Kişisel verilerimiz için büyük bir tehdit; “Oltalama”

Mehmet Efe MENGAASLAN, Utku YILDIZ, Doruk TATLISU, Emir ÇUKUR

İbrahim Turhan Anadolu Lisesi, 9. Sınıf, İstanbul

İbrahim Turhan Anadolu Lisesi, 9. Sınıf, İstanbul

İbrahim Turhan Anadolu Lisesi, 9. Sınıf, İstanbul

İbrahim Turhan Anadolu Lisesi, 9. Sınıf, İstanbul

Özet

Günümüzde hızla dijitalleşen dünyada, teknolojinin hayatımıza entegrasyonu arttıkça kişisel veri güvenliği kritik bir sorun haline gelmiştir. Özellikle oltalama gibi sosyal mühendislik saldırıları, bireylerin insanî zafiyetlerini hedef alarak dijital güvenliği tehlikeye atmaktadır. Merak, acelecilik, güvenme eğilimi ve dikkat dağınıklığı gibi insana özgü zaaflar, bu saldırıların başarı oranını artırmaktadır. Oltalama saldırıları genellikle bireylerin dijital ayak izlerinden faydalanır; sosyal medya hesaplarından, çevrimiçi alışveriş alışkanlıklarından ve diğer internet aktivitelerinden toplanan veriler, kişiye özel ve inandırıcı saldırılar düzenlenmesini kolaylaştırır. Bu durum, kullanıcıların dijital izlerini farkında olmadan nasıl genişlettiğini ve bunu nasıl kötüye kullanılabilir hale getirdiğini göstermektedir. Dijital ayak izinin kontrolsüz büyümesi, yalnızca bireylerin değil, aynı zamanda şirketlerin ve toplulukların da güvenliğini riske atmaktadır. İki faktörlü kimlik doğrulama, güçlü şifre yönetimi ve güvenlik yazılımlarının kullanımı gibi teknolojik çözümler bu sorunu hafifletmeye yardımcı olsa da tamamen ortadan kaldırmak imkânsıza yakındır. Çünkü insan zafiyeti teknolojik çözümleri devre dışı bırakabilecek kadar güçlüdür; zafiyetlerini en aza indirgeyebilecek farkındalık eğitimlerini ve teknolojik önlemleri bir araya getirerek bireylerin bu tehditlere karşı nasıl daha dirençli hale gelebileceğini incelemektedir. Dijitalleşmenin kaçınılmaz olduğu bu çağda, yalnızca teknolojiyi değil, insanı da merkeze alan bir yaklaşım geliştirilmesi şarttır. Bu çerçevede, bilinçlendirme kampanyalarının yanı sıra, bireylerin dijital davranışlarını daha sorumlu bir şekilde yönetmeleri gerektiği savunulmaktadır. Ancak, dijital izlerin tamamen silinemez oluşu ve insana özgü zaafların her zaman var olması, veri güvenliğini sağlamanın çok boyutlu ve sürekli bir mücadele olduğunu kanıtlamaktadır.

Anahtar Kavramlar:

Sosyal mühendislik saldırıları

Dijital ayak izi yönetimi

İnsan zafiyetleri ve güvenlik

Farkındalık eğitimlerinin önemi

1. Giriş

Günümüzde hızla dijitalleşen dünyada, teknolojinin hayatımıza entegrasyonu arttıkça kişisel veri güvenliği kritik bir sorun haline gelmiştir. Özellikle oltalama gibi sosyal mühendislik

saldırıları, bireylerin insana özgü zafiyetlerini hedef alarak dijital güvenliği tehlikeye atmaktadır. Oltalama saldırıları, sosyal medya hesapları, çevrimiçi alışveriş alışkanlıkları ve diğer internet aktiviteleri gibi bireylerin dijital ayak izlerinden faydalanarak kişiye özel ve inandırıcı yöntemlerle gerçekleştirilir. (Çallı, Y. (2024) *Dijital Ayak İzi Nedir? Dijital Ayak İzini Azaltmanın Yolları Nelerdir?,* 1 Şubat 2025 tarihinde https://berqnet.com/blog/dijital-ayak-izi adresinden alındı.)

Bu çalışma, bireylerin farkında olmadan dijital ayak izlerini nasıl genişlettiğini, bunun güvenlik açısından doğurduğu tehlikeleri ve bu sorunun çözümüne yönelik yaklaşımları ele almayı amaçlamaktadır. Çalışmadan bireyler, kurumlar ve topluluklar yararlanabilir. Ayrıca bu araştırma, teknolojik önlemlerin yanı sıra insan odaklı farkındalık eğitimlerini de ön plana çıkarması açısından yenilikçi bir perspektif sunmaktadır.

