vodafone business

Cebinizdeki Risk:
Mobil Çağda İşletmeler İçin Siber Güvenlik Rehberi

TEMMUZ 2026

İçindekiler

Önsöz

Cep telefonları ve bağlantı hizmetleri artık hayatımızın ayrılmaz bir parçası. Gözümüzü açtığımız andan itibaren işimizi yönetmemize, günlük sorumluluklarımızı yerine getirmemize ve sevdiklerimizle iletişimde kalmamıza yardımcı oluyorlar. Zamanla yalnızca bir iletişim aracı olmaktan çıkıp dijital yaşamımızın merkezi haline geldiler. Kimlik bilgilerimizden finansal verilerimize, fotoğraflarımızdan mesajlarımıza kadar pek çok önemli bilgi artık tek bir cihazda bulunuyor.

Telefonlarımızı her yerde kullanıyoruz; toplu taşımada, kafelerde, otellerde ve gün boyunca hareket halindeyken. Pek çok kişi için günlük yaşamın vazgeçilmez bir parçası olan bu cihazlarda yaşanan herhangi bir aksaklık, tahmin edilenden çok daha büyük etkiler yaratabiliyor.

İş dünyasında da mobil cihazlar artık yalnızca yardımcı araçlar değil, operasyonların ayrılmaz bir parçası haline gelmiş durumda. Buna rağmen çoğu zaman diğer kurumsal teknolojiler kadar güvenlik odağında değerlendirilmiyorlar.

Oysa mobil cihazlar bugün dijital dünyamızın neredeyse tüm unsurlarını bir araya getiriyor. İş e-postaları ile kişisel mesajlaşmalar, kurumsal uygulamalar ile bankacılık, alışveriş ve sosyal medya uygulamaları aynı cihaz üzerinde buluşuyor.

Kişisel ve profesyonel kullanımın bu kadar iç içe geçmesi, hassas verilerin tek bir ortamda toplanmasına neden oluyor. Üstelik telefonlarımızı çoğu zaman hareket halindeyken, küçük ekranlarda ve dikkatimizin kolayca bölündüğü anlarda kullanıyoruz. Bu durum mobil cihazları siber saldırganlar için daha cazip hedefler haline getiriyor. Araştırmalar, mobil cihazların artık saldırganların öncelikli hedeflerinden biri olduğunu ve kullanıcıların sürekli olarak mobil tehditlerle karşı karşıya kaldığını gösteriyor. Mobil cihazlar bir yandan en güçlü verimlilik araçlarımızdan biri olurken, diğer yandan en önemli güvenlik risklerimiz arasında yer alıyor.

Vodafone olarak dünya genelinde 15 ülkede 310 milyondan fazla mobil müşteriye hizmet veriyoruz. Bu nedenle yalnızca cihazları değil, bu cihazlara güvenen insanları korumanın da ne kadar önemli olduğunu biliyoruz.

Bu raporda, mobil dünyadaki başlıca tehditleri, bu tehditleri nasıl tespit edebileceğinizi ve işletmenizi korumak için hangi adımları atabileceğinizi ele alıyoruz.

Jenn Didoni,
Bulut, Güvenlik ve Yönetilen Hizmetler Direktörü,
Vodafone Business

1. ENISA Tehdit Ortamı Raporu 2025
2. Vodafone 2025 yıllık raporu

Mobil Cihazlar: Günümüz İşletmeleri İçin En Büyük Güvenlik Riski

Avrupa genelinde, insan sayısından daha fazla mobil bağlantı bulunuyor; her 100 kişi için yaklaşık 122 ila 146 mobil abonelik düşüyor.[3]

Mobil cihazlar üzerinden gerçekleştirilen saldırılar artık tüm siber güvenlik olaylarının %42'sinden fazlasını oluşturuyor.[4] Bu durum işletmeler açısından büyük önem taşıyor. Akıllı telefonlar ve tabletler; kurumsal e-postalardan müşteri bilgilerine, bankacılık uygulamalarından hassas dosyalara kadar pek çok kritik veriyi barındırıyor. Bu da onları siber suçlular için cazip bir giriş noktası haline getiriyor.[3]

İşletmelerin operasyonlarında mobil platformlara geçiş hızı da giderek artıyor. Vodafone, Avrupa genelinde işletmelerin daha fazla satış kanalını dijital ortama taşıdığını, tüketicilerin ise nakit kullanımından uzaklaşarak mobil telefonlar ve akıllı saatler aracılığıyla dijital ödemelere yöneldiğini gözlemliyor.

Nitekim bu eğilimler, mobil para işlemlerinin değerinde yıllık bazda %14'lük bir artışa yol açtı.[5] Mobil kullanımın hızla yaygınlaşması işletmeler için önemli fırsatlar sunarken, aynı zamanda siber suçlular için de yeni ve cazip hedefler oluşturuyor.

3. Digital 2026: Küresel Genel Bakış Raporu — DataReportal – Global Dijital İçgörüler
4. ENISA Tehdit Görünümü Raporu 2025
5. Vodafone yıllık raporu 2025

Yıllar boyunca güvenlik stratejileri bilgisayarlar, sunucular, ağlar ve güvenlik duvarları üzerine odaklandı. Ancak çalışma biçimlerimiz değişti. Uzaktan çalışma, bulut tabanlı uygulamalar ve kesintisiz bağlantı sayesinde çalışanlar artık iş sistemlerine her yerden erişebiliyor. Üstelik bu erişim çoğu zaman kurumsal ağın dışındaki kişisel cihazlar üzerinden gerçekleşiyor.

