çalışan ve bireysel otorite figürlerini oluşturacak şekilde hedefli oltalama senaryosuna dahil edilen gerçek kişilerin, kişilik haklarını korumak amacıyla, bu yayında tüm kişisel olarak tanımlanabilir bilgiler anonimleştirilmiştir. Bu nedenle bu kişilerin isim bilgileri mahmutmahmut şeklinde ifade edilmiştir.

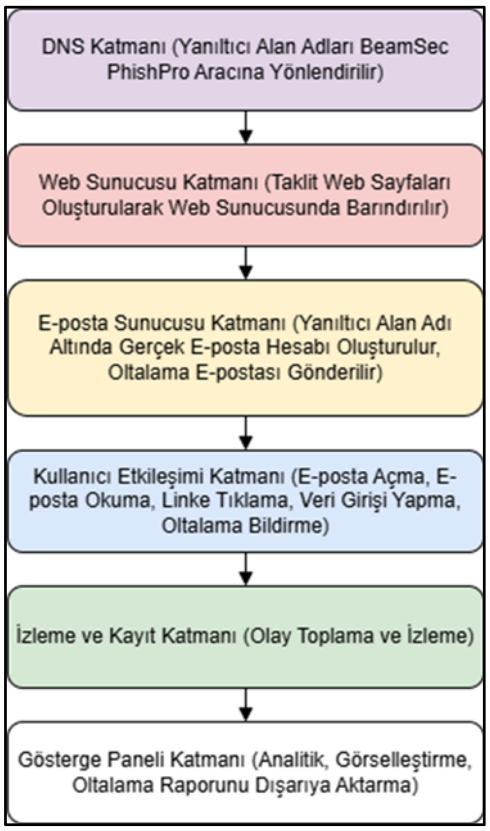
Oltalama bağlantısına tıklama yoluyla ulaşılan veri girişi yapılacak oltalama sayfaları, güvenilirliği maksimize etmek ve kullanıcı aldatmacasını kolaylaştırmak için resmi regülatör kurumların web sayfalarını (Türkiye'de EPDK, Katar'da QatarEnergy) görsel olarak taklit edecek şekilde hazırlanmıştır.

3.2.2.3 Teknik Kurulum ve Altyapı Hazırlığı

Altyapı hazırlıkları, Beam Security tarafından geliştirilen Phishing simülasyon platformu kullanılarak gerçekleştirilmiştir. platformun sistem

mimarisi Şekil 3.1'de gösterilmektedir. Araştırmacı, oltalama senaryoları için stratejik olarak aşağıdaki alan adlarını kaydetmiştir:

- **Kontrol Grupları**: Kontrol grubuna genel oltalama kapsamında parola sıfırlama senaryosu uygulanacağı için; Türkiye'de ve Katar'da faaliyet gösteren elektrik dağıtım şirketlerinin alan adları typosquatting tekniği ile gerçek kurumsal adları taklit edilecek şekilde (doma-in.gtld ve doma-in.cctld) kaydedilmiştir.
- **Deney Grupları**: İki ülkenin de ulusal regülatör kurumlarının alan adları typosquatting tekniği ile gerçek kurumsal alan adları taklit edilecek şekilde kaydedilmiştir:
  - Türkiye: epdkqov.tr (EPDK'nın meşru alan adı: epdk.gov.tr).
  - Katar: gatarenergy.qa (QatarEnergy'nin meşru alan adı: qatarenergy.qa).



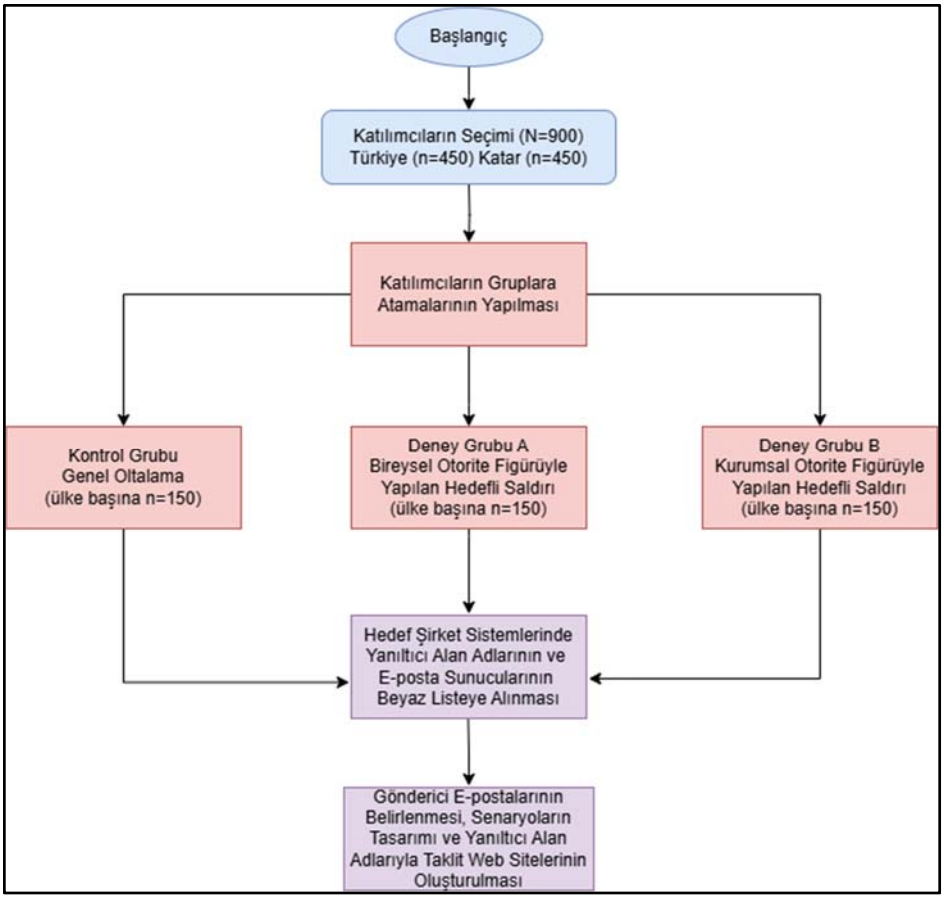
Şekil 3.1 Phishing Aracı İzleme Mimarisi Diyagramı

3.2.2.4 Davranışsal Veri Toplama Prosedürleri

Otomatik teknik yöntemler, çalışan etkileşimlerini sistematik olarak takip etmiştir:

- **E-posta Açılma Durumu**: E-posta açıldığında doğru (1) olarak işaretlenmiştir.
- **E-posta Okunma Durumu**: E-posta en az beş saniye açık kaldığında doğru (1) olarak işaretlenmiştir.
- **Bağlantı Tıklama Durumu**: E-postalar içindeki benzersiz izleme bağlantılarına tıklanıldığında doğru (1) olarak işaretlenmiştir.
- **Veri Gönderim Durumu**: Katılımcı gizliliğini sağlamak ve etik standartlara uymak için, araştırmacı sistemi yalnızca kullanıcı adlarını kaydedecek şekilde yapılandırmıştır. Oltalama aracı, oltalama web sayfalarında yapılan veri girişlerinde herhangi bir parola verisini kaydetmeden; sadece e-posta alanına girilen e-postaları kaydetmiştir. E-posta adresi ve parola verisi girildikten sonra kullanıcı tarafından veri gönderimi yapıldığında sadece e-posta adresi verisi kayıt altına alınarak bu parametre için doğru (1) olarak işaretlenmiştir. Sonuç olarak, çalışmanın hiçbir aşamasında gerçek parola bilgileri toplanmamış ve saklanmamıştır.
- **Oltalama Bildirimi Durumu**: Kullanıcı tarafından Outlook uygulaması üzerinden oltalama bildirimi yapıldığında bu parametre için doğru (1) olarak işaretlenmiştir.

  Hazırlık aşaması adımları aşağıdaki Şekil 3.2'de özetlenmiştir.



Şekil 3.2 Senaryoların Hazırlık Aşaması Akış Şeması

3.2.3 Uygulama Aşaması

Uygulama aşaması, Türkiye ve Katar'da gerçek dünya oltalama deneylerinin eş zamanlı olarak yürütülmesini içermektedir. Araştırmacılar tarafından her ülkedeki katılımcılar üç gruba ayrılmıştır: Kontrol Grubu (genel oltalama), Deney Grubu A (bireysel otorite temelli hedefli oltalama) ve Deney Grubu B (kurumsal otorite temelli hedefli oltalama).

3.2.3.1 E-postaların Dağıtımı ve Zamanlaması

Araştırmacılar tarafından, dahili iletişim müdahalesini en aza indirmek için oltalama e-postaları tüm gruplara eş zamanlı olarak gönderilmiştir. Araştırmacılar tarafından, özgünlüğü ve katılımcı etkileşimini en üst düzeye

çıkarmak için tipik çalışma saatleri sırasında, düzenli kurumsal e-posta trafiğiyle sorunsuz bir şekilde karışacak şekilde stratejik bir zamanlama seçilmiştir.

3.2.3.2 Kontrol Grubu (Genel Oltalama)

Katılımcılar, standart Microsoft parola kullanım süresi sona erme bildirimlerini taklit eden genel oltalama e-postaları almışlardır. E-postalar, hedeflenen kuruluşların gerçek kurumsal alan adlarını taklit etmek üzere tasarlanmış anonimleştirilmiş typosquatting alan adlarından (doma-in.gtld ve doma-in.cctld) gönderilmiştir. Gömülü köprü bağlantıları, alıcıları parolalarını güncellemeye teşvik ederek, genel oltalama taktiklerine karşı temel duyarlılığı test etmiştir.

3.2.3.3 Deney Grupları (Hedefli Oltalama)

Deney grupları, farklı otorite figürlerini (bireysel ve kurumsal) kullanan hedefli oltalama e-postaları almışlardır:

- **Bireysel Otorite (Deney Grubu A):** E-postalar açıkça ISO 27001 uyumluluğuna ve yapay zeka kullanılmışsa ek ISO 42001 uyumluluk gerekliliklerine atıfta bulunmuştur. Katılımcılar, oltalama bağlantıları aracılığıyla uyumluluk doğrulamasını teşvik eden, doğrulanmış bireysel otoritelerden e-postalar almışlardır. Araştırmacılar tarafından, güvenilirliği ve aldatmayı artırmak için oltalama sayfaları her iki ülkenin ulusal regülatör kurumların web sayfalarını görsel olarak taklit edecek şekilde hazırlanmıştır.
- **Kurumsal Otorite (Deney Grubu B):** E-postalar aynı uyumluluk anlatılarını taşımış, ancak kurumsal denetim e-posta adreslerinden (Türkiye'de denetim@epdkqov.tr, Katar'da audit@gatarenergy.qa) gönderilmiş gibi gösterilmiştir.

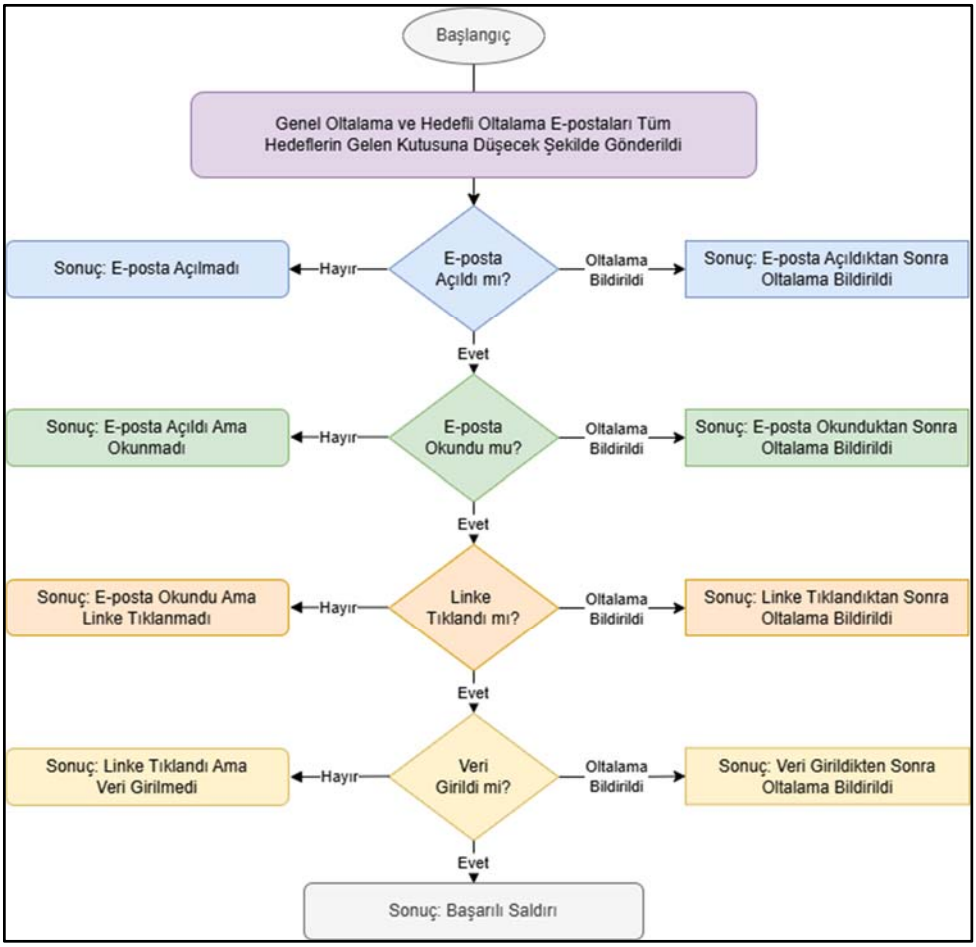
Bu yaklaşım, oltalama duyarlılığı üzerinde bireysel ve kurumsal otorite figürlerinin etkisini birbirinden izole etmek için tasarlanmıştır.

3.2.3.4 Teknik İzleme ve Gerçek Zamanlı Veri Toplama

Oltalama deneyi, e-posta teslimatını ve katılımcı davranışlarını gerçek zamanlı olarak izlemek için otomatik araçlardan yararlanmıştır. Sistem, katılımcı etkileşimi üzerine verileri anında kaydetmiştir:

- E-posta açıldı, e-posta okundu, bağlantı tıklandı, veri gönderildi ve oltalama bildirildi olayları kaydedilmiş ve güvenli bir şekilde saklanmıştır.
- Toplanan veriler anonimleştirilmiş ve sonraki istatistiksel analiz için sistematik olarak düzenlenmiştir.