2. Araştırmanın Amacı

Bu araştırmanın amacı, dijital ayak izlerini kontrol altına alarak bireylerin ve kurumların dijital güvenliğini artırmaktır. Bu kapsamda, insan zafiyetlerini azaltmayı hedefleyen farkındalık eğitimleri ile iki faktörlü kimlik doğrulama ve güçlü şifre yönetimi gibi teknolojik çözümlerin etkisi incelenmektedir.

Araştırma, bireylerin dijital davranışlarını daha sorumlu bir şekilde yönetmelerine katkı sağlamayı, dijital tehditlere karşı daha dirençli olmalarını mümkün kılmayı hedeflemektedir. Ayrıca, dijital izlerin tamamen silinemez olması ve insan zafiyetlerinin tamamen ortadan kaldırılamayacağı gerçeğinden yola çıkarak, veri güvenliğinin çok boyutlu bir mücadele gerektirdiğini vurgulamaktadır.

3. Yöntem

Bu araştırma, dijital güvenlik ve oltalama saldırılarının farkındalığını artırmaya yönelik bir kuramsal araştırma olarak planlanmıştır. Araştırmanın ana kitlesi, dijital güvenlik hakkında bilgi edinmek isteyen ve dijital ortamda aktif olan genel internet kullanıcılarıdır. Ancak, bu çalışmada gerçek veri toplama yapılmayacak, bunun yerine daha önce yapılmış ve güvenilir kaynaklardan elde edilen veriler kullanılacaktır. Literatür taraması yapılarak, dijital güvenlik ve oltalama saldırıları konusundaki mevcut çalışmalar ve araştırmalar incelenecek, elde edilen bulgular analiz edilecektir.

Araştırmanın modeli betimsel araştırma modeli olup, dijital güvenlik ve oltalama saldırılarının nasıl işlendiği ve bu konularda bireylerin farkındalık düzeylerinin arttırılabileceği üzerine bir inceleme yapılacaktır. Bu model, dijital güvenlik ile ilgili çeşitli çalışmaları analiz ederek, bu alandaki bilgi eksikliklerini ve iyileştirme alanlarını belirlemeyi amaçlamaktadır. Ölçekler kullanılmayacak, çünkü bu araştırma daha çok bilgi toplama ve mevcut verileri analiz etme temellidir. Ancak, araştırmada kullanılan veriler ve bulgular, dijital güvenlik konusundaki farkındalığı ölçen daha önceki anketler ve araştırmalardan alınan verilerle desteklenecektir.

Veri toplama araçları olarak, güvenilir internet kaynakları, akademik makaleler ve güvenlik üzerine yazılmış kitaplar gibi literatür taraması yapılacaktır. Bu kaynaklar, dijital güvenlik ve oltalama saldırıları hakkında yapılmış önceki çalışmalardan elde edilen verilerden faydalanarak bilgi sağlamak için kullanılacaktır. Ayrıca, görüşme ve anket yapılmayacaktır, çünkü bu çalışma daha çok teorik bilgiye dayalıdır ve uygulamalı veri toplamayı içermemektedir.

Araştırma sürecinde, literatür taraması ile elde edilen bilgiler, dijital güvenlik ve oltalama saldırıları hakkında yapılan araştırmaların sonuçlarıyla karşılaştırılacak ve analiz edilecektir.

Bu analizler, dijital güvenlik konusunda bireylerin nasıl daha bilinçli hale gelebileceği, oltalama saldırılarının etkilerini azaltmak için neler yapılabileceği gibi önemli başlıkları ele alacaktır.

Veri analizi kısmında, toplanan veriler üzerinde yapılan literatür taraması ve incelemeler sonucunda dijital güvenlik alanındaki mevcut durum değerlendirilecektir. Bu değerlendirme, dijital güvenliğin önemi hakkında farkındalık yaratmayı ve oltalama saldırılarına karşı alınması gereken önlemleri anlatmayı hedefleyecektir. Ayrıca, elde edilen veriler ışığında, dijital güvenlik hakkında toplumsal bilinç düzeyinin artırılması için önerilerde bulunulacaktır.