Siber saldırganlar da bu değişime hızla uyum sağladı. Sürekli internete bağlı, her an kullanılan ve genellikle dizüstü bilgisayarlar, masaüstü bilgisayarlar veya sunucular kadar iyi korunmayan mobil cihazları hedef alıyorlar.

Bugün ekiplerinizin telefonlarını nasıl kullandığını düşünün: Müşteri e-postalarını yanıtlamak, tedarikçilerle WhatsApp üzerinden iletişim kurmak, Teams veya Slack üzerinde iş birliği yapmak, ödemeleri onaylamak, satış ve rezervasyon araçlarına erişmek, belge paylaşmak ya da sosyal medya hesaplarını yönetmek için mobil cihazlardan yararlanıyorlar. Bunlar size tanıdık geliyorsa, mobil güvenliğin artık bir tercih değil, bir zorunluluk olduğunu da biliyorsunuz demektir.

Özellikle küçük ve orta ölçekli işletmelerde, çalışanlara mobil güvenlik eğitimi verilmemesi ve güvenlik katmanlarının yetersiz kalması nedeniyle tek bir cihazın ele geçirilmesi; veri ihlallerine, veri kaybına veya finansal dolandırıcılıklara hızla dönüşebiliyor.

2026'nın Öne Çıkan Mobil Güvenlik Tehditleri

1. Mobil oltalama (Phishing) ve SMS dolandırıcılığı (Smishing)
2. Mobil kötü amaçlı yazılımlar (uygulamalar)
3. İşletim sistemi güvenlik açıkları ve casus yazılımlar
4. Ağ saldırıları (ortadaki adam saldırıları ve veri ele geçirme girişimleri)
5. SIM kart ele geçirme ve kimlik hırsızlığı

6. Lookout Mobil Tehdit Ortamı Raporu 2025 2. Çeyrek
7. Vodafone Business Araştırması, tarafından gerçekleştirilen Savanta, 2026

1. Oltalama (Phishing) ve SMS Dolandırıcılığı (Smishing): Çok Kanallı Saldırı Kampanyaları

Sosyal mühendislik, siber suçluların şifreler, ödeme bilgileri veya işletmenize erişim gibi hassas bilgileri ele geçirmek amacıyla güvendiğiniz bir kişi ya da kurum gibi davranmasıdır. Bu dolandırıcılık girişimleri e-posta (phishing), SMS (smishing), sahte web siteleri veya telefon aramaları (vishing) yoluyla gerçekleştirilebilir. Saldırganlar, taleplerini daha inandırıcı göstermek ve sizi bilgi paylaşmaya yönlendirmek için bu yöntemlerin birkaçını bir arada kullanır.

ENISA verilerine göre oltalama saldırıları, siber saldırıların başlangıcında hâlâ en yaygın yöntem olmaya devam ediyor ve **güvenlik olaylarının %60'ı tek bir sahte mesajla başlıyor**.[9] Günümüzde saldırganlar, mesajlarını en hızlı görebileceğiniz ve yanıt verebileceğiniz kanalları hedef alıyor. Bu nedenle SMS, WhatsApp (ve diğer mesajlaşma uygulamaları), sesli mesajlar ve sosyal medya üzerinden gönderilen doğrudan mesajlar mobil cihazlarda önemli riskler oluşturuyor.

Vodafone tarafından yakın zamanda gerçekleştirilen bir araştırmaya göre, ankete katılan işletmelerin yarısından fazlası oltalama girişimlerinde artış yaşandığını belirtti. Katılımcıların %70'i ise mobil güvenlik saldırıları konusunda 12 ay öncesine kıyasla daha fazla endişe duyduğunu ifade etti.[10]

Bir sonraki sayfadaki şema, saldırganların tipik bir çok kanallı oltalama saldırısını nasıl planladığını ve uyguladığını adım adım göstermektedir.

8. Kimlik avı dolandırıcılıkları nelerdir? | V-Hub | Vodafone Ireland | v-hub.vodafone.ie

9. ENISA Tehdit Ortamı raporu 2025

10. Vodafone Business Research tarafından yürütülen Savanta, 2026

Mobil cihazlarınız her zaman açık, her zaman bağlı ve her zaman erişilebilir olduğu için saldırganların birincil hedefi haline geliyor. Oltalama saldırıları tüm iletişim kanallarına yayıldıkça, akıllı telefonlar güvenlik risklerinin merkezinde yer almaya başladı.

Jenn Didoni,
Bulut, Güvenlik ve Yönetilen Hizmetler Direktörü, Vodafone Business

SALDIRI Akışı

1 Araştırma

Saldırganlar, inandırıcı mesajlar oluşturmak için herkese açık bilgileri (LinkedIn profilleri, görev tanımları, e-posta formatları, tedarikçi bilgileri ve güncel duyurular gibi) inceler.
Korunma yöntemi: Gereğinden fazla bilgi paylaşımını sınırlandırın ve çalışanlarınıza sosyal mühendislik belirtilerini tanımaları için eğitim verin.

2 İlk Temas

Saldırganlar, sahte kimlikler kullanarak, aciliyet hissi yaratarak veya kötü amaçlı bağlantılar ve ekler içeren oltalama e-postaları ya da mesajlar gönderir.