Uygulama aşaması adımları Şekil 3.3'te özetlenmiştir.



Şekil 3.3 Uygulama Aşaması Akış Şeması

3.2.4 Veri Analizi Teknikleri

İstatistiksel analizler IBM SPSS yazılımı (Sürüm 28) kullanılarak gerçekleştirilmiştir. Toplanan veriler, katılımcı davranışlarını temsil eden ikili kategorik değişkenlerden (0 = Hayır, 1 = Evet) oluşmaktadır: e-posta açıldı, e-posta okundu, bağlantıya tıklandı, veri gönderildi ve oltalama bildirildi.

3.2.4.1 Hipotez Testi ve İstatistiksel Prosedürler

Çalışmada tüm hipotezleri (H1, H2, H3 ve H4) test etmek için Ki-Kare Bağımsızlık Testi kullanılmış, gruplar ve ülkeler arasındaki kategorik değişkenler karşılaştırılmıştır. Ki-kare analizi özellikle kategorik veriler için uygun olup değişkenler arasındaki ilişkilerin net yorumlarını sağlamaktadır.

İlişkilerin gücünü ölçmek için Olasılık Oranları (OR) hesaplanmış, otorite türleri arasında başarılı oltalama saldırılarının (veri gönderimi) göreceli olasılığı vurgulanmıştır.

Analiz, Ki-kare testleri ile belirlenen ilişkilerin etki büyüklüklerini ölçmek için Cramer's V ve Phi Katsayılarının hesaplanmasını içermektedir. Bu istatistikler, kategorik değişkenler arasında gözlemlenen ilişkilerin büyüklüğü ve pratik önemi hakkında ek açıklık sağlamıştır.

3.2.4.2 Çoklu Karşılaştırmalar ve Düzeltmeler

Çoklu testlerden kaynaklanan Tip I hata riskini kontrol etmek için Bonferroni düzeltmesi uygulanmış, sağlam sonuçlar sağlamak için düzeltilmiş anlamlılık eşiği $p < 0.05$ olarak belirlenmiştir.

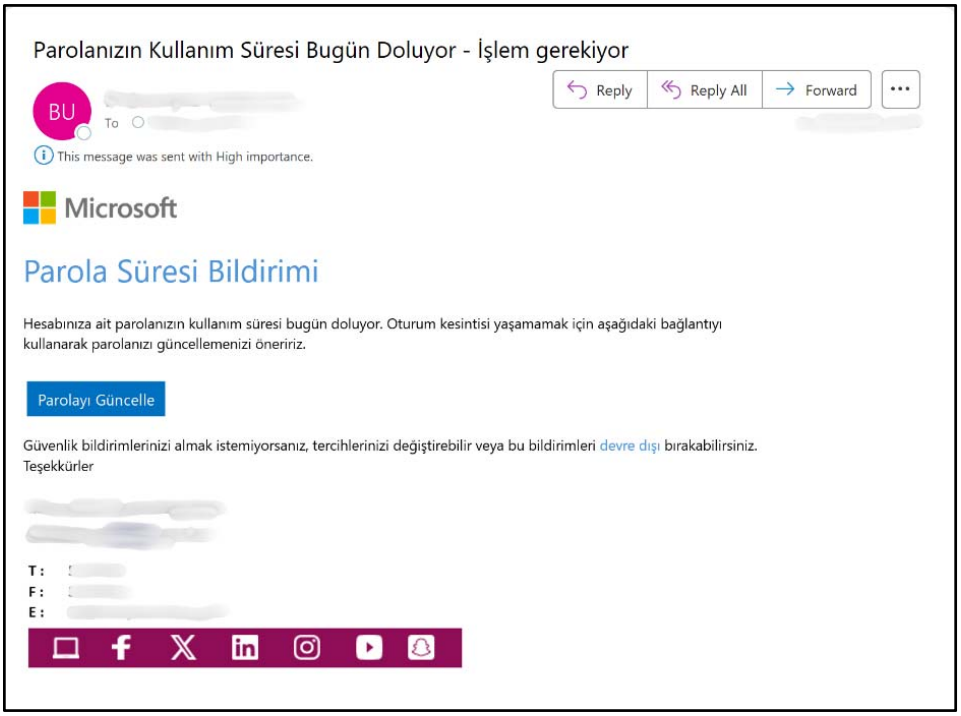
3.2.4.3 Davranışsal Geçiş Analizi (H4)

Ki-kare testi, ilk eylemlerin (oltalama bağlantılarına tıklama) sonraki kritik eylemlerin (hassas verileri gönderme) olasılığını önemli ölçüde artırıp artırmadığını incelemek için kullanılmıştır. Sonuçlar p-değerleri, olasılık oranları ve netlik için etki büyüklükleri ile rapor edilmiştir.

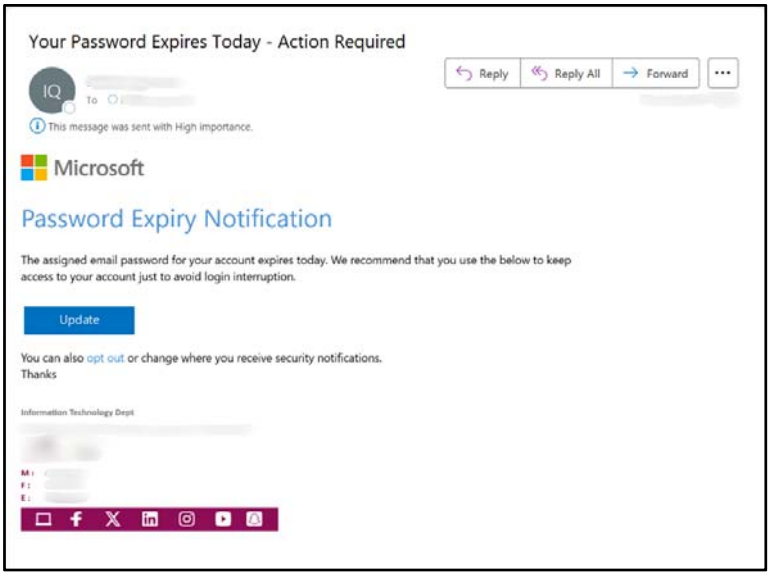
3.2.5 Oltalama Saldırıları Ekran Görüntüleri

3.2.5.1 Genel Oltalama Saldırısı Ekran Görüntüleri

Genel oltalama e-postaları, hem Türkiye hem de Katar'daki kontrol grubu katılımcılarına gönderilmiştir. Bu e-postalar, kullanıcıları gömülü bağlantılar aracılığıyla parolalarını güncellemeye teşvik eden standart Microsoft parola kullanım süresi doldu bildirimlerini simüle etmiştir. Türkiye'deki kontrol grubuna gönderilen genel oltalama saldırısı e-postaları Türkçe dilinde hazırlanmıştır. Katar'daki kontrol grubuna gönderilen genel oltalama saldırısı e-postaları ise, e-postaların Microsoft otomasyon sisteminden gönderildiğinin taklit edilmesi nedeniyle, kullanıcının klavye dil ayarına göre dil seçimi yapılmayarak, İngilizce dilinde hazırlanmıştır. Türkiye'deki kontrol grubuna gönderilen genel oltalama saldırısı e-posta ekran görüntüsü Şekil 3.4'te, Katar'daki kontrol grubuna gönderilen genel oltalama saldırısı e-posta ekran görüntüsü Şekil 3.5'te sunulmuştur.

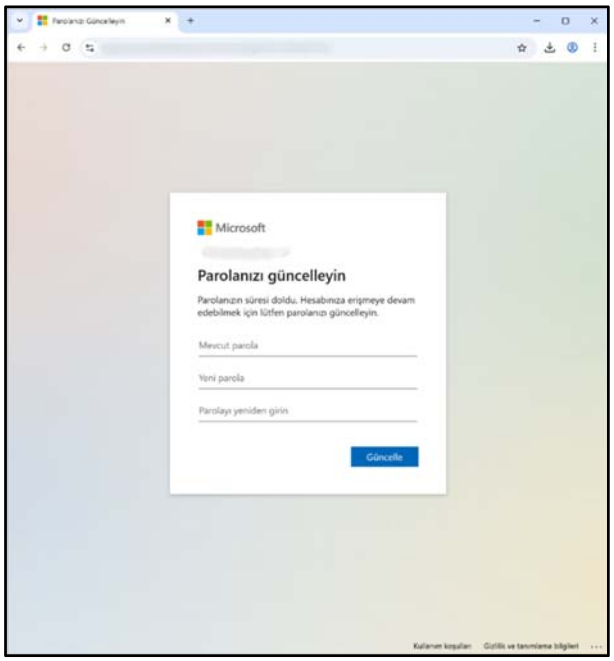


Şekil 3.4 Genel Oltalama Saldırısı E-Posta Ekran Görüntüsü – Türkiye



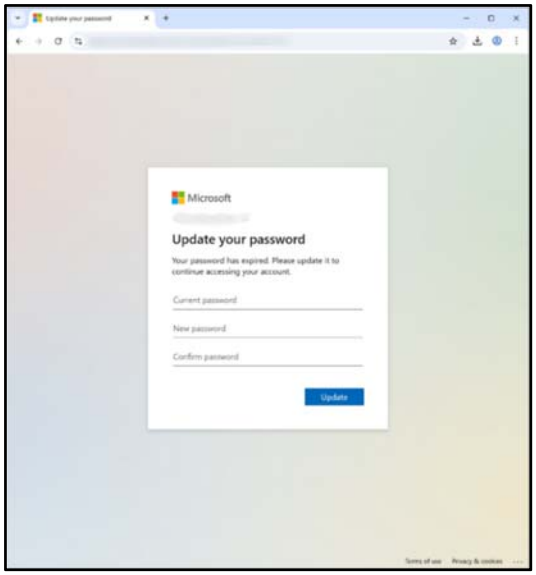
Şekil 3.5 Genel Oltalama Saldırısı E-Posta Ekran Görüntüsü - Katar

Türkiye'deki kontrol grubuna gönderilen genel oltalama saldırısı e-postasında bulunan bağlantıya kullanıcıların tıklaması halinde yönlendirildikleri taklit edilen web sayfası ekran görüntüsü Şekil 3.6'da gösterilmektedir.

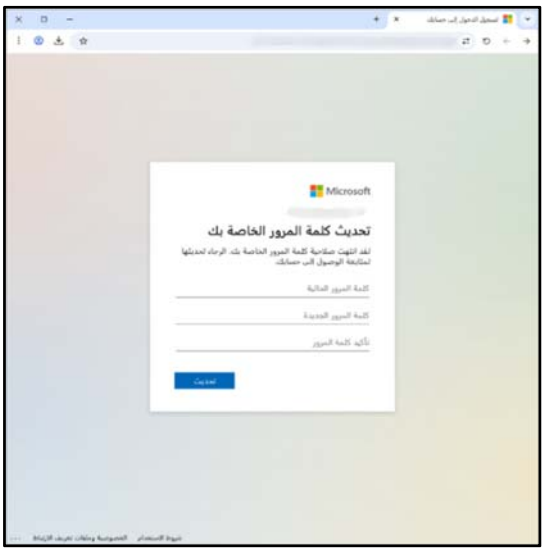


Şekil 3.6 Microsoft Parola Güncelleme Sayfası Klonu - Türkiye

Katar'daki kontrol grubuna gönderilen genel oltalama saldırısı e-postasında bulunan bağlantıya kullanıcıların tıklaması halinde; kullanıcının web tarayıcısının arayüz dili ile bağlantılı olarak, yönlendirildikleri taklit edilen web sayfasının İngilizce ekran görüntüsü Şekil 3.7'de, Arapça ekran görüntüsü ise Şekil 3.8'de gösterilmektedir.



Şekil 3.7 Microsoft Parola Güncelleme Sayfası Klonu – Katar (İngilizce)

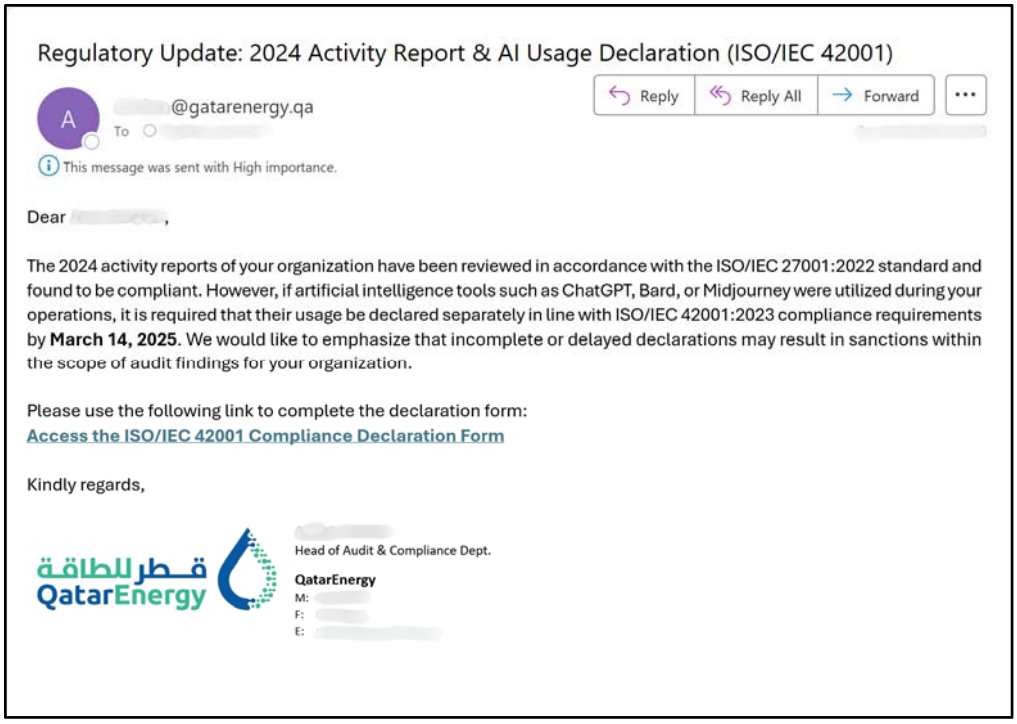


Şekil 3.8 Microsoft Parola Güncelleme Sayfası Klonu – Katar (Arapça)

3.2.5.2 Bireysel Otorite Figürü Kullanılan Hedefli Oltalama Saldırısı Ekran Görüntüleri

Bireysel otorite figürlerinden gelen hedefli oltalama e-postaları Türkiye ve Katar'daki "Deney Grubu A" katılımcılarına gönderilmiştir. Türkiye'deki "Deney Grubu A" katılımcılarına bireysel otorite figüründen gönderilen e-posta ekran görüntüsü Şekil 3.9'da, Katar'daki "Deney Grubu A" katılımcılarına bireysel otorite figüründen gönderilen e-posta ekran görüntüsü Şekil 3.10'da yer almaktadır.