4. Bulgular ve Tartışma

Bu araştırma, dijital güvenlik ve oltalama saldırıları konusunda yapılan önceki çalışmaların verileri üzerinden bir literatür taraması yapmayı amaçlamaktadır. Bulgular, dijital güvenlik hakkında farkındalık eksikliklerinin yaygın olduğunu ve bireylerin oltalama saldırıları konusunda çoğu zaman bilgi eksikliği yaşadığını ortaya koymaktadır. Literatürdeki araştırmalara göre, dijital güvenlik önlemleri alınmadığı takdirde, kişisel verilerin sızması ve kötüye kullanımı gibi sonuçlarla karşılaşılabilir. Ayrıca, oltalama saldırılarının sosyal mühendislik tekniklerini kullanarak bireylerin güven duygusunu hedef alması, bu tür saldırıların etkisini artırmaktadır.

Beklenen bulgular arasında, dijital güvenlik konusunda farkındalık oluşturulması gereken kritik alanların vurgulanması ve bu farkındalığın artırılmasına yönelik önerilerin ortaya konması yer almaktadır. Bu araştırma, dijital güvenlik önlemleri konusunda toplumsal bilinç oluşturmanın, özellikle genç kullanıcılar arasında önemli bir etki yaratacağını göstermektedir. Özellikle, dijital güvenlik eğitimlerinin okullarda ve gençlere yönelik etkinliklerde yaygınlaştırılması gerektiği vurgulanmaktadır. Ayrıca, insanların dijital dünyada daha dikkatli olmalarını sağlayacak farkındalık kampanyalarının toplum üzerindeki etkisi büyük olacaktır.

Elde edilen bulgulara göre, toplumda dijital güvenlik konusunda hala önemli bir bilgi eksikliği bulunmakta ve oltalama gibi saldırılar genellikle bireylerin dikkat eksikliklerinden ve güvenme eğilimlerinden faydalanmaktadır. Bu sebeple, dijital güvenliğe dair bilgi ve farkındalık artırıcı eğitimlerin, özellikle okullarda, daha yaygın hale getirilmesi önerilmektedir.

Bu araştırma, dijital güvenlik konusunda toplumsal bilinç oluşturmanın önemini ortaya koymuş ve dijital güvenliğe yönelik eğitimlerin, kişisel verilerin korunmasında ve oltalama

saldırılarının etkilerinin azaltılmasında nasıl bir rol oynayabileceğini göstermiştir. Ayrıca, dijital güvenliğin, sadece teknolojik araçlarla değil, aynı zamanda bireylerin davranışsal değişiklikleri ile de desteklenmesi gerektiği sonucuna varılmıştır.

5. Sonuç ve Öneriler

Günümüzde hızla dijitalleşen dünyada, teknolojinin hayatımıza entegrasyonu arttıkça kişisel veri güvenliği kritik bir sorun haline gelmiştir. Özellikle oltalama gibi sosyal mühendislik saldırıları, bireylerin insana özgü zafiyetlerini hedef alarak dijital güvenliği tehlikeye atmaktadır. Merak, acelecilik, güvenme eğilimi ve dikkat dağınıklığı gibi insana özgü zaaflar, bu saldırıların başarı oranını artırmaktadır (KVKK Kişisel Veri Güvenliği Rehberi – Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler, 2018).

Oltalama saldırıları genellikle bireylerin dijital ayak izlerinden faydalanır. Sosyal medya hesaplarından, çevrimiçi alışveriş alışkanlıklarından ve diğer internet aktivitelerinden toplanan

veriler, kişiye özel ve inandırıcı saldırılar düzenlenmesini kolaylaştırır (KVKK Kişisel Veri Güvenliği Rehberi - Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler, 2018). Bu durum, kullanıcıların dijital izlerini farkında olmadan nasıl genişlettiğini ve bunun nasıl kötüye kullanılabilir hale geldiğini göstermektedir.

Öte yandan, kişisel verilerin sızdırılması ve kötüye kullanılması giderek büyüyen bir tehdit haline gelmektedir. Kimlik Hırsızlığı Kaynak Merkezi'nin 2019 raporuna göre, dünya genelinde 1.152 veri ihlali tespit edilmiştir (IBM Cyber Security Report, 2020). Uzmanlara göre, yıllar geçtikçe kişisel veri güvenliği azalmakta ve kullanıcıların rızası olmadan veriler toplanmaktadır (Wikipedia - Data Breach).