Korunma yöntemi: Oltalama karşıtı güvenlik çözümlerini etkinleştirin ve çalışanlarınıza gönderen bilgilerini ve bağlantıları kontrol etmeyi öğretin.

3 İkincil İletişim

Saldırganlar, telefon görüşmeleri aracılığıyla dolandırıcılığı destekleyerek daha inandırıcı görünmeye çalışır.

Korunma yöntemi: Beklenmedik talepleri, size iletilen iletişim bilgileri yerine daha önce doğrulanmış ve güvenilir iletişim kanalları üzerinden teyit edin.

4 Yönlendirme

Saldırganlar, kullanıcıları sahte giriş sayfalarına, sahte ödeme portallarına veya uzaktan erişim araçlarına yönlendirir; ayrıca çok faktörlü kimlik doğrulama (MFA) kodları ve şifreleri talep edebilir.

Korunma yöntemi: MFA, URL filtreleme, güçlü parola yönetimi ve koşullu erişim kontrolleri gibi güvenlik önlemlerini kullanın.

5 Ele geçirme

Saldırganlar, kullanıcı bilgilerini ele geçirir, MFA korumalarını aşar, zararlı yazılım yükler veya sahte işlemler gerçekleştirir.

Korunma yöntemi: Olağan dışı oturum açma girişimlerini ve riskli kullanıcı davranışlarını sürekli izleyin.

6 Kurum İçinde Yayılma

Saldırganlar, kurum içi dosyalara erişir, yetkilerini artırır veya ele geçirilmiş hesaplar üzerinden kurum içi oltalama saldırıları gerçekleştirir.

Korunma yöntemi: En az yetki prensibini uygulayın, anomali tespit mekanizmalarından yararlanın ve güçlü olay müdahale süreçleri oluşturun.

7 Nihai hedef

Saldırganlar, dolandırıcılık gerçekleştirir, veri çalar, fidye yazılımı yayar veya kurumsal e-posta hesaplarının ele geçirilmesinden yararlanır.

Korunma yöntemi: Çok katmanlı güvenlik yaklaşımı benimseyin ve çalışan farkındalığını sürekli olarak artırın.

Mobil Oltalama (Phishing) Saldırıları Neden Etkili?

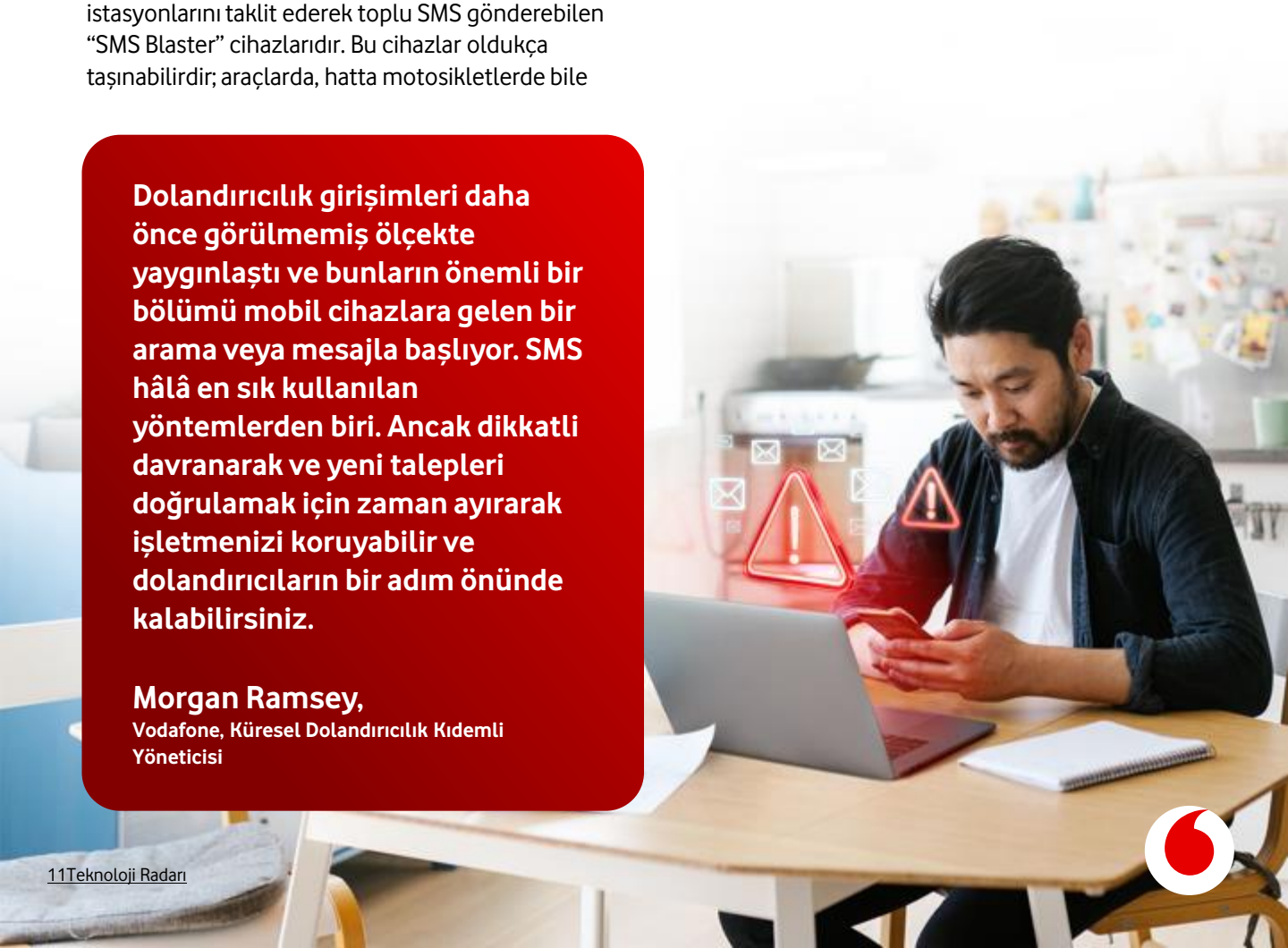
Mobil cihazlara gönderilen oltalama mesajları, kullanıcıları hazırlıksız yakalamak üzere tasarlanır. Bu mesajlar çoğu zaman bankanızdan gelen bir bildirim, bir kargo teslimatı SMS'i ya da IT ekibinizden gönderilmiş gibi görünen bir sesli mesaj gibi güvenilir kaynaklardan geliyormuş izlenimi yaratır. Genellikle sizden hesabınızı doğrulamanız veya bir güvenlik kodunu onaylamanız istenir. Sürekli bildirimlerle dolu küçük telefon ekranlarında ise bu mesajlara hızlıca göz atıp işlem yapmak oldukça kolaydır. Ancak tek bir dokunuş, saldırganların hesaplarınıza erişmesine veya cihazınıza zararlı yazılım yüklemesine neden olabilir.