Şekil 3.9 Bireysel Otorite Hedefli Oltalama E-postası - Türkiye



Şekil 3.10 Bireysel Otorite Hedefli Oltalama E-postası – Katar

3.2.5.3 Kurumsal Otorite Figürü Kullanılan Hedefli Oltalama Saldırısı Ekran Görüntüleri

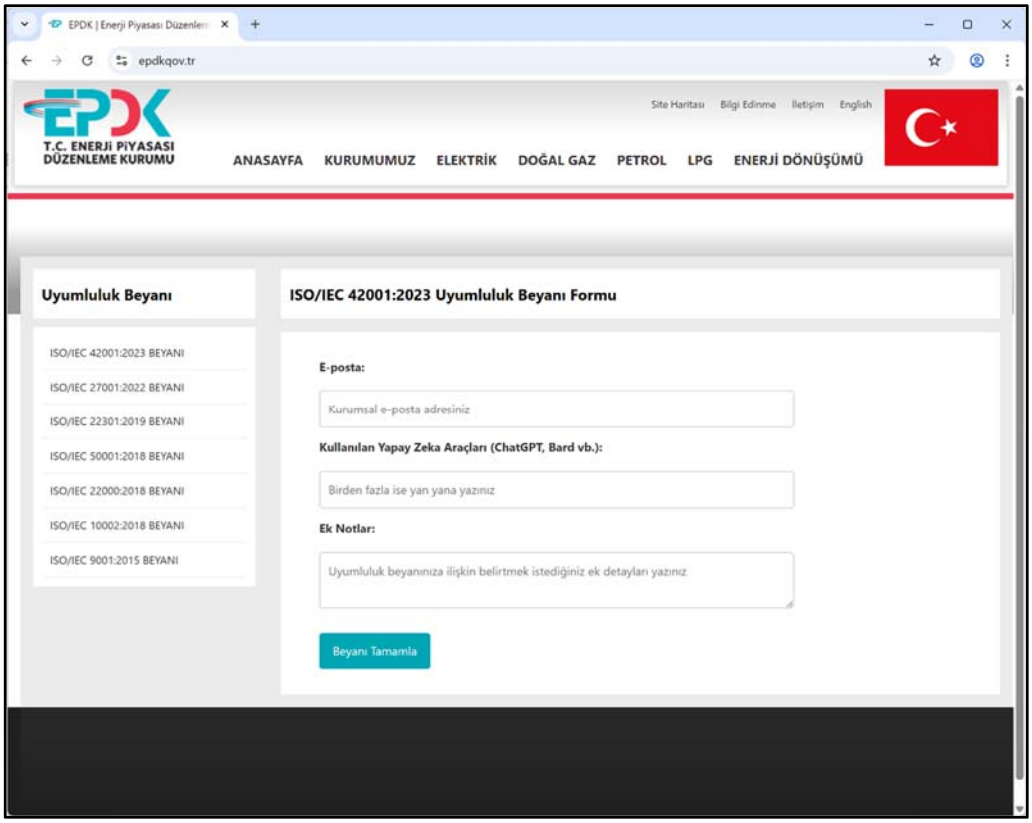
Kurumsal otorite figürlerinden gelen hedefli oltalama e-postaları Türkiye ve Katar'daki "Deney Grubu B" katılımcılarına gönderilmiştir. Türkiye'deki "Deney Grubu B" katılımcılarına kurumsal otorite figüründen gönderilen e-posta ekran görüntüsü Şekil 3.11'de, Katar'daki "Deney Grubu B" katılımcılarına kurumsal otorite figüründen gönderilen e-posta ekran görüntüsü Şekil 3.12'de yer almaktadır.

Şekil 3.11 Kurumsal Otorite Hedefli Oltalama E-postası - Türkiye

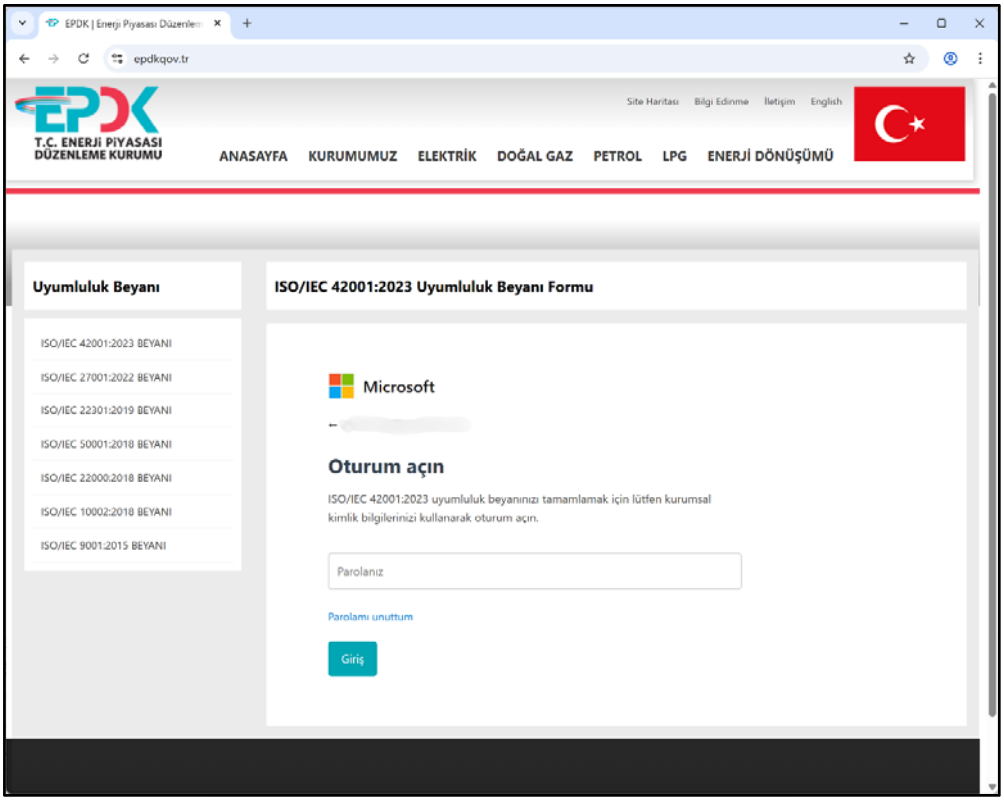
Şekil 3.12 Kurumsal Otorite Hedefli Oltalama E-postası – Katar

3.2.5.4 Otorite Figürü Kullanılan Saldırılarda Web Sitesi Klonları

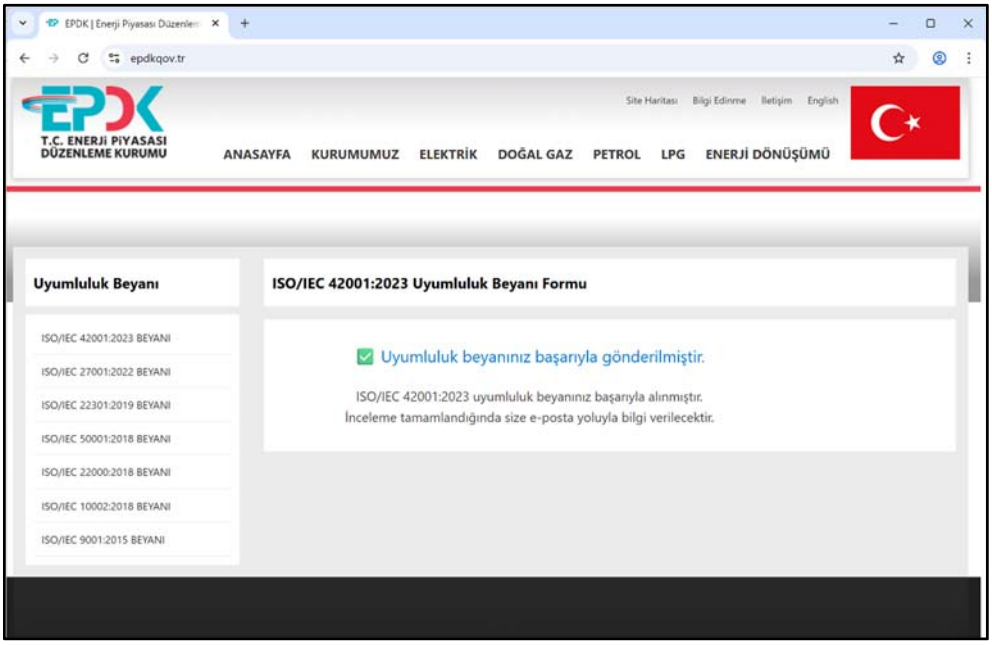
Türkiye'de otorite figürü kullanılarak gönderilen e-postalarda bulunan bağlantıya tıklanılması halinde, kullanıcılar EPDK-taklit sayfasına yönlendirilmiştir. Hedef kullanıcıların parola bilgilerini girmeye yönlendiren klon EPDK sayfalarının ekran görüntüleri Şekil 3.13 ile Şekil 3.15 arasında yer almaktadır.