İki faktörlü kimlik doğrulama, güçlü şifre yönetimi ve güvenlik yazılımlarının kullanımı gibi teknolojik çözümler bu sorunu hafifletmeye yardımcı olsa da tamamen ortadan kaldırmak imkânsıza yakındır. Çünkü insan zafiyeti, teknolojik çözümleri devre dışı bırakabilecek kadar güçlüdür. Bu nedenle farkındalık eğitimleri ile teknolojik önlemleri bir araya getirerek bireylerin bu tehditlere karşı nasıl daha dirençli hale gelebileceği incelenmelidir (KVKK Kişisel Veri Güvenliği Rehberi - Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler, 2018).

Dijitalleşmenin kaçınılmaz olduğu bu çağda, yalnızca teknolojiyi değil, insanı da merkeze alan bir yaklaşım geliştirilmesi şarttır. Bilinçlendirme kampanyalarının yanı sıra, bireylerin dijital davranışlarını daha sorumlu bir şekilde yönetmeleri gerektiği savunulmaktadır (Wikipedia - Cyber Security Awareness). Ancak, dijital izlerin tamamen silinemez oluşu ve insana özgü zaafların her zaman var olması, veri güvenliğini sağlamanın çok boyutlu ve sürekli bir mücadele olduğunu kanıtlamaktadır (IBM X-Force Threat Intelligence Index 2021).

Çevrimiçi hesaplarınızı güvence altına almak, kişisel verilerinizi korumanın ilk adımıdır. Hesaplarınızı güvenli hale getirmek için virüs yazılımları ve uçtan uca şifreleme

kullanabilirsiniz. Verilerinizi korumak için şifreleme, özellikle dosyalarınıza şifre koymak ve SSL şifreleme ile çalışan web sitelerini tercih etmek önemlidir (KVKK Kişisel Veri Güvenliği Rehberi - Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler, 2018). Ayrıca, VPN kullanarak internet trafiğinizi şifrelemek de güvenliği artıran bir yöntemdir (Wikipedia - Virtual Private Network).

Yazılım güncellemelerini ihmal etmemek, veri hırsızlarının fırsat bulmasını engeller. Yazılımınızı düzenli olarak güncelleyerek güvenlik açıklarını kapatabilirsiniz (IBM Cyber Security Report, 2020). Çevrimiçi ayak izinizi en aza indirmek için kullanılmayan hesapları silmeli ve kalan hesapları güvenli e-posta adresleriyle ilişkilendirmelisiniz (Wikipedia - Digital Footprint). Son olarak, verilerinizi belirli aralıklarla yedeklemeli ve virüslere karşı anti-virüs programı kullanmalısınız (KVKK Kişisel Veri Güvenliği Rehberi - Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler, 2018).

Kaynakça

Afyon Kocatepe Üniversitesi Bilgi İşlem Merkezi. (t.y.). Oltalama (oltalama) nedir? Afyon Kocatepe Üniversitesi. https://bim.aku.edu.tr/oltalama-oltalama-nedir/

Cisco Umbrella. (t.y.). Oltalama for dummies: Discover the real risks of oltalama. Cisco. https://umbrella.cisco.com/info/oltalama-for-dummies-ebook-discover-real-risks-of-oltalama?

Kişisel Verileri Koruma Kurumu. (t.y.). Veri güvenliğine ilişkin yükümlülükler. KVKK Resmi Web Sitesi. https://www.kvkk.gov.tr/Icerik/2040/Veri-Guvenligine-Iliskin-Yukumlulukler

Kişisel Verileri Koruma Kurumu. (t.y.). Veri güvenliği rehberi. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

Laba Türkiye. (t.y.). KVKK eğitimi. Laba Eğitim Platformu. https://laba.com.tr/lecture/1423-kvkk-egitimi

Veri Sistem. (t.y.). Kişisel verilerin korunması kanunu (KVKK) danışmanlık ve uyum hizmetleri. Veri Sistem. https://www.verisistem.com/tr/hizmetlerimiz/kisisel-verilerin-korunmasi-kanunu-kvkk-danismanlik-uyum-hizmetleri/

Kaspersky Lab. (t.y.). Dijital ayak izlerinizi azaltmanın yolları. Kaspersky Blog. https://www.kaspersky.com/blog/digital-footprint

TechRadar. (t.y.). 2024 yılında en iyi dijital güvenlik önlemleri. TechRadar. https://www.techradar.com/best-digital-security-tips

Trend Micro. (t.y.). Oltalama saldırılarının yeni türleri ve korunma yöntemleri. Trend Micro Güvenlik Raporu. https://www.trendmicro.com/latest-oltalama-attacks

Vikipedi katılımcıları. (2025, 1 Şubat). Siber güvenlik. *Vikipedi, Özgür Ansiklopedi*. https://tr.wikipedia.org/wiki/Siber_güvenlik