Siber suçlular, mobil oltalama kampanyalarını yürütmek için geniş insan ve teknoloji ağları oluşturmuş durumdadır. Yüzlerce çalışanın görev aldığı dolandırıcılık merkezlerinden, yüz binlerce SIM kart üzerinden mesaj gönderip alabilen yapılara kadar uzanan bu ekosistem, her geçen gün daha büyük ve daha gelişmiş hale gelmektedir. Saldırganlar aynı zamanda giderek daha yaratıcı yöntemler kullanıyor. Bunlardan biri de mobil baz istasyonlarını taklit ederek toplu SMS gönderebilen "SMS Blaster" cihazlarıdır. Bu cihazlar oldukça taşınabilirdir; araçlarda, hatta motosikletlerde bile kullanılabilir. Böylece dolandırıcılar yoğun şehir bölgelerinde dolaşarak binlerce potansiyel kurbana ulaşabilir. Üstelik telefon numaranızı paylaşmış olmanız da gerekmez. Cihaz kapsama alanındaki tüm telefonlara aynı dolandırıcılık mesajını gönderebilir ve birilerinin düşünmeden tepki vermesini bekler.

Mobil oltalama saldırıları, binlerce kişiye gönderilen basit bir dolandırıcılık mesajından, belirli bir kişi veya kuruluşu hedef alan detaylı ve kişiselleştirilmiş saldırılara kadar farklı şekillerde gerçekleştirilebilir. Yapay zekâ destekli "deepfake" teknolojilerinin ve telefonunuzda görünen arayan numarayı değiştirebilen araçların da kullanılmasıyla birlikte tehdit seviyesi hiç olmadığı kadar yükselmiştir. Bu nedenle, güvenilir bir kaynaktan geliyor gibi görünseler bile beklenmedik mesaj ve aramalara karşı dikkatli olmak büyük önem taşımaktadır.

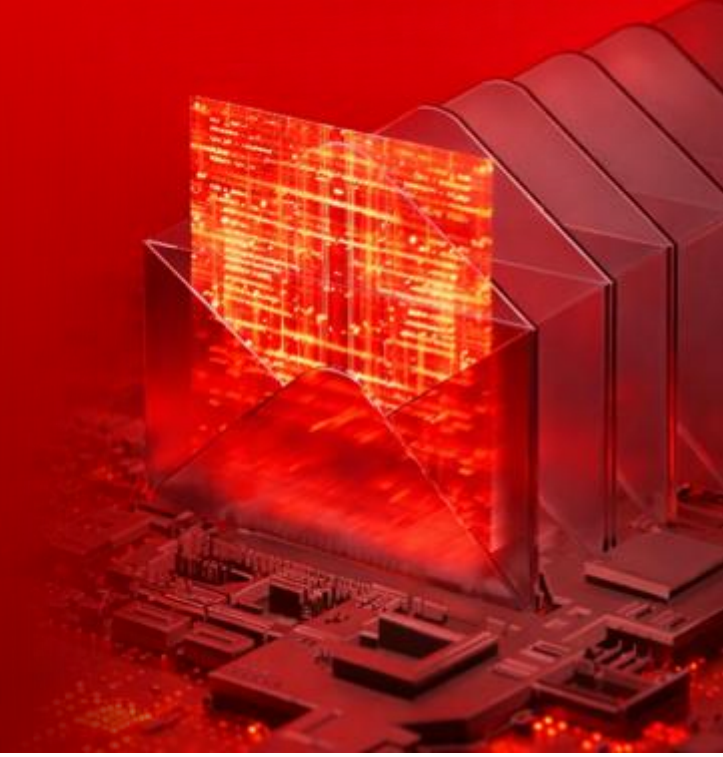
Dolandırıcılık girişimleri daha önce görülmemiş ölçekte yaygınlaştı ve bunların önemli bir bölümü mobil cihazlara gelen bir arama veya mesajla başlıyor. SMS hâlâ en sık kullanılan yöntemlerden biri. Ancak dikkatli davranarak ve yeni talepleri doğrulamak için zaman ayırarak işletmenizi koruyabilir ve dolandırıcıların bir adım önünde kalabilirsiniz.