Şekil 3.13 EPDK Web Sitesi Klonu Açılış Sayfası

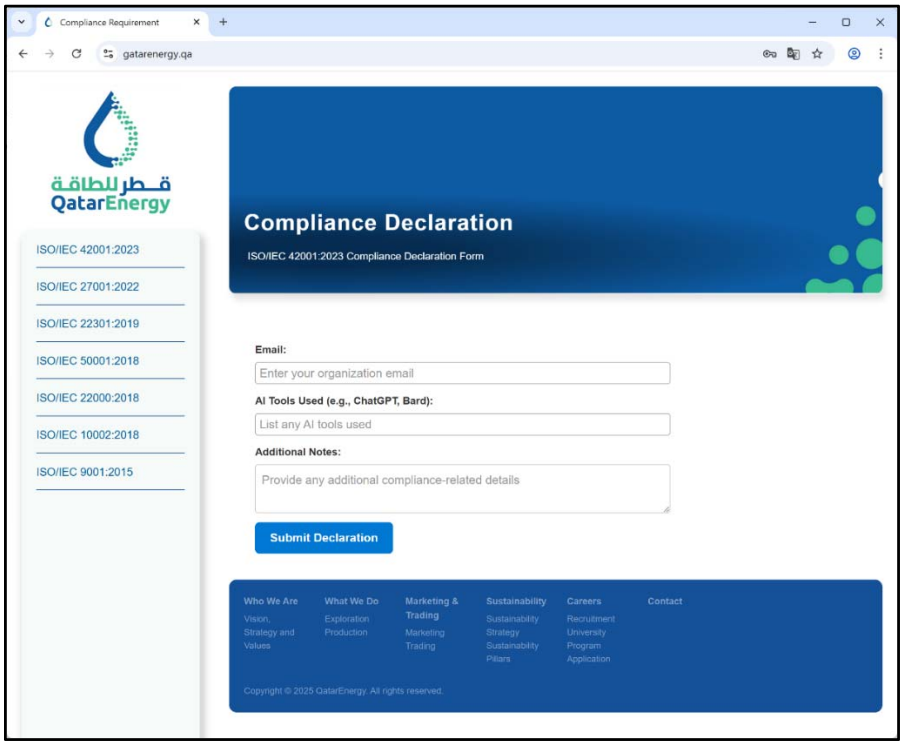


Şekil 3.14 EPDK Web Sitesi Klonu Parola Giriş Sayfası

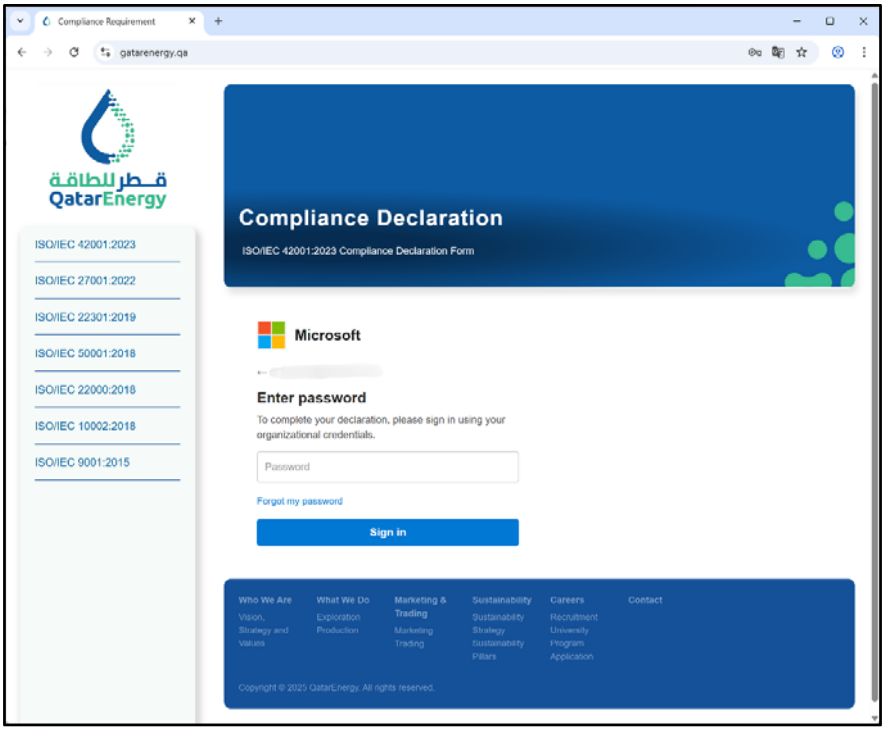


Şekil 3.15 EPDK Web Sitesi Klonu Sonuç Sayfası

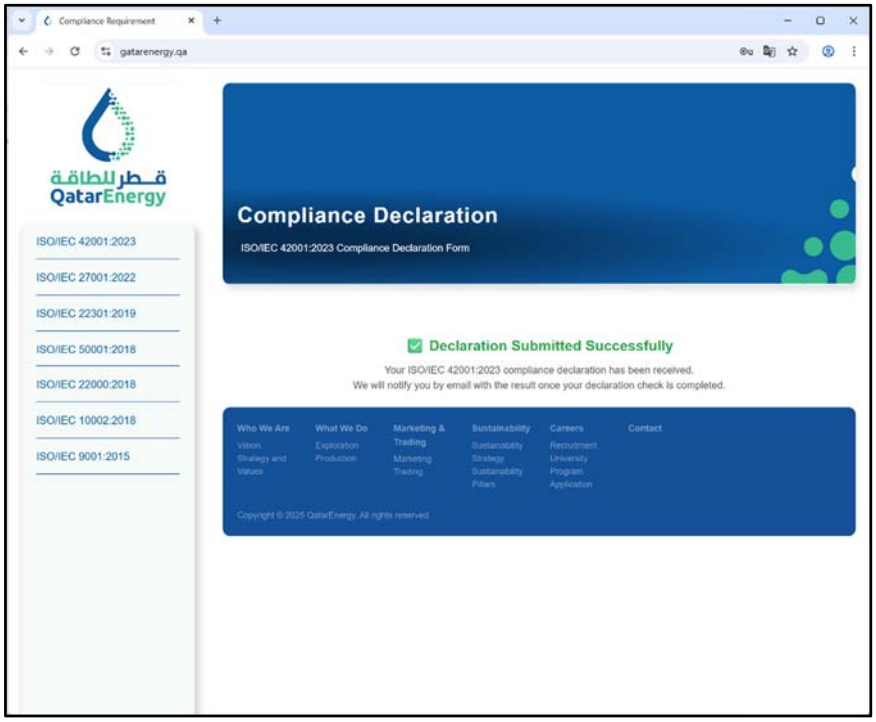
Katar'da otorite figürü kullanılarak gönderilen e-postalarda bulunan bağlantıya tıklanılması halinde, kullanıcılar QatarEnergy-taklit sayfasına yönlendirilmiştir. Hedef kullanıcılar, web tarayıcılarının arayüz dili ile bağlantılı olarak, İngilizce veya Arapça hazırlanmış olan taklit web sayfalarına yönlendirilmiştir. Hedef kullanıcıların parola bilgilerini girmeye yönlendiren QatarEnergy-taklit sayfalarının ekran görüntüleri; İngilizce olarak Şekil 3.16 ile Şekil 3.18 arasında, Arapça olarak Şekil 3.19 ile Şekil 3.21 arasında yer almaktadır.



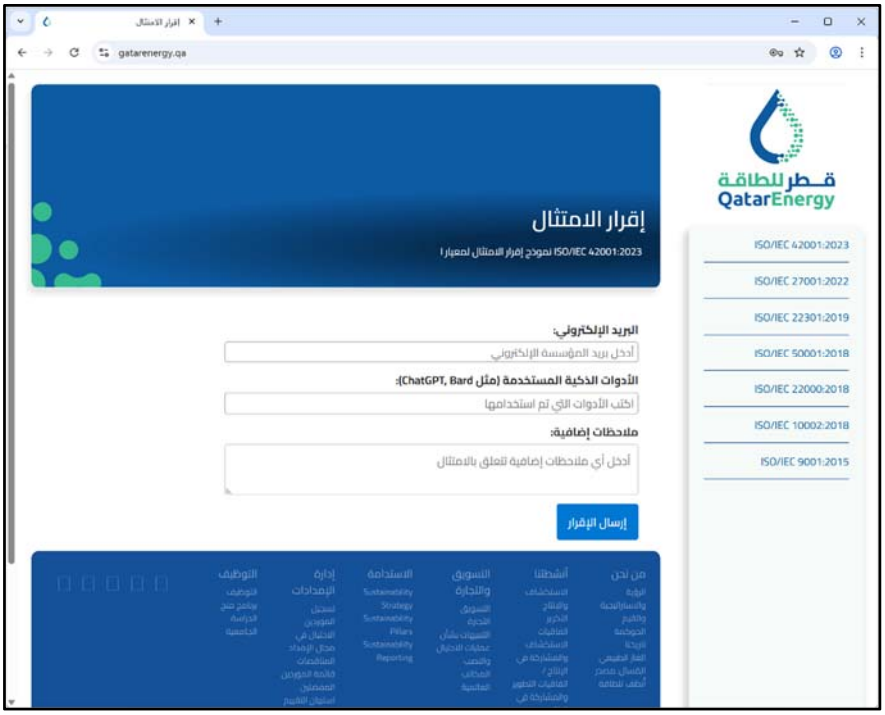
Şekil 3.16 QatarEnergy Web Sitesi Klonu Açılış Sayfası - İngilizce



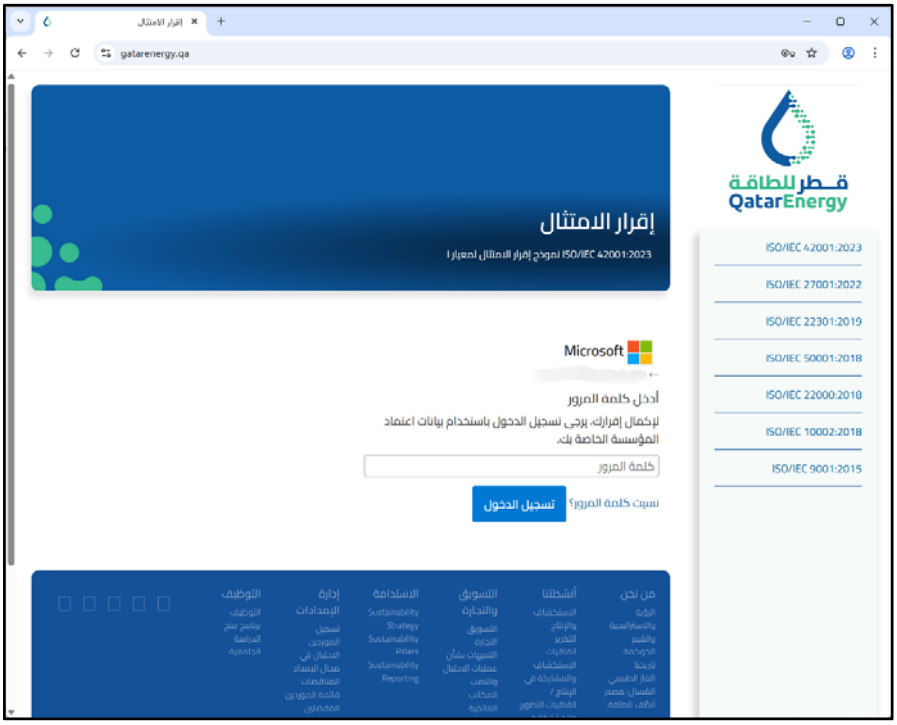
Şekil 3.17 QatarEnergy Web Sitesi Klonu Parola Giriş Sayfası - İngilizce



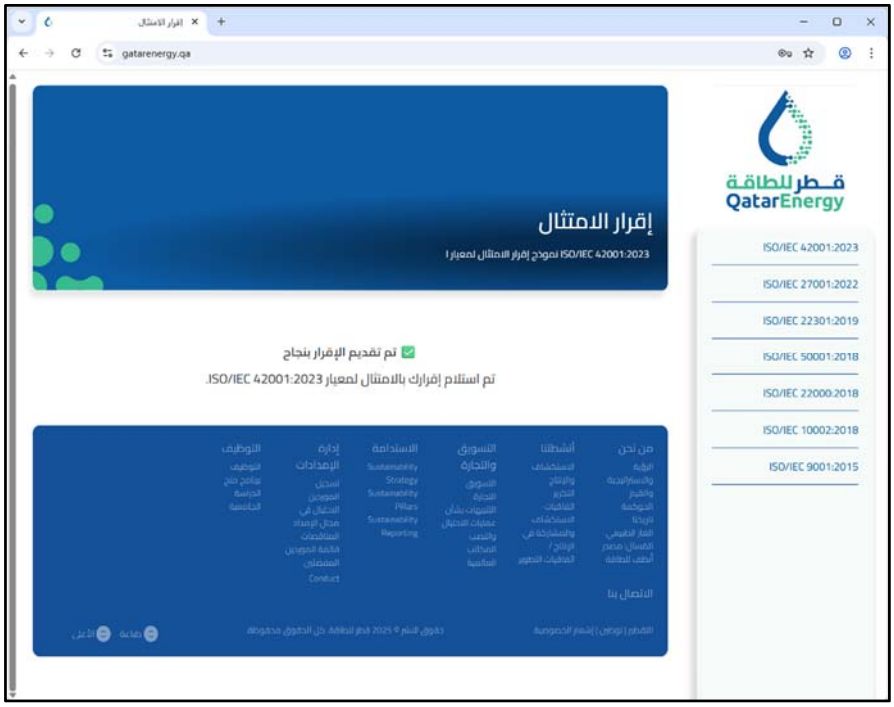
Şekil 3.18 QatarEnergy Web Sitesi Klonu Sonuç Sayfası - İngilizce



Şekil 3.19 QatarEnergy Web Sitesi Klonu Açılış Sayfası – Arapça



Şekil 3.20 QatarEnergy Web Sitesi Klonu Parola Giriş Sayfası - Arapça



Şekil 3.21 QatarEnergy Web Sitesi Klonu Sonuç Sayfası - Arapça

3.3 ARAŞTIRMANIN SINIRLILIKLARI

Bu çalışmanın belirtilmesi gereken çeşitli sınırlamaları bulunmaktadır:

Üst Düzey Yöneticilerin Dahil Edilmemesi: İlgili şirketler, C-Seviye Yöneticilerin bu oltalama deneyine dahil edilmesini onaylamamıştır. Sonuç olarak, çalışmada üst düzey liderlerin sosyal mühendislik saldırılarına karşı duyarlılığı analiz edilememiştir. Bu durum, bulguların yönetim kademesindeki hiyerarşik dinamiklere genellenebilirliğini sınırlamaktadır.

Bilgi Güvenliği Farkındalık Eğitimi Durumuna Göre Segmentasyon Eksikliği: Katılımcı seçim süreci, bilgi güvenliği farkındalık eğitimindeki farklılıkları hesaba katmamıştır. Şirketler karışık bir seçim talep etmiş ve çalışanların eğitim durumları hakkında bilgi paylaşmamıştır. Sonuç olarak, çalışmada eğitimli ve eğitimsiz çalışanlar arasındaki davranışsal farklılıklar karşılaştırılamamıştır.

Coğrafi ve Sektörel Sınırlamalar: Çalışma yalnızca Türkiye ve Katar'daki elektrik dağıtım şirketlerinde gerçekleştirilmiştir. Bu sektörel ve coğrafi sınırlama, bulguların daha geniş uygulanabilirliğini kısıtlamaktadır. Bulguların farklı organizasyonel ve kültürel bağlamlarda doğrulanması ve genişletilmesi için daha geniş sektörler arası ve çok ülkeli çalışmalar yürütülmelidir.

Potansiyel Organizasyonel ve Kendi Kendine Seçim Yanlılığı: Katılımcılar belirli organizasyonel kültürler içinde çalıştığından ve oltalama simülasyonlarına gönüllü olarak katıldığından, sonuçları etkileyen organizasyonel veya kendi kendine seçim yanlılıkları riski bulunmaktadır. Bu tür yanlılıklar, daha yüksek siber güvenlik farkındalığına sahip veya güvenlik girişimlerine katılma konusunda daha istekli çalışanların aşırı temsil edilmesine yol açmış olabilir ve bu durum potansiyel olarak oltalama girişimlerine karşı gözlemlenen direnç oranlarını şişirmiş olabilmektedir.

3.4 ETİK HUSUSLAR

Çalışma, phishing platformunu kullanan bir siber güvenlik çözümleri üreticisi olan Beam Security ile işbirliği içinde yürütülmüştür. Oltalama saldırılarının uygulaması, veri toplama altyapısının tasarımı ve anonimleştirme süreçleri, Beam Security'nin iç Etik ve Yasal Uyum Kurulu tarafından resmi olarak incelenmiş ve onaylanmıştır. Çalışma boyunca gözetim, Beam Security'nin ISO/IEC 27001 sertifikalı Bilgi Güvenliği Yönetim Sistemi (BGYS) çerçevesi altında ve ISO/IEC 29100 Gizlilik Çerçevesi doğrultusunda sürdürülmüştür. Toplanan tüm meta veriler yalnızca araştırma analizi için gerekli olan minimum süre (altı ayı aşmayan) boyunca tutulmuş ve daha sonra ISO/IEC 27040'ın veri saklama ve güvenli veri imha önerileri doğrultusunda güvenli bir şekilde silinmiştir.

Katılımcılar, İstanbul, Türkiye'de bulunan devlet düzenlemesine tabi bir elektrik dağıtım şirketinden ve Katar'ın ulusal enerji çerçevesine bağlı bir devlete ait elektrik ve su hizmetleri işletmesinden seçilmiştir. Her iki kurum da

çalışmanın akademik kapsamı ve operasyonel yapısı hakkında tam olarak bilgilendirilmiş ve katılım için resmi yazılı onay vermiştir. Katılımcılara, davranışsal verilerinin yalnızca araştırma amaçları için kullanılacağı ve istihdam durumlarını veya değerlendirmelerini etkilemeyeceği bildirilmiştir. Katılımcılar ayrıca, herhangi bir ceza olmaksızın istedikleri zaman çalışmadan çekilme haklarının olduğu konusunda bilgilendirilmiştir. Bu onay, kontrollü oltalama kampanyalarının teknik yapılandırması için izni, gerçekçiliği artırmak amacıyla kurumsal isimler, logolar, departman başlıkları ve seçilmiş bireysel çalışan tanımlayıcılarının kullanımını içermiş ve tümü ilgili etik ve yasal uyum kurulları tarafından incelenip onaylanmıştır.

Kişisel, hassas veya kimlik bilgileriyle ilgili veriler toplanmamıştır. E-postanın açılması, bağlantıya tıklanması ve veri gönderilmesi gibi davranışsal eylemler, anonimleştirilmiş meta veriler kullanılarak otomatik olarak izlenmiştir. Parola alanları, uygun olduğu durumlarda, iletimden önce yer tutucu karakterlerle değiştirilmiş, böylece gerçek kimlik bilgilerinin çalışmanın hiçbir aşamasında saklanmadığı veya açığa çıkmadığı sağlanmıştır.