Morgan Ramsey,
Vodafone, Küresel Dolandırıcılık Kıdemli Yöneticisi



Sorunun Boyutu Giderek Artıyor

Microsoft Security verileri, oltalama saldırıları ve kimlik temelli siber saldırıların hızla arttığını gösteriyor. Üç aylık bir dönemde yaklaşık %30'luk bir artış yaşanırken[12], mobil güvenlik şirketi Lookout da kurumsal mobil oltalama vakalarında üç ay içerisinde %20'lik bir yükseliş tespit etti. Bu durum, saldırganların dolandırıcılık girişimlerini giderek daha fazla doğrudan mobil cihazlara yönelttiğini açıkça ortaya koyuyor.[13]



Teknolojiden Önce İnsan Faktörü

İşletmeler, bu tür dolandırıcılık girişimlerine karşı özellikle savunmasızdır; çünkü kurumların merkezinde insanlar yer alır. Vodafone'un yakın tarihli bir araştırmasına göre, kuruluşların %41'i çalışanlarının kişisel cihazları üzerinden şirket kaynaklarına herhangi bir güçlü güvenlik önlemi veya koruma aracı olmadan erişmesine izin veriyor.[14] Bu durum, çalışanların muhakeme gücünü oltalama saldırılarına karşı hem ilk hem de son savunma hattı haline getiriyor. Saldırganlar bunun farkında ve bundan en üst düzeyde yararlanıyor.

Burada bir güven algısı farkı da söz konusu. Küçük işletmeler arasında gerçekleştirilen bir Vodafone araştırmasında, yöneticilerin %78'i çalışanlarının gelişmiş bir oltalama girişimini fark edebileceğine inanırken, yapılan testlerde çalışanların yaklaşık üçte ikisinin gerçek bir oltalama mesajını tespit edemediği görüldü.[15]

Başka bir ifadeyle, birçok kişi karşısına gerçekten ikna edici bir dolandırıcılık girişimi çıkana kadar bu tür saldırılara kanmayacağından emin hissediyor.

Siber suçluların güvendiği nokta da tam olarak bu aşırı özgüvendir. Kilit ekranında kısa süreliğine görülen zamanlaması iyi ayarlanmış ve inandırıcı bir mesaj çoğu zaman yeterli olabiliyor. Bir kullanıcı kötü amaçlı bir bağlantıya tıklayıp bilgilerini sahte bir giriş sayfasına girdiğinde, saldırganlar şifreleri ele geçirebilir, hesapları devralabilir ve hatta daha geniş kurumsal sistemlere erişim sağlayabilir.

Tek bir mesaj, kısa sürede veri ihlali, finansal dolandırıcılık veya fidye yazılımı saldırısı gibi çok daha ciddi sonuçlara yol açabilir.

12. Microsoft Digital Savunma 2025 Raporu
13Lookout Mobil Tehdit Ortamı 2025 2. Çeyrek
14. Vodafone Business Araştırması, tarafından yürütülen Savanta, 2026
15. Vodafone: Proaktif Güvenlik – Geleceğin Phishing'i

Ne Yapabilirsiniz?

Mobil oltalama riskini önemli ölçüde azaltmak için farkındalık çalışmaları ile doğru güvenlik teknolojilerini bir arada kullanmak gerekir.

Oltalama Farkındalığını Günlük Çalışma Kültürünün Bir Parçası Haline Getirin: Kısa ve uygulamaya yönelik hatırlatmalar, uzun ve tek seferlik eğitimlerden çok daha etkilidir. Ekiplerinizle gerçek oltalama e-postaları ve mesaj örneklerini paylaşın. Aciliyet hissi yaratılması, bilinmeyen göndericiler, şüpheli bağlantılar veya beklenmedik şifre ve ödeme talepleri gibi uyarı işaretlerine dikkat çekin. Düzenli olarak gerçekleştirilen güvenli oltalama testleri, çalışanların farkındalığını canlı tutmaya yardımcı olabilir. Ayrıca bu raporun sonunda yer alan oltalama farkındalığı posterine göz atabilirsiniz.

Durup kontrol etme kültürü oluşturun: Çalışanları harekete geçmeden önce doğrulama yapmaya teşvik edin. SMS, WhatsApp veya e-posta yoluyla gelen beklenmedik talepler mutlaka ikinci ve güvenilir bir yöntemle doğrulanmalıdır. Bilinen bir telefon numarası üzerinden yapılacak kısa bir doğrulama görüşmesi, dolandırıcılık girişimlerini daha başlamadan engelleyebilir.

Mevcut Güvenlik Önlemlerini Güçlendirin: Spam ve oltalama filtrelerinin etkin olduğundan ve düzenli olarak güncellendiğinden emin olun. Lookout Mobil Uç Nokta Güvenliği, Microsoft Defender veya Trend Micro Mobile gibi özel mobil güvenlik çözümlerinin kullanımını değerlendirin. En önemlisi ise e-posta, bankacılık ve bulut uygulamaları dâhil tüm temel sistemlerde çok faktörlü kimlik doğrulamayı (MFA) etkinleştirin. Bu basit iki adım, otomatik saldırıların büyük bölümünü engelleyebilir ve bir şifrenin ele geçirilmesi durumunda ek bir koruma katmanı sağlar.