Yayın sırasında bireysel hakları daha da korumak için, kurumsal onay ile deney sırasında kullanılan gerçek e-posta adresleri ve çalışan isimleri dahil olmak üzere tüm kişisel tanımlayıcı bilgiler bu çalışmada anonimleştirilmiştir. Çalışma ayrıca Türkiye'nin KVKK ve Katar'ın QCB uyumluluk düzenlemeleri dahil olmak üzere ulusal veri koruma yasalarıyla tam uyum içinde yürütülmüştür. Tüm araştırma faaliyetleri, kurumsal siber güvenlik politikalarına ve her iki ülkede geçerli yasal çerçevelere uygun olarak gerçekleştirilmiştir.

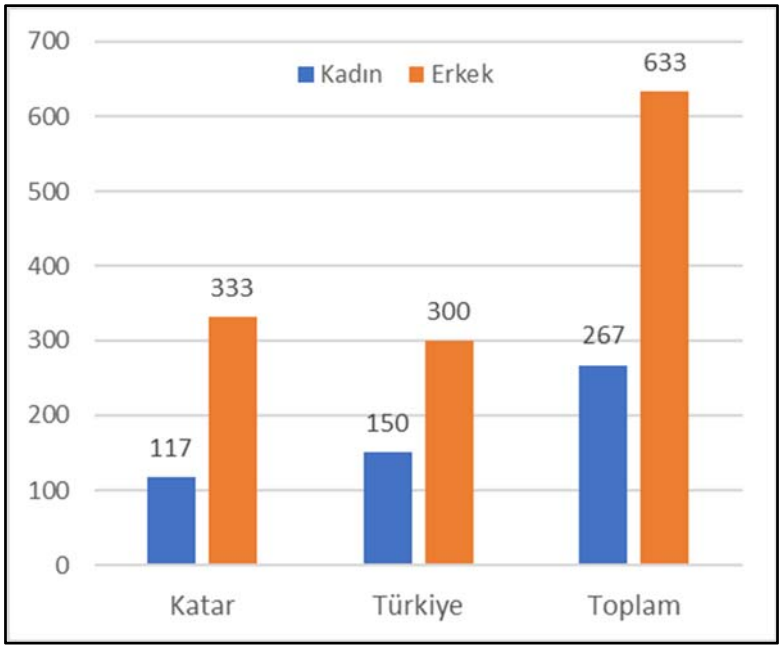
BÖLÜM 4

4. BULGULAR

4.1 BETİMSEL İSTATİSTİKLER

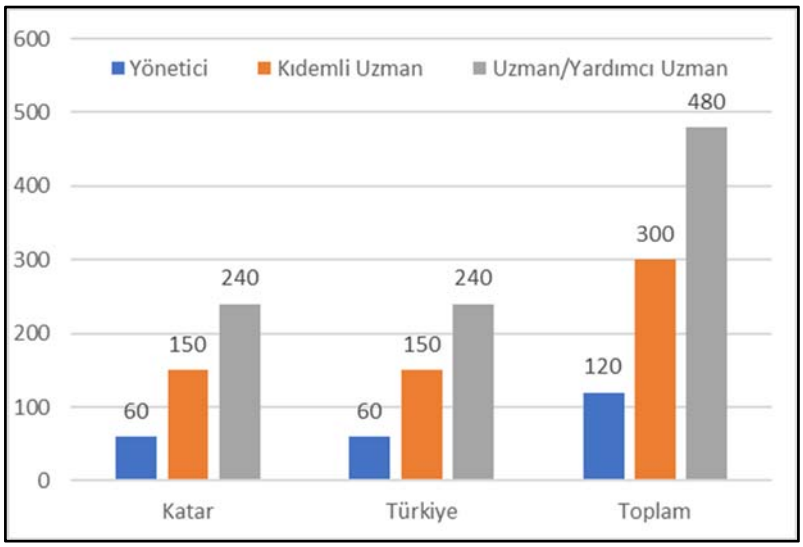
Katılımcılar incelendiğinde; 900 katılımcının 267'sinin (%29,7) kadın ve 633'ünün (%70,3) erkek olduğu görülmektedir. Ülkeye göre cinsiyet dağılımı incelendiğinde; Katar'daki katılımcıların 117'sinin (%26) kadın ve 333'ünün (%74) erkek olduğu, Türkiye'deki katılımcıların ise 150'sinin (%33,3) kadın ve 300'ünün (%66,7) erkek olduğu görülmektedir. Katılımcıların cinsiyet dağılımı Tablo 4.1'de sunulmuştur. Her iki ülkede de erkek katılımcılar çoğunluktadır, ancak kadın katılımcıların oranı Türkiye'de Katar'a göre daha yüksektir. Cinsiyet ile sosyal mühendislik saldırısının başarısı arasında istatistiksel olarak anlamlı bir ilişki bulunmamaktadır ($\chi^2 = 0,590$, $p = 0,442$).

Tablo 4.1 Katılımcıların Cinsiyet Dağılımı



Katılımcıların pozisyonlarına göre dağılımı incelendiğinde, her iki ülkede de aynı dağılım modeli olduğu görülmektedir. Toplam 900 katılımcının 120'si (%13,3) yönetici, 300'ü (%33,3) kıdemli uzman ve 480'i (%53,3) uzman/yardımcı uzmandır. Katılımcıların iş pozisyonlarına göre dağılımı Tablo 4.2'de sunulmuştur. Her iki ülkede de 60 yönetici, 150 kıdemli uzman ve 240 uzman/yardımcı uzman bulunmaktadır. Pozisyon ile sosyal mühendislik saldırısının başarısı arasında istatistiksel olarak anlamlı bir ilişki bulunmaktadır (χ^2=44,598, p<0,001).

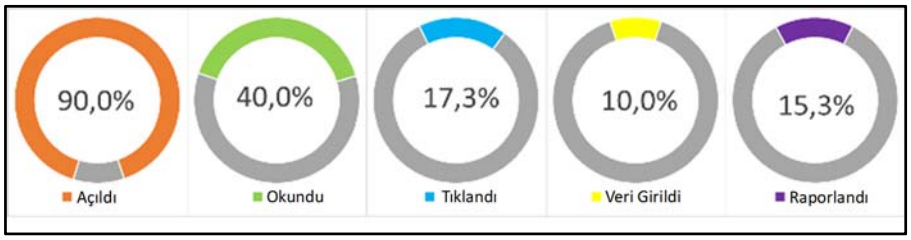
Tablo 4.2 Katılımcıların İş Pozisyonlarına Göre Dağılımı



Araştırmada, katılımcıların sosyal mühendislik saldırılarına karşı tepkileri; e-postayı açma, okuma, bağlantıya tıklama, veri girişi yapma ve oltalama saldırısını bildirme açısından incelenmiştir.

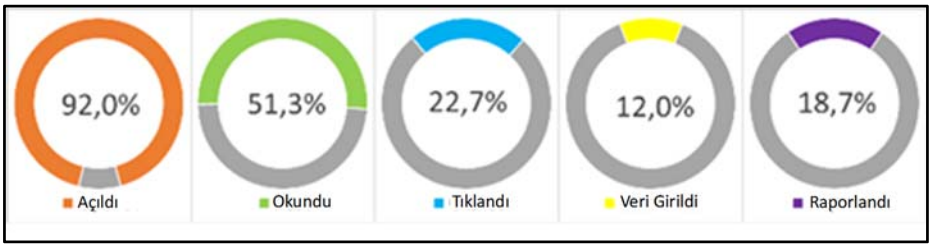
Türkiye'deki kontrol grubunda, gönderilen genel oltalama e-postalarının %90,0'ı (n=135) katılımcılar tarafından açılmıştır. Bu e-postaların %40,0'ı (n=60) okunmuş, %17,3'ünde (n=26) oltalama bağlantısına tıklanmış ve %10,0'ında (n=15) veri girişi yapılmıştır. Ayrıca, katılımcıların %15,3'ü (n=23) oltalama girişimini yetkililere bildirmiştir. Türkiye'deki kontrol grubu için sonuçlar Tablo 4.3'te sunulmuştur.

Tablo 4.3 Türkiye'de Kontrol Grubu Genel Oltalama Sonuçları



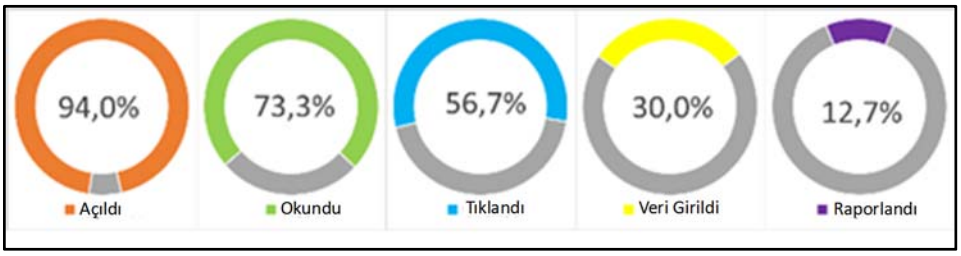
Katar'daki kontrol grubunda, gönderilen genel oltalama e-postalarının %92,0'ı (n=138) katılımcılar tarafından açılmıştır. Bunların %51,3'ü (n=77) okunmuş, %22,7'sinde (n=34) oltalama bağlantısına tıklanmış ve %12,0'ında (n=18) veri girişi yapılmıştır. Oltalama girişimini yetkili birimlere bildirme oranı %18,7'dir (n=28). Katar'daki kontrol grubu için sonuçlar Tablo 4.4'te sunulmuştur.

Tablo 4.4 Katar'da Kontrol Grubu Genel Oltalama Sonuçları



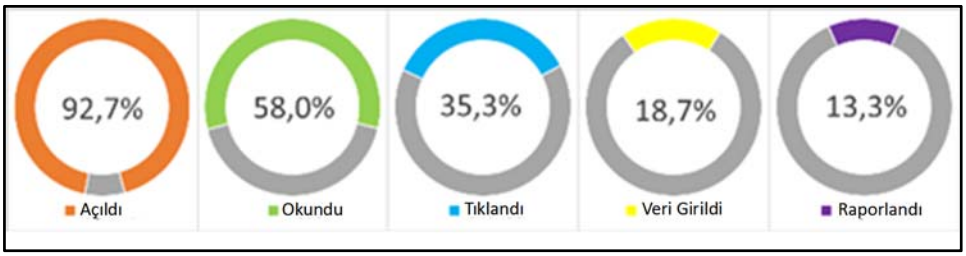
Türkiye'de, bireysel otorite figürü kullanılarak gönderilen hedefli oltalama e-postalarının %94,0'ı (n=141) katılımcılar tarafından açılmıştır. Bu e-postaların %73,3'ü (n=110) okunmuş, %56,7'sinde (n=85) oltalama bağlantısına tıklanmış ve %30,0'ında (n=45) veri girişi yapılmıştır. Oltalama girişimini yetkili birimlere bildirme oranı %12,7'dir (n=19). Türkiye'de bireysel otorite figürlerini kullanan hedefli oltalama e-postaları için sonuçlar Tablo 4.5'te sunulmuştur.

Tablo 4.5 Türkiye'de Bireysel Otorite Figürü Hedefli Oltalama Sonuçları



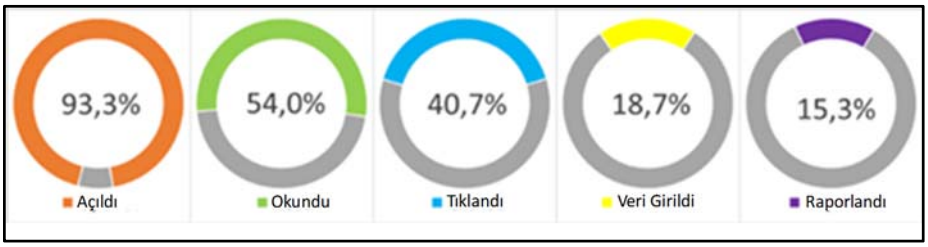
Katar'da, bireysel otorite figürü kullanılarak gönderilen hedefli oltalama e-postalarının %92,7'si (n=139) katılımcılar tarafından açılmıştır. Bunların %58,0'ı (n=87) okunmuş, %35,3'ünde (n=53) oltalama bağlantısına tıklanmış ve %18,7'sinde (n=28) veri girişi yapılmıştır. Oltalama girişimini yetkili birimlere bildirme oranı %13,3'tür (n=20). Katar'da bireysel otorite figürlerini kullanan hedefli oltalama e-postaları için sonuçlar Tablo 4.6'da sunulmuştur.

Tablo 4.6 Katar'da Bireysel Otorite Figürü Hedefli Oltalama Sonuçları



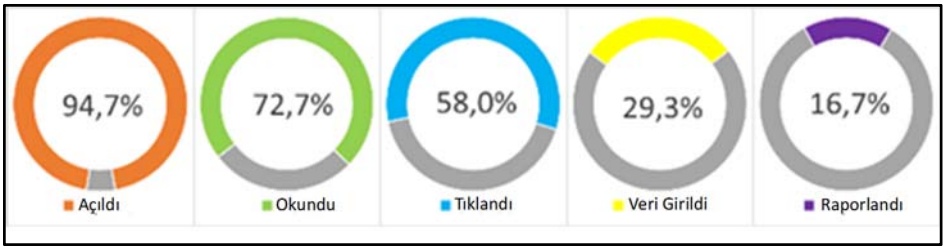
Türkiye'de, kurumsal otorite figürü kullanılarak gönderilen hedefli oltalama e-postalarının %93,3'ü (n=140) katılımcılar tarafından açılmıştır. Bu e-postaların %54,0'ı (n=81) okunmuş, %40,7'sinde (n=61) oltalama bağlantısına tıklanmış ve %18,7'sinde (n=28) veri girişi yapılmıştır. Oltalama girişimini yetkili birimlere bildirme oranı %15,3'tür (n=23). Türkiye'de kurumsal otorite figürlerini kullanan hedefli oltalama e-postaları için sonuçlar Tablo 4.7'de sunulmuştur.

Tablo 4.7 Türkiye'de Kurumsal Otorite Figürü Hedefli Oltalama Sonuçları



Katar'da, kurumsal otorite figürü kullanılarak gönderilen hedefli oltalama e-postalarının %94,7'si (n=142) katılımcılar tarafından açılmıştır. Bunların %72,7'si (n=109) okunmuş, %58,0'ında (n=87) oltalama bağlantısına tıklanmış ve %29,3'ünde (n=44) veri girişi yapılmıştır. Oltalama girişimini yetkili birimlere bildirme oranı %16,7'dir (n=25). Katar'da kurumsal otorite figürlerini kullanan hedefli oltalama e-postaları için sonuçlar Tablo 4.8'de sunulmuştur.