Bir Sorun Yaşandığında Ne Yapılacağını Önceden Belirleyin: En iyi güvenlik alışkanlıklarına sahip kurumlarda bile hatalar yaşanabilir. Önemli olan hızlı hareket etmektir. Çalışanların şüpheli bir bağlantıya tıkladıklarında veya yanlışlıkla bilgi paylaştıklarında kiminle iletişime geçmeleri gerektiğini açıkça belirleyin. Ayrıca çalışanları durumu bildirdikleri için suçlanmayacakları konusunda teşvik edin. Kimin bilgilendirileceğini, hesapların nasıl güvence altına alınacağını ve şifrelerin nasıl sıfırlanacağını kapsayan basit bir eylem planı, küçük bir hatanın büyük bir güvenlik olayına dönüşmesini önleyebilir.

16. Microsoft: Hesaplarınıza yönelik saldırıların %99,9'unu engellemek için atabileceğiniz tek bir basit adım

2. Kötü Amaçlı Uygulamalar: Güvenilir Araçlar Gibi Görünen Mobil Zararlı Yazılımlar

Mobil zararlı yazılımlar, akıllı telefonları ve tabletleri hedef almak için tasarlanmış kötü amaçlı yazılımlardır. Genellikle tamamen masum görünen bir uygulama aracılığıyla cihazlara bulaşırlar. Bu bir oyun, yardımcı bir uygulama ya da iş süreçlerini kolaylaştırdığını iddia eden bir araç olabilir. Ancak perde arkasında uygulama değiştirilmiş veya zararlı yazılımı gizlemek amacıyla özel olarak hazırlanmış olabilir. Uygulama yüklendiğinde, zararlı yazılım sessizce çalışmaya başlar; kişi listeleri ve kayıtlı parolalar gibi hassas bilgileri çalabilir, konum verilerini takip edebilir, kullanıcı faaliyetlerini izleyebilir veya saldırganlara cihaz üzerinde uzaktan erişim sağlayabilir.

Ancak zararlı yazılımlar yalnızca uygulamalar aracılığıyla bulaşmaz. Şüpheli bir e-posta eki veya telefonunuza otomatik indirme başlatan bir web sitesi üzerinden de cihazlara sızabilir.

Sorunun boyutunu ortaya koymak gerekirse, her on iki siber olaydan yaklaşık biri ele geçirilmiş bir mobil uygulamaya kadar izlenebilmektedir. Bu uygulamalar çoğu zaman resmi uygulama mağazalarının dışından yüklenmiş ya da güvenilir görünmesi için ustalıkla gizlenmiş uygulamalardır.[17]

Çalışanların iş amaçlı olarak kişisel telefonlarını kullanması veya teknik kontrollerin yeterli olmadığı durumlarda kurumsal cihazlara serbestçe uygulama yüklemesi oldukça yaygındır. Kendi cihazını kullan (BYOD) yaklaşımı birçok işletme için pratik ve gerekli olsa da, iş süreçlerini kolaylaştırmak amacıyla sürekli yeni uygulamalar yüklemek siber riskleri de beraberinde getirmektedir.

Sahte "ChatGPT" tuzağı

2025 yılının başlarında siber suçlular, yapay zekâ araçlarına yönelik yoğun ilgiden yararlanarak Avrupa'daki işletmelere zararlı yazılım yaymaya çalıştı. Bu kapsamda, popüler yapay zekâ sohbet robotunun resmi mobil uygulaması gibi görünen sahte bir "ChatGPT" uygulaması dolaşıma sokuldu.

Verimliliklerini artıracak yeni araçlar arayan birçok çalışan, herhangi bir riskten şüphelenmeden bu uygulamayı indirdi. Ancak uygulama yüklendikten sonra cihazlara gizlice bir arka kapı yerleştirildi ve saldırganlara tam erişim sağlandı. Bu kampanya onlarca küçük işletmeyi etkiledi; bilinen mağdurların %50'sinden fazlası Avusturya, Almanya ve Portekiz'de bulunuyordu.[18]

Bu olay, uygulama indirmeden önce durup düşünmenin, yalnızca resmi uygulama mağazalarını kullanmanın ve piyasaya sürülen her yeni aracı sağlıklı bir şüpheyle değerlendirmenin ne kadar önemli olduğunu gösteriyor.

17. ENISA Tehdit Ortamı Raporu 2025

18. KOBİ'lere güvenlik uyarısı - yeni kötü amaçlı yazılımlar ChatGPT, Microsoft Office ve Google Drive gibi araçları taklit ediyor, bu yüzden tetikte olun | TechRadar

Güvenilir Uygulama Mağazaları Bile Hata Yapabilir

Güvenilir uygulama mağazalarının inceleme süreçlerinden zaman zaman kötü amaçlı uygulamalar geçebilmektedir.

Yakın zamanda yaşanan bir olayda, güvenlik araştırmacıları tespit edilip kaldırılmadan önce on milyonlarca kez indirilen yüzlerce zararlı uygulamayı ortaya çıkardı. Bu uygulamalar, fotoğraf düzenleme araçları ve oyunlar gibi tamamen meşru uygulamalar gibi görünüyordu.

Bu durum, güvenilir uygulama mağazalarının kullanılmasının bilinmeyen kaynaklardan uygulama yüklemeye kıyasla riski önemli ölçüde azalttığını gösterse de, hiçbir platformun tamamen güvenli olmadığını ve kararlı saldırganların güvenlik kontrollerini aşmanın yollarını bulabileceğini ortaya koymaktadır.

Ne yapabilirsiniz?

İşletmenizi kötü amaçlı uygulamalardan ve zararlı yazılımlardan korumak için uygulama kullanım alışkanlıklarını ve cihaz güvenliğini güçlendirin.

Cihazlarınızı ve Uygulamalarınızı Güncel Tutun: Güncellemeler, çoğu kişinin düşündüğünden daha önemlidir. Hem uygulama güncellemeleri hem de işletim sistemi güncellemeleri, saldırganların yararlanabileceği güvenlik açıklarını kapatır. Mümkün olduğunca otomatik güncellemeleri etkinleştirin ve çalışanlarınızı güncellemeleri yayımlandığı anda yüklemeye teşvik edin. Güncellemeleri ertelemek, zararlı yazılımlar için kapıyı açık bırakır.

Güvenilir Uygulama Mağazalarını Tercih Edin: Süreci basit tutun. Çalışanları yalnızca Google Play veya Apple App Store gibi resmi uygulama mağazalarından uygulama yüklemeye teşvik edin. Bağlantılar, açılır pencereler, forumlar veya resmî olmayan mağazalar üzerinden uygulama indirmekten kaçının. Çünkü zararlı yazılımların yayılmasında en sık kullanılan yöntemlerden biri budur.

Cihazları Mümkün Olduğunca Merkezi Olarak Yönetin: İşletmenizde temel seviyede bile bir IT desteği varsa, mobil cihaz yönetimi araçları önemli fark yaratabilir. Mobil Cihaz Yönetimi (MDM) çözümleri; hangi uygulamaların yüklenebileceğini kontrol etmenizi, PIN ve şifreleme gibi temel güvenlik özelliklerini yönetmenizi ve güncellemeleri uzaktan dağıtmanızı sağlar. Vodafone Secure Device Manager bu konuda iyi bir başlangıç noktasıdır.

Uygulama İzinlerine Dikkat Edin: Bir uygulama ihtiyaç duymadığı verilere erişim talep ediyorsa bunu bir uyarı işareti olarak değerlendirin. Örneğin bir el feneri veya hesap makinesi uygulamasının kişilerinize ya da mikrofonunuza erişmesi için makul bir neden yoktur. Çalışanları olağan dışı izin taleplerini sorgulamaya ve gereğinden fazla erişim isteyen uygulamalardan kaçınmaya teşvik edin. Yönetilen cihazlarda ise kötü amaçlı uygulamalar tarafından sıkça istismar edilen Erişilebilirlik (Accessibility) izinleri gibi yüksek riskli yetkilendirmeleri sınırlandırmayı değerlendirin.

Mobil Cihazlarda Ek Koruma Katmanları Kullanın: Lookout Mobile Endpoint Security, Microsoft Defender for Endpoint veya Trend Micro Mobile gibi güvenilir mobil güvenlik ve antivirüs çözümleri, bilinen tehditleri tespit ederek ve kullanıcıları tehlikeli web sitelerine karşı uyararak ek bir koruma katmanı sağlar.

3. Güncelliğini Yitirmiş Yazılımlar: Siber Suçlular İçin Açık Bir Kapı

Mobil işletim sistemleri; Android ve iOS gibi, her gün kullandığımız uygulamaları çalıştıran yazılımlardır. Ancak her yazılım gibi, siber suçluların hızla istismar edebileceği hatalar veya güvenlik açıkları içerebilirler. Bu tür zafiyetler tespit edildiğinde Google ve Apple gibi şirketler genellikle bunları gidermek için güncellemeler yayımlar. Ancak cihazlar zamanında güncellenmezse, bilinen güvenlik açıkları saldırganlar için erişilebilir olmaya devam eder.

Sorunun temelinde, günümüzde kullanılan birçok mobil cihazın eski yazılım sürümleriyle çalışması ve önemli güvenlik yamalarını almamış olması yatıyor. Araştırmalar, Android telefonların %30'undan fazlasının artık güvenlik güncellemesi almayan işletim sistemi sürümlerini kullandığını gösteriyor.[19]

Lookout verileri bunun neden önemli olduğunu açıkça ortaya koyuyor. Şirket, tam olarak güncellenmemiş cihazlara yönelik saldırılarda belirgin bir artış gözlemledi. Buna hem Android hem de iOS cihazlar dâhil.[20] Eksik güncellemelerin yanı sıra, kurumsal cihazlarda ekran kilidinin etkinleştirilmemesi, şifrelemenin kapalı bırakılması veya temel güvenlik ayarlarının doğru yapılandırılmaması gibi yaygın zafiyetler de bulunuyor. Bir çalışanın parola kullanmaması ya da iki yıl öncesine ait bir işletim sistemi sürümünü kullanmaya devam etmesi bile cihazını kolay bir hedef hâline getirebilir.

ENISA araştırmalarına göre güvenlik olaylarının %21'i yazılım açıklarının istismar edilmesiyle ilişkilidir.[21] Bu tür saldırılarda siber suçlular, yazılımdaki bilinen güvenlik açıklarından yararlanarak sistemlere sızar. Birçok mobil zararlı yazılım vakası ve veri ihlali, yanlış yapılandırılmış sistemler veya zamanında güncellenmemiş yazılımlar nedeniyle başarılı olmuştur. Yani saldırganlar çoğu zaman aslında çoktan giderilmiş olması gereken zafiyetlerden yararlanmaktadır.