Tablo 4.8 Katar'da Kurumsal Otorite Figürü Hedefli Oltalama Sonuçları



Sonuçlar, katılımcıların e-postaları büyük ölçüde açtıklarını, e-postaları açan kullanıcıların büyük kısmının e-posta içeriğini okuduğunu göstermektedir. Bağlantıya tıklama ve veri girişi yapma oranları kademeli olarak azalmaktadır. Sonuçlar ayrıca, oltalama bildirimi oranının düşük bir seviyede kaldığını göstermektedir.

4.2 HİPOTEZ TESTLERİ

4.2.1 Saldırı Tekniğine Dayalı Hipotez Testi

Bu bölümde, saldırı tekniğinin (genel oltalama ve hedefli oltalama) sosyal mühendislik saldırılarının başarısı üzerindeki etkisi incelenmektedir. İlk hipotez (H1), genel oltalama ve hedefli oltalama teknikleri arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark olup olmadığını test etmektedir.

- $H1_0$: Genel oltalama ve hedefli oltalama teknikleri arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark yoktur.
- $H1_1$: Genel oltalama ve hedefli oltalama teknikleri arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark vardır.

Hipotezi test etmek için Ki-kare bağımsızlık testi kullanılmıştır. Saldırı başarısı, katılımcıların veri gönderim durumu (DataSubmissionStatus) ile ölçülmüştür. Analizin sonuçları Tablo 4.9'de sunulmaktadır.

Tablo 4.9 Saldırı Tekniğine Göre Veri Gönderme Durumu Karşılaştırması

Değişkenler		Veri Girişi				İstatistiksel Analizler
		Girilmedi		Girildi		
		N	%	N	%	
Saldırı Tekniği	Genel Oltalama	267[a]	37.0	33[b]	18.5	χ^2=21.853; p<0.001; Phi=0.156; Cramer's V=0.156
	Hedefli Oltalama	455[a]	63.0	145[b]	81.5	

Satırlardaki farklı harf sembolleri (a, b) kategorilerin 0.05 anlamlılık düzeyinde istatistiksel olarak birbirinden farklı olduğunu göstermektedir. Aynı harfe sahip değerler arasında anlamlı bir fark yokken, farklı harflere sahip değerler arasında istatistiksel olarak anlamlı bir fark vardır.

Tablo 4.9 incelendiğinde; veri girişi yapan kullanıcılar içerisinde genel oltalama oranının %18,5 (n=33), hedefli oltalama oranının ise %81,5 (n=145) olduğu görülmektedir. Ki-kare testi sonuçları, saldırı tekniği ile veri girişi durumu arasında istatistiksel olarak anlamlı bir ilişki olduğunu göstermektedir

($\chi^2 = 21{,}853$; df = 1; $p < 0{,}001$). Etki büyüklüğü değerleri (Phi=0,156; Cramer's V=0,156), bu ilişkinin küçük-orta düzeyde olduğunu göstermektedir.

Analiz sonuçları, $H1_0$ hipotezinin reddedildiğini ve $H1_1$ hipotezinin kabul edildiğini göstermektedir. Başka bir deyişle, genel oltalama ve hedefli oltalama teknikleri arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark vardır. Hedefli oltalama tekniği, genel oltalama tekniğine kıyasla daha yüksek bir başarı oranına sahiptir.

4.2.2 Otorite Türüne Göre Hipotez Testi

Bu bölümde, otorite türünün (bireysel ve kurumsal) sosyal mühendislik saldırılarının başarısı üzerindeki etkisi, önce genel olarak ve ardından ülkelere göre ayrı ayrı analiz edilmektedir. İkinci hipotez (H2), bireysel otorite ve kurumsal otorite temelli hedefli oltalama saldırıları arasında başarı oranında bir fark olup olmadığını ve ayrıca her iki ülkede ayrı ayrı test etmektedir.

- $H2_0$: Tüm katılımcı verileri birleştirildiğinde, bireysel ve kurumsal otorite temelli hedefli oltalama saldırıları arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark yoktur.
- $H2_1$: Türkiye'de, bireysel otorite figürlerini kullanan hedefli oltalama saldırıları, kurumsal otorite figürlerini kullananlardan daha başarılıdır.
- $H2_2$: Katar'da, kurumsal otorite figürlerini kullanan hedefli oltalama saldırıları, bireysel otorite figürlerini kullananlardan daha başarılıdır.

$H2_0$ hipotez testi, bireysel otorite figürlerini kullanan Deney Grubu A ile kurumsal otorite figürlerini kullanan Deney Grubu B arasındaki farklılıkları incelemektedir. $H2_1$ ve $H2_2$ hipotezleri, Türkiye ve Katar'da bireysel ve kurumsal otorite figürlerini kullanan hedefli oltalama saldırılarının başarı oranları arasındaki farklılıkları incelemektedir. Çalışmada saldırı başarısı, katılımcıların veri gönderim durumu (DataSubmissionStatus) ile ölçülmüştür. Hipotezi test etmek için Ki-kare bağımsızlık testi kullanılmıştır. Analiz sonuçları Tablo 4.10'da sunulmaktadır.

Tablo 4.10 Ülkeler Arasında Otorite Türüne Göre Veri Gönderim Durumunun Karşılaştırılması

Ülke	Değişken		Gruplar				İstatistiksel Analizler
			Deney-A: Bireysel		Deney-B: Kurumsal		
			N	%	N	%	
TOPLAM	Veri Gönderim Durumu	Gönderilmedi	227_a	75.7	228_a	76,0	χ^2=0,009; p=0,924 Phi=-0.004; Cramer's V=0.004
		Gönderildi	73_a	24.3	72_a	24,0	
Türkiye	Veri Gönderim Durumu	Gönderilmedi	105_a	70	122_b	81.3	χ^2=5,232; p=0,022 Phi=-0.132; Cramer's V=0.132
		Gönderildi	45_a	30	28_b	18.7	
Katar	Veri Gönderim Durumu	Gönderilmedi	122_a	81.3	106_b	70.7	χ^2=4.678; p=0,031 Phi=0.125; Cramer's V=0.125
		Gönderildi	28_a	18.7	44_b	29.3	

Satırlardaki farklı harf sembolleri (a, b) kategorilerin 0.05 anlamlılık düzeyinde istatistiksel olarak birbirinden farklı olduğunu göstermektedir. Aynı harfe sahip değerler arasında anlamlı bir fark yokken, farklı harflere sahip değerler arasında istatistiksel olarak anlamlı bir fark vardır.

Tablo 4.10 incelendiğinde; $H2_0$ hipotezine ilişkin bulgularda, veri gönderim oranının bireysel otorite figürlerini kullanan Deney Grubu A'da %24,3 (n=73) ve kurumsal otorite figürlerini kullanan Deney Grubu B'de %24,0 (n=72) olduğu görülmektedir. Ki-kare testi sonuçları, grup türü ile veri gönderim durumu arasında genel olarak istatistiksel olarak anlamlı bir ilişki olmadığını göstermektedir (χ^2 = 0,009; p = 0,924). Etki büyüklüğü değerleri (Phi=-0,004; Cramer's V=0,004), bu ilişkinin neredeyse var olmadığını göstermektedir. Bu bulgular ışığında, genel olarak (tüm katılımcı verileri birleştirildiğinde) $H2_0$ hipotezi kabul edilmektedir. Başka bir deyişle, genel olarak bireysel ve kurumsal

otorite temelli hedefli oltalama saldırıları arasında saldırı başarısı açısından istatistiksel olarak anlamlı bir fark yoktur.

Tablo 4.10'daki $H2_1$ hipotezine ilişkin bulgular, Türkiye'de bireysel otorite figürü kullanan Deney Grubu A'daki (%30,0, n=45) veri gönderim oranının, kurumsal otorite figürü kullanan Deney Grubu B'den (%18,7, n=28) daha yüksek olduğunu ve bu farkın istatistiksel olarak anlamlı olduğunu ortaya koymaktadır (χ^2=5,232; p=0,022). Etki büyüklüğü değerleri (Phi=-0,132; Cramer's V=0,132), bu ilişkinin küçük olduğunu göstermektedir. Bu bulgular ışığında, $H2_1$ hipotezi kabul edilmektedir. Başka bir deyişle, Türkiye'de bireysel otorite figürlerini kullanan hedefli oltalama saldırıları, kurumsal otorite figürlerini kullanan saldırılardan istatistiksel olarak anlamlı derecede daha başarılıdır.

Tablo 4.10'daki $H2_2$ hipotezine ilişkin bulgular, Katar'da kurumsal otorite figürlerini kullanan Deney Grubu B'deki (%29,3, n=44) veri gönderim oranının, bireysel otorite figürlerini kullanan Deney Grubu A'dan (%18,7, n=28) daha yüksek olduğunu ve bu farkın istatistiksel olarak anlamlı olduğunu göstermektedir (χ^2 = 4,678; p = 0,031). Etki büyüklüğü değerleri (Phi=0,125; Cramer's V=0,125), bu ilişkinin küçük olduğunu göstermektedir. Bu bulgular ışığında, $H2_2$ hipotezi kabul edilmektedir. Başka bir deyişle, Katar'da kurumsal otorite figürlerini kullanan hedefli oltalama saldırıları, bireysel otorite figürlerini kullanan saldırılardan istatistiksel olarak anlamlı derecede daha başarılıdır.

4.2.3 Ülke ve Otorite Türü Arasındaki Etkileşim Hipotezi Testi

Bu bölümde, farklı ülkelerde sosyal mühendislik saldırılarının başarısı üzerinde otorite türlerinin etkileşimini inceleyen H3 hipotezi test edilmektedir. Hipotezler aşağıdaki şekilde formüle edilmiştir:

- $H3_0$: Saldırı başarısı açısından ülke ve otorite türü arasında istatistiksel olarak anlamlı bir etkileşim yoktur.
- $H3_1$: Saldırı başarısı açısından ülke ve otorite türü arasında istatistiksel olarak anlamlı bir etkileşim vardır.

Hipotezi test etmek için ikili lojistik regresyon analizi kullanılmıştır. Analiz, veri gönderme durumunu (DataSubmissionStatus) bağımlı değişken

olarak, ülke (Country), otorite türü (Group) ve bu iki değişken arasındaki etkileşim terimini bağımsız değişkenler olarak içermektedir.

Omnibus testlerinin sonuçlarına göre, model istatistiksel olarak anlamlı bulunmuştur (χ^2 = 9.988, df = 3, p = .019). Model, bağımlı değişkendeki varyansın yaklaşık %2.5'ini açıklamaktadır (Nagelkerke R^2 = .025). Hosmer ve Lemeshow testi sonuçları, modelin veriye iyi uyum sağladığını göstermektedir (χ^2 = .000, p = 1.000).

Tablo 4.11 İkili Lojistik Regresyon Analiz Sonuçları

Değikenler	B	S.E.	Wald	Sig. (p)	Exp(B)	95% C.I.for EXP(B)	
						Lower	Upper
Ülke(1)	0,625	0,275	5,155	0,023	1.868	1,090	3,200
Grup(1)	0,593	0,276	4,616	0,032	1.809	1,060	3,080
Etkileşim Terimi	-1,217	0,390	9,763	0,002	0,296	0,138	0,635
Sabit	-1,472	0,210	49,33	0,000	0,230		

Bağımlı Değişken: *Veri Gönderim Durumu (0 = Gönderilmedi, 1 = Gönderildi)* ***B:*** *Regresyon katsayısı - Bağımsız değişkendeki bir birimlik değişimin bağımlı değişkenin log-odds'inde neden olduğu değişimi gösterir.* ***S.E.:*** *Standart hata - Regresyon katsayısı tahmininin kesinliğini ölçer. Daha düşük bir standart hata değeri, katsayı tahmininin daha güvenilir olduğunu gösterir.* ***Wald:*** *Wald istatistiği - Regresyon katsayısının istatistiksel olarak anlamlı olup olmadığını test eder. Yüksek bir Wald değeri ve düşük bir p değeri, değişkenin modele önemli bir katkı sağladığını gösterir.* ***Exp(B):*** *Odds oranı - Bağımsız değişkendeki bir birimlik artışın olayın gerçekleşme olasılığını kaç kat artırdığını/azalttığını gösterir. 1'den büyük değerler olasılığın arttığını, 1'den küçük değerler ise azaldığını gösterir.*

Tablo 4.11'de gösterilen lojistik regresyon analizi sonuçlarına göre, ülke değişkeni (B = 0.625, p = .023, Exp(B) = 1.868), otorite türü değişkeni (B = 0.593, p = .032, Exp(B) = 1.809) ve ülke ile otorite türü arasındaki etkileşim terimi (B = −1.217, p = .002, Exp(B) = 0.296) istatistiksel olarak anlamlı bulunmuştur.

Model, sonucu önemli ölçüde tahmin etmekte ve ülke, otorite türü ve bunların etkileşiminin dahil edilmesini desteklemektedir. Açıklanan varyans (Nagelkerke R^2 = 0.025) davranışsal araştırmalarda tipik olduğu gibi düşük

olmasına rağmen, model küçük etkilerin bile sosyal mühendislik saldırılarını anlamada önemli olduğunu göstermektedir. Mütevazı varyansla anlamlı sonuçların tespit edilmesi, kültürel olarak uyarlanabilir müdahalelerin geliştirilmesi ve bireysel ve bağlamsal faktörlerin ele alınması için çok önemlidir.

İstatistiksel olarak anlamlı etkileşim terimi ($p = .002$), $H3_1$ hipotezini desteklemekte ve boş hipotez $H3_0$'u reddetmektedir. Sonuç, sosyal mühendislik saldırılarının başarısının, ülke ve otorite türünün bağımsız etkilerinin ötesinde, bu iki faktörün etkileşimine bağlı olduğunu göstermektedir.

Anlamlı etkileşim terimi ($B = -1.217$), ülke ve otorite türü arasında "sinerjik" veya "güçlendirici" bir etki olduğunu düşündürmektedir. Bir ülkede kullanılan bir otorite türü, başka bir ülkede kullanıldığında farklı etkiler gösterebilmektedir. Başka bir deyişle, bir sosyal mühendislik saldırısında bir otorite türünün etkinliği, kültürel bağlama göre önemli ölçüde değişmektedir.

4.2.4 Davranışsal Geçiş İlişkisi Hipotezi Testi

Bu bölümde, kullanıcı davranışının sıralı doğasını inceleyen dördüncü hipotez (H4) test edilmektedir. H4 hipotezi, bir davranışa (bağlantıya tıklama) katılmanın, bir sonraki daha kritik adıma (hassas veri gönderme) geçme olasılığını önemli ölçüde artırıp artırmadığını incelemektedir.

- $H4_0$: Oltalama bağlantısına tıklama ile veri gönderme davranışı arasında istatistiksel olarak anlamlı bir ilişki yoktur.
- $H4_1$: Oltalama bağlantısına tıklayan çalışanlar, tıklamayanlara göre veri gönderme olasılığı önemli ölçüde daha yüksektir.

Hipotezi test etmek için Ki-kare bağımsızlık testi kullanılmıştır. Bu analiz, bağlantı tıklama durumu (LinkClickedStatus) ile veri gönderme durumu (DataSubmissionStatus) arasındaki ilişkiyi incelemektedir. Analiz sonuçları Tablo 4.12'de sunulmaktadır.

Tablo 4.12 Oltalama Bağlantısına Tıklama Durumu ile Veri Gönderme Davranışı Arasındaki İlişki

Değişkenler		Veri Gönderme Durumu				İstatistiksel Analizler
		Gönderilmedi		Gönderildi		
		N	%	N	%	
Bağlantıya Tıklama Durumu	Tıklanmadı	554[a]	76.6	0[b]	0.0	χ^2=352.786; p<0.001 Phi=0. 626 Cramer's V=0. 626
	Tıklandı	169[a]	26.4	177[b]	100.0	

Satırlardaki farklı harf sembolleri (a, b) kategorilerin 0.05 anlamlılık düzeyinde istatistiksel olarak birbirinden farklı olduğunu göstermektedir. Aynı harfe sahip değerler arasında anlamlı bir fark yokken, farklı harflere sahip değerler arasında istatistiksel olarak anlamlı bir fark vardır.

Tablo 4.12 incelendiğinde; oltalama bağlantısına tıklayan 346 katılımcıdan 177'sinin (%51,2) veri gönderdiği, 169'unun (%48,8) ise göndermediği gözlemlenmektedir. Ki-kare testi sonuçları, bağlantıya tıklama ile veri gönderme arasında istatistiksel olarak anlamlı ve güçlü bir ilişki olduğunu göstermektedir (χ^2=352,786, df=1, p<0,001). Etki büyüklüğü değerleri (Phi=0,626; Cramer's V=0,626) büyük bir ilişkiyi göstermektedir.

Bu bulgular, $H4_0$'ın reddedilmesine ve $H4_1$'in kabul edilmesine yol açmaktadır. Başka bir deyişle, oltalama bağlantısına tıklayan çalışanların, tıklamayanlara göre veri gönderme olasılığı önemli ölçüde daha yüksektir.

SONUÇ VE ÖNERİLER

Bu çalışmada, Türkiye ve Katar'daki elektrik dağıtım şirketlerinde çalışan bireylerin farklı otorite figürlerine (bireysel ve kurumsal) dayalı sosyal mühendislik saldırılarına verdikleri tepkileri incelenmiştir. Sonuçlar, hem saldırı tekniğinin hem de kültürel bağlamdaki otorite figürlerinin sosyal mühendislik saldırılarının başarısında önemli bir rol oynadığını göstermektedir.

H1 için elde edilen sonuçlar, hedefli oltalama (spear phishing) saldırılarının genel oltalama (generic phishing) saldırılarından istatistiksel olarak anlamlı derecede daha başarılı olduğunu göstermektedir. Bu durum, kişiselleştirilmiş saldırı vektörlerinin genel tehditlere göre daha etkili olmaya devam ettiğini göstermektedir. Xu ve arkadaşları, kişiselleştirilmiş bilgi kullanan oltalama saldırılarının kişiselleştirilmemiş saldırılara göre 2,97 kat daha etkili olduğunu bulmuşlardır (Xu vd., 2023). Benzer şekilde, Rizzoni ve arkadaşları büyük bir hastanede bir oltalama simülasyonu gerçekleştirmiş ve özelleştirilmiş oltalama e-postalarının standart oltalama e-postalarına kıyasla daha yüksek bir başarı oranına sahip olduğunu tespit etmişlerdir (Rizzoni vd., 2022). İlk uygulamada, personelin %64'ü genel oltalama e-postalarını açmazken, özelleştirilmiş oltalama e-postalarını açmayanların oranı sadece %38 olmuştur. Saldırganlar, hedefleri hakkında topladıkları kişisel bilgileri kullanarak bağlamsal olarak anlamlı kimlik taklitleri ve anlatılar oluşturarak hedefli oltalama saldırılarının başarısını elde etmektedirler (Xu vd., 2023). Bu tür saldırılarda, saldırganlar hedeflenen kişi tarafından güvenilen bir kaynaktan geliyormuş gibi görünen e-postalar kullanarak başarı şansını artırmaktadırlar (Lin vd., 2019). Burrell, saldırganların özellikle üst düzey yöneticileri hedefleyen balina avcılığı (whaling) olarak bilinen oltalama türünde otorite yanlılığını ve kurumsal güveni istismar ettiklerini belirtmektedir (Burrell, 2024).

H2 için elde edilen sonuçlar, otorite türünün sosyal mühendislik saldırılarının başarısı üzerindeki etkisinin kültürel bağlama göre farklılık gösterdiğini ortaya koymaktadır. Türkiye'de, sonuçlar bireysel otorite figürlerine

dayalı hedefli oltalama saldırılarının kurumsal otorite figürlerine dayalı saldırılardan daha başarılı olduğunu gösterirken, Katar'da tam tersi bir eğilim görülmüştür. Türk kültüründeki orta-yüksek güç mesafesi ve kurumlara duyulan güven endeksinin düşük olması, bireysel otorite figürlerinin Türkiye'de neden daha etkili olduğunu açıklamaktadır. Hofstede'nin kültürel boyutlar teorisine göre, Türkiye orta-yüksek güç mesafesi değerine sahiptir ve bu durum hiyerarşik yapıların önemli kabul edildiği ve otorite figürlerine saygının değerli olduğu bir kültürel ortamı yansıtmaktadır (Hofstede, 2015). Bununla birlikte, Türkiye'deki nispeten düşük kurumsal güven düzeyi, bireysel ilişkilere ve kişisel bağlantılara daha fazla önem verilmesine yol açabilmektedir. Bu nedenle, bireysel otorite figürlerine dayalı sosyal mühendislik saldırıları Türkiye'de daha etkili olabilmektedir. Katar'da, kurumsal otorite figürleri daha etkilidir ve bu durum Katar'ın yüksek güç mesafesi değeri ve kurumlara duyulan güven endeksinin yüksek olması ile ilişkilendirilebilinir. Kültürel bağlamın sosyal mühendislik saldırılarının etkinliğini şekillendirdiği ve farklı toplumların otoriteyi farklı algıladıklarını gösteren sonuçlar mevcut literatürle uyumludur. Tiwari, otorite ilkesinin oltalama saldırılarında önemli bir ikna mekanizması olarak hizmet ettiğini ve saldırganların insanların otoriteye itaat etme eğilimini istismar ettiğini belirtmektedir (Tiwari, 2020). Özellikle belirgin hiyerarşik yapılara sahip kültürlerde, insanlar otorite figürlerinin taleplerine uyma konusunda daha yüksek bir eğilim gösterebilmektedirler. Rocha Flores ve arkadaşları, oltalama saldırılarına karşı direncin ulusal kültüre göre farklılık gösterdiğini bulmuşlardır. Araştırmacılar, İsveç, ABD ve Hindistan'daki çalışanların oltalama davranışları arasında önemli farklılıklar tespit etmişlerdir (Rocha Flores vd., 2015).

H3 için elde edilen sonuçlar, ülke ve otorite türü arasında istatistiksel olarak anlamlı bir etkileşim olduğunu göstermektedir. Bu bulguya göre, bir otorite türünün etkinliği kültürel bağlama göre değişebilmektedir. Lojistik regresyon analizi sonuçları, ülke değişkeninin, otorite türü değişkeninin ve bu iki değişken arasındaki etkileşim teriminin istatistiksel olarak anlamlı olduğunu göstermektedir. Anlamlı etkileşim terimi ($B = -1.217$), ülke ve otorite türü arasında "sinerjik" veya "güçlendirici" bir etki olduğunu düşündürmektedir. Bir

ülkede kullanılan bir otorite türü, başka bir ülkede kullanıldığında farklı etkiler gösterebilmektedir. Başka bir deyişle, bir sosyal mühendislik saldırısında bir otorite türünün etkinliği, kültürel bağlama göre önemli ölçüde değişmektedir. Bu durum, Hofstede'nin kültürel boyutlar teorisi ile ilişkilendirilebilmektedir. Özellikle güç mesafesi boyutu, bir toplumda otoriteye verilen önem derecesini belirlemektedir (Rocha Flores vd., 2015). Yüksek güç mesafesine sahip kültürler otoriteye daha fazla saygı ve itaat gösterme eğilimindeyken, düşük güç mesafesine sahip kültürler otoriteye karşı daha sorgulayıcı bir yaklaşım gösterme eğilimindedirler. Bulgular, Rocha Flores ve arkadaşlarının çalışmasıyla da uyumludur (Rocha Flores vd., 2015). Bu çalışmada, araştırmacılar farklı ulusal kültürlerin oltalama saldırılarına karşı direnci etkilediğini ve bu etkinin kültürel boyutlarla ilişkili olduğunu belirtmişlerdir. Benzer şekilde, diğer çalışmalarda da kültürel farklılıkların bilgi güvenliği davranışlarını etkilediğini belirtilmektedir (Bayl-Smith vd., 2022; Kim ve Kim, 2013).

H4 için elde edilen sonuçlar, oltalama bağlantısına tıklama davranışı ile veri gönderme davranışı arasında istatistiksel olarak anlamlı ve güçlü bir ilişki olduğunu göstermektedir. Bir oltalama bağlantısına tıklayan çalışanlar, tıklamayanlara göre veri gönderme olasılığı önemli ölçüde daha yüksektir. Bu bulgu, sosyal mühendislik saldırılarında kullanıcı davranışının sıralı bir doğaya sahip olduğunu ve bir davranışın bir sonraki davranışı etkileyebileceğini göstermektedir. Bu bulgu, literatürdeki çeşitli çalışmalarla tutarlıdır. Abroshan ve arkadaşları çalışmalarında, oltalama sürecinin farklı aşamalardan oluştuğunu ve kullanıcıların her aşamada farklı davranışsal tepkiler gösterdiğini belirtmişlerdir (Abroshan vd., 2021). Söz konusu çalışmada, araştırmacılar oltalama saldırısının başında kullanıcının e-postayı açması, ardından bağlantıya tıklaması ve son olarak kişisel bilgileri paylaşması şeklinde ilerleyen bir süreç tanımlamışlardır. Bu süreçte, araştırmacılar bir aşamayı tamamlayan kullanıcıların bir sonraki aşamaya geçme olasılığının daha yüksek olduğunu gözlemlemişlerdir. Greitzer ve arkadaşları deneysel araştırmalarında, kullanıcı davranışının oltalama saldırısının farklı aşamalarında tutarlı kaldığını ve bir

aşamada güvenlik açıkları sergileyen kullanıcıların sonraki aşamalarda benzer güvenlik açıkları sergileme eğiliminde olduklarını belirtmişlerdir (Greitzer vd., 2021).

Bu bulgular, sosyal mühendislik saldırıları sırasında tam davranış dizisini ele alan önleyici karşı önlemlerin tasarlanmasının gerekliliğini ortaya koymaktadır. Bu önlemler, yalnızca ilk etkileşime (örneğin, bağlantıya tıklama) odaklanmak yerine, davranışsal tırmanmayı önlemek için kullanıcıların ilk temastan sonra da tetikte kalmalarını sağlamalıdır. Erken aşama müdahaleleri gerekli olmaya devam etmektedir; ancak, sonuçlar davranışsal tırmanmayı önlemek için ilk temastan sonra kullanıcıların tetikte kalmasını sürdürmenin de eşit derecede önemli olduğunu göstermektedir. Bu sıralı güvenlik açığı yolunun kapsamlı bir şekilde anlaşılması, oltalama saldırı döngüsünü önemli güvenlik ihlallerine dönüşmeden önce etkili bir şekilde kesintiye uğratabilecek çok katmanlı, aşamaya özgü savunma mekanizmalarının geliştirilmesi için esastır.

Ampirik bulgulara ek olarak, sonuçlar aynı zamanda siber güvenlik bağlamlarında kullanıcı davranışına ilişkin teorik çıkarımlar da sunmaktadır. Özellikle, gözlemlenen sıralı tırmanma, tehdit değerlendirmesi (algılanan güvenlik açığı ve ciddiyeti) ve başa çıkma değerlendirmesinin (öz-yeterlilik ve yanıt etkinliği) oltalama saldırısının her aşamasında davranışı dinamik olarak etkilediği Koruma Motivasyonu Teorisi (PMT) ile uyumludur (Rogers, 1975). Ayrıca, bulgular Planlı Davranış Teorisi (TPB) ile de uyumludur ve başlangıç davranışsal niyetlerinin (bir e-postayı açmak gibi) sosyal mühendislik baskısı altında sonraki riskli davranışları (veri gönderimi gibi) önemli ölçüde öngörebileceğini göstermektedir (Ajzen, 1991). Gelecekteki çalışmalar, siber güvenlik davranış araştırmalarında teori oluşturmayı ilerletmek için bu ilişkileri daha kapsamlı olarak modelleyebilir.

Bu çalışmada, Türkiye ve Katar'daki elektrik dağıtım şirketlerinde çalışan bireylerin farklı otorite figürlerine (bireysel ve kurumsal) dayalı sosyal mühendislik saldırılarına verdikleri tepkiler incelenmiştir. Sonuçlar, hem saldırı türünün hem de otorite figürlerinin kültürel bağlamının sosyal mühendislik saldırılarının etkinliğini belirlemede kritik öneme sahip olduğunu göstermiştir.

Hedefli oltalama (spear phishing) saldırılarının, genel oltalama (generic phishing) saldırılarına göre önemli ölçüde daha etkili olduğu tespit edilmiş olup, bu durum kişisel saldırı vektörlerinin oluşturduğu artan riski ortaya koymaktadır. Ayrıca, otorite türünün etkisinin kültürler arasında farklılık gösterdiği belirlenmiştir. Türkiye'de bireysel otorite figürleri daha ikna edici bulunurken, Katar'da kurumsal otoritelerin daha etkili olduğu görülmüştür. Ülke ve otorite türü arasındaki etkileşim etkisi, güç mesafesi ve kurumlara duyulan güven endeksi gibi kültürel boyutların sosyal mühendislik güvenlik açıklarını analiz ederken kontrol edilmesi gerektiğini göstermektedir.

Son olarak, kullanıcı davranışının sıralı doğası doğrulanmış ve oltalama bağlantısı ile etkileşimin sonraki veri gönderimine güçlü bir şekilde işaret ettiği tespit edilmiştir. Bu bulgular, güvenliğin bir giriş noktasında ihlal edilmesinin ardından, kullanıcıların daha ileri ve derin sömürüye karşı güçlü bir şekilde savunmasız kaldığını göstermektedir.

Genel olarak, bu çalışma sosyal mühendislik saldırılarına karşı kültürel olarak uyarlanabilir ve davranışsal olarak bilgilendirilmiş savunma alışkanlıkları geliştirmenin gerekliliğini ortaya koymakta ve genel farkındalık programlarından kültürel ve davranışsal olarak uyarlanmış güvenlik müdahalelerine doğru bir evrim öngörmektedir. Organizasyonlar, siber güvenlik farkındalık programlarını yalnızca saldırı tipolojilerine göre değil, aynı zamanda otoriteye, uyumluluğa ve kurumsal güven dinamiklerine yönelik ulusal kültürel yatkınlıkları da dikkate alarak uyarlamalıdır. Güvenlik farkındalık girişimlerinin kültürel olarak uyarlanmaması, kuruluşları gelişen sosyal mühendislik tehditlerine karşı orantısız bir şekilde savunmasız bırakabilmektedir.

Gelecek araştırmalarda, sosyal mühendislik saldırılarına karşı duyarlılığı etkileyen ek kültürel ve psikolojik faktörlerin incelenmesi düşünülebilir. Özellikle, Hofstede'nin kültürel çerçevesinin bireycilik-toplulukçuluk, erillik-dişilik ve belirsizlikten kaçınma gibi diğer boyutlarının incelenmesi, kültürel etkilerin güvenlik davranışları üzerindeki etkisine dair daha ayrıntılı bir anlayış sağlayabilir.

Gelecekteki çalışmalarda, güç mesafesi ve kurumsal güven üzerinde münhasır bir odaklanmadan kaçınılmalıdır. Belirsizlikten kaçınma, toplulukçuluk ve erillik-dişilik dahil olmak üzere daha geniş kültürel boyutlar, kullanıcıların otoriteye dayalı oltalama girişimlerine karşı duyarlılığını kritik şekilde düzenleyebilmektedir ve gelecekteki karşılaştırmalı analizlere sistematik olarak dahil edilmelidir.

Ayrıca, gelecekteki araştırmalarda, sıralı davranışsal güvenlik açıklarının PMT (Koruma Motivasyonu Teorisi) ve TPB (Planlanmış Davranış Teorisi) gibi yerleşik psikolojik çerçeveler aracılığıyla formal olarak modellenmeye çalışılması düşünülebilir. Ek olarak, gelecekteki çalışmalarda, başlangıç bağlantı etkileşimi ile sonraki veri ifşa davranışları arasındaki geçiş olasılıklarını ölçerek sıralı karar verme modellerinin ampirik olarak doğrulanması sağlanabilir. Böyle bir çalışma, oltalama saldırılarındaki tırmanma dinamiklerini tahmin etmek için daha güçlü bir teorik temel oluşturulmasına yardımcı olacaktır.

Bunun yanında, gelecekteki araştırmalarda, risk algısı, karar verme stilleri (örneğin, sezgisel ve analitik düşünme) ve bilişsel önyargılar gibi bireysel düzeydeki faktörlerin oltalama saldırılarına kurban gitme olasılığını nasıl etkilediği de incelenebilir. Bu psikolojik mekanizmaların araştırılması, kişiselleştirilmiş müdahalelerin tasarlanmasına yönelik daha derin bulgular sunabilir.

Gelecekteki araştırmalarda, özellikle üst düzey yöneticileri hedef alan, balina avı (whaling) simülasyonları da dahil olmak üzere kontrollü deneysel tasarımlar geliştirilebilir ve böylece organizasyonlardaki hiyerarşik güvenlik açıklarının daha iyi anlaşılması sağlanabilir. Yöneticilerin katılımı, siber güvenlik dayanıklılığı üzerindeki yukarıdan aşağıya etkilere ilişkin bilgi birikimindeki önemli bir boşluğun doldurulmasına yardımcı olacaktır.

Bulguların genellenebilirliğini artırmak için, gelecekteki araştırmalar elektrik dağıtımı dışında finans, sağlık, eğitim ve kamu kurumları gibi çeşitli sektörleri de kapsayacak şekilde genişletilebilir. Ayrıca, çalışmalar özellikle güç mesafesi ve kurumsal güven boyutları açısından farklı kültürel profillere sahip daha fazla sayıda ülkeyi kapsayabilir.

Ek olarak, gelecekteki çalışmalarda, rastgele katılımcı seçim yöntemleri kullanılarak potansiyel örnekleme yanlılıklarının azaltılması hedeflenebilir. Ayrıca, sektörler ve organizasyon büyüklükleri arasında orantılı temsili sağlamak için tabakalı örnekleme teknikleri kullanılabilir, böylece sektöre özgü yanlılıklar en aza indirilerek sonuçların geçerliliği artırılabilir. Farklı sektörler ve bölgeler genelinde organizasyonel çeşitliliğin genişletilmesi, sonuçların genellenebilirliğini ve sağlamlığını daha da güçlendirecektir.

Son olarak, nicel oltalama simülasyon verileri ile nitel görüşmeleri birleştiren karma yöntem araştırma yaklaşımlarının benimsenmesi, sosyal mühendislik girişimlerine verilen tepkilerin altında yatan bilişsel, duygusal ve organizasyonel faktörler hakkında daha ayrıntılı bulgular sağlayabilir.

KAYNAKLAR

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.* https://doi.org/10.1109/ACCESS.2021.3066383

Aldawood, H. ve 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

Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M., & Mahalle, P. (2023). Defending against vishing attacks: A comprehensive review for prevention and mitigation techniques. *In International Conference on Recent Developments in Cyber Security (pp. 411-422).* Singapore: Springer Nature Singapore.

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2022). Response to a phishing attack: persuasion and protection motivation in an organizational context. *Information & Computer Security, 30*(1), 63-78. https://doi.org/10.1108/ICS-02-2021-0021

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). A comprehensive survey of social engineering attacks: Taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research, 20*(2), 244-292. https://doi.org/10.1080/19361610.2024.2372986

Bose, I., & Leung, A. C. M. (2007). Unveiling the mask of phishing: Threats, preventive measures, and responsibilities. *Communications of the Association for Information Systems*, *19*(1), 544-566.

Brehm, J. W. (1966). *A theory of psychological reactance*. New York.

Brewer, P. ve Venaik, S. (2011). Individualism–collectivism in Hofstede and GLOBE. *Journal of International Business Studies*, *42*(3), 436-445.

Bujold, L. McM. (2002). *Diplomatic immunity* (Cilt 14). Baen Books.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, 15(1), 20-45.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2015). The persuasion and security awareness experiment: reducing the success of

social engineering attacks. *Journal of Experimental Criminology*, 11, 97-115.

Burger, J. M. (2009). Replicating Milgram: Would people still obey today? *American Psychologist*, 64(1), 1-11.

Burrell, D. N. (2024). *Exploring the cyberpsychology and criminal psychology of whaling and spear fishing on-line attacks*. RAIS Conference Proceedings, November 21-22, 2024, 114-123. DOI:10.5281/zenodo.14514640

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. https://doi.org/10.1016/j.eswa.2018.03.050

Choo, E. Y. (2021). A review of culture and leadership in cross-cultural context: Linking Hofstede's theory. *World Academics Journal of Management, 9*(3), 33-36.

Cialdini, R. B. (2009). *Influence: science and practice* (5. baskı). Pearson.

Cialdini, R. B., ve Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, 55, 591-621.

Conteh, N. Y. ve Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31-38. https://doi.org/10.19101/IJACR.2016.623006

CSO Online. (2013). The Ultimate Guide to Social Engineering. Erişim tarihi: 2013-06-19. http://www.csoonline.com/article/701042/cso-s-ultimate-guide-to-social-engineering

Darmawati, B., Murmahyati, & Herlina, A. (2019). Bugis cultural taxonomy: An overview of Hofstede's cultural dimension. *Advances in Social Science, Education and Humanities Research, 349*, 108-110.

Darwish, A., El Zarka, A., & Aloul, F. (2013). Towards understanding phishing victims' profile. *International Conference on Computer Systems and Industrial Informatics*, 1-5.

Desetty, A. G., Jangampet, V. D., & Pulyala, S. R. (2020). Phishing attacks: Evolving techniques, emerging trends, and countermeasure strategies. *International Journal for Innovative Engineering and Management Research*, *9*(12), 985-991.

Eftimie, S., Moinescu, R., & Răcuciu, C. (2022). *Spear-phishing susceptibility stemming from personality traits*. IEEE Access, 10, 73548-73559. https://doi.org/10.1109/ACCESS.2022.3190009

Festinger, L., ve Carlsmith, J. M. (1959). Cognitive consequences of forced compliance. *Journal of Abnormal and Social Psychology*, 58(2), 203-210.

Galadima, S. A., Shrivastava, M., & Sonowal, G. (2024). QR code phishing: A review of the current attacks and countermeasures. JuniKhyat, 14(9), 1-6.

Greenspan, S. (2008). *Annals of Gullibility: Why We Get Duped and How to Avoid It*. Bloomsbury Publishing USA.

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). *Experimental investigation of technical and human factors related to phishing susceptibility*. ACM Transactions on Social Computing, 4(2), 1-48. https://doi.org/10.1145/3461672

Guadagno, R., ve Cialdini, R. B. (2005). Online persuasion and compliance: Social influence on the Internet and beyond. *The social net: Human behavior in cyberspace*, 91-113.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2. baskı). Wiley.

Hatfield, J. M. (2017). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Hofstede Insights. (2023). Country Comparison Tool. https://www.hofstede-insights.com/country-comparison-tool

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations* (2. baskı). Thousand Oaks, CA: Sage Publications.

Hofstede, G. (2015). *The Hofstede Centre: Strategy, culture, change*. Helsinki: The Hofstede Centre.

Ivaturi, K. ve Janczewski, L. (2011). A taxonomy for social engineering attacks. *International Conference on Information Resources Management*, 1-12.

Jain, V., Pandey, B., Aldasheva, L., Shukla, P., Pandey, P., & Jain, D. (2025). A Comprehensive Usage of AI in Prevention of Social Engineering Attack. In *2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 668-673). IEEE.

Jari, M. (2022). An overview of phishing victimization: Human factors, training and the role of emotions. *arXiv preprint arXiv:2209.11197*.

Khadka, K., Ullah, A. B., Ma, W., Marroquin, E. M., & Alem, Y. (2023). A survey on the principles of persuasion as a social engineering strategy in phishing. *IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1631-1638.

Krombholz, K., Hobel, H., Huber, M. ve Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, 48, 101343.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). *Susceptibility to spear-phishing emails: Effects of internet user demographics and email content*. ACM Transactions on Computer-Human Interaction, 26(5), 1-28. https://doi.org/10.1145/3336141

Longtchi, T. T., Rodriguez, R. M., Al-Shawaf, L., Atyabi, A., & Xu, S. (2024). Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey. *Proceedings of the IEEE*, 112(3), 18-9219.

Malik, M. S. M. (2020). A Brief Overview of Social Engineering. *International Journal for Electronic Crime Investigation*, *4*(1), 5-5.

Milgram, S. (1963). Behavioral study of obedience. *The Journal of Abnormal and Social Psychology*, 67(4), 371-378.

Milgram, S. (1965). Some conditions of obedience and disobedience to authority. *Human Relations*, 18(1), 57-76.

Mouton, F., Leenen, L. ve Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209. https://doi.org/10.1016/j.cose.2016.03.004

Muscanell, N. L., Guadagno, R. E., & Murphy, S. (2014). Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass*, 8(7), 388-396.

Nurse, J. R. C. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *The Oxford Handbook of Cyberpsychology*, 663-690.

Packer, D. J. (2008). Identifying systematic disobedience in Milgram's obedience experiments: A meta-analytic review. *Perspectives on Psychological Science*, 3(4), 301-304.

Papathanasiou, A., Liontos, G., Liagkou, V., & Glavas, E. (2023). Business email compromise (BEC) attacks: threats, vulnerabilities and countermeasures—a perspective on the greek landscape. *Journal of Cybersecurity and Privacy*, *3*(3), 610-637.

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, 1-13. https://doi.org/10.1177/20552076221081716

Rocha Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security, 23*(2), 178-199. https://doi.org/10.1108/ICS-05-2014-0029

Schumacher, S. (2011). Die psychologischen Grundlagen des Social Engineerings. *Magdeburger Journal zur Sicherheitsforschung*, 1, 1-26.

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, 12(12), 6042.

Smith, P. B. ve Bond, M. H. (1998). *Social psychology across cultures* (2. baskı). Prentice Hall.

Tiwari, P. (2020). *Exploring phishing susceptibility attributable to authority, urgency, risk perception and human factors* [Master's Thesis]. Purdue University.

Tukur, M. N., & Adam, S. I. (2017). Culture and entrepreneurship: An overview of Hofstede's cultural dimensions. *Dynamic Research Journals of Economics and Finance, 2*(7), 17-21.

Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annual Review of Psychology*, 57, 375-400.

Uebelacker, S., & Quiel, S. (2014). The social engineering personality framework. *Workshop on Socio-Technical Aspects in Security and Trust*, 24-30.

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access*, 8, 85094-85115. https://doi.org/10.1109/ACCESS.2020.2992807

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9, 11895-11910. https://doi.org/10.1109/ACCESS.2021.3051633

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806-820.

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16*(5), 463-483.

Xu, T., Singh, K., & Rajivan, P. (2023). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. *Applied Ergonomics*, 108, 103908. https://doi.org/10.1016/j.apergo.2022.103908

Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. *Security and Privacy*, *2*(4), e73.

ÖZGEÇMİŞ