Bu durum, telefonları güncel tutmanın ve temel güvenlik ayarlarını doğru şekilde yapılandırmanın korunmanın en basit ve en etkili yollarından biri olduğunu bir kez daha göstermektedir.

19. Dijital Bilgi Dünyası
20Vodafone/Lookout Çeyrek Dönem Raporlaması 2024/25
21Vodafone/Lookout Çeyrek Dönem Raporlaması 2024/25
22. ENISA 2025 Tehdit Ortamı Raporu

2025 Yılı, Güncellenmemiş Cihazlar Hakkında Bize Ne Öğretti?

iPhone'larda Apple, sıfır gün (zero-day) açığını kapatmak için acil bir güvenlik güncellemesi yayımlamak zorunda kaldı. Saldırganlar, kullanıcı hiçbir işlem yapmadan cihazlara zararlı yazılım yükleyebilen kötü amaçlı bir iMessage gönderebiliyordu. Mesajın açılmasına bile gerek yoktu. Bu tür saldırılar genellikle üst düzey hedeflere yönelik siber casusluk faaliyetlerinde görülse de, olay güncel olmayan bir iPhone'un yalnızca bir mesaj alınmasıyla bile enfekte olabileceğini gösterdi. Güvenlik açığı, güncellemeyi yükleyen kullanıcılar için yayımlanan yamayla kapatıldı.[22]

"Birçok kuruluş dizüstü bilgisayarlarını sıkı şekilde yönetiyor ancak mobil cihazlar hâlâ zayıf bir halka olmaya devam ediyor. Güncellemeleri merkezi olarak zorunlu kılacak bir yapı olmadığında güvenlik şansa bırakılmış oluyor ve saldırganlar da tam olarak nereye bakacaklarını biliyor."

Pedro Peixe Ribeiro
Vodafone Business Siber Güvenlik Direktörü

Ne yapabilirsiniz?

Yazılımları güncel tutmak, güvenliğinizi korumanın en basit ve en düşük maliyetli yollarından biridir. Bunun için aşağıdaki adımları uygulayabilirsiniz:

1. **Güncelleme Almayan Cihazları Kullanımdan Kaldırın:** Artık güncelleme almayan telefon ve tabletler ciddi bir güvenlik riski oluşturur. Özellikle müşteri bilgilerini işleyen, ödeme süreçlerinde kullanılan veya kurumsal sistemlere erişim sağlayan cihazların yenilenmesini planlayın. Hemen değiştirme imkânı yoksa, bu cihazların erişebileceği sistemleri sınırlandırın.
2. **Otomatik Güncellemeleri Etkinleştirin:** Bu, uygulanabilecek en hızlı önlemlerden biridir. Tüm kurumsal telefon ve tabletlerin uygulama ve işletim sistemi güncellemelerini otomatik olarak yükleyecek şekilde ayarlandığından emin olun. Çoğu güncelleme gece saatlerinde sessizce yüklenebilir ve kullanıcıların bunları takip etme yükünü ortadan kaldırır. Kısa bir yeniden başlatma işlemi, cihazların korunmasına yardımcı olur.
3. **Net ve Basit Bir Güncelleme Politikası Oluşturun:** Kuralları kolay anlaşılır hale getirin. İş amaçlı kullanılan cihazların güncel tutulması gerektiğini açıkça belirtin. Çalışanları güncelleme bildirimi aldıklarında güncellemeyi yüklemeye veya cihazlarını gece boyunca açık bırakmaya teşvik edin. Aylık kısa bir "güncelleme kontrolü" alışkanlığı oluşturmak faydalı olabilir.
4. **Mümkün Olduğunca Takip ve Yönetim Araçları Kullanın:** Halihazırda mobil cihaz yönetimi veya güvenlik araçları kullanıyorsanız, bunların izleme özelliklerinden yararlanın. Birçok çözüm, güncelleme almayan veya eski yazılım kullanan cihazları tespit edebilir. Bazıları ise gerekli güncellemeler yapılana kadar kurumsal sistemlere erişimi kısıtlayabilir.
5. **Kritik Güvenlik Güncellemelerinde Hızlı Hareket Edin:** Önemli bir güvenlik açığı gündeme geldiğinde veya bir üretici acil güvenlik güncellemesi yayımladığında vakit kaybetmeyin. Ekibinizi hızlı ve açık bir şekilde bilgilendirin, cihazlarını güncellemeleri için yönlendirin.

Mobil Güvenlik Her Zamankinden Daha Önemli

Bu raporda ele alınan temel risklerin her biri için uygulanabilecek etkili korunma yöntemleri bulunmaktadır. IT kaynakları sınırlı olsa bile, her ölçekteki işletme güvenliğini güçlendirmek için hemen uygulanabilecek pratik ve yönetilebilir adımlar atabilir. Çalışanların oltalama girişimlerini fark edip bunlardan kaçınmalarına yardımcı olmak, uygulamaların hangi kaynaklardan indirileceği ve hangi verilere erişebileceği konusunda net kurallar belirlemek ve cihazları güncel tutmak, işletmelerin mobil güvenlik seviyelerini önemli ölçüde artırabilir. Bunların hiçbiri büyük bütçeler gerektirmez; temel güvenlik uygulamalarına odaklanmak ve gerektiğinde uzman iş ortaklarından destek almak yeterlidir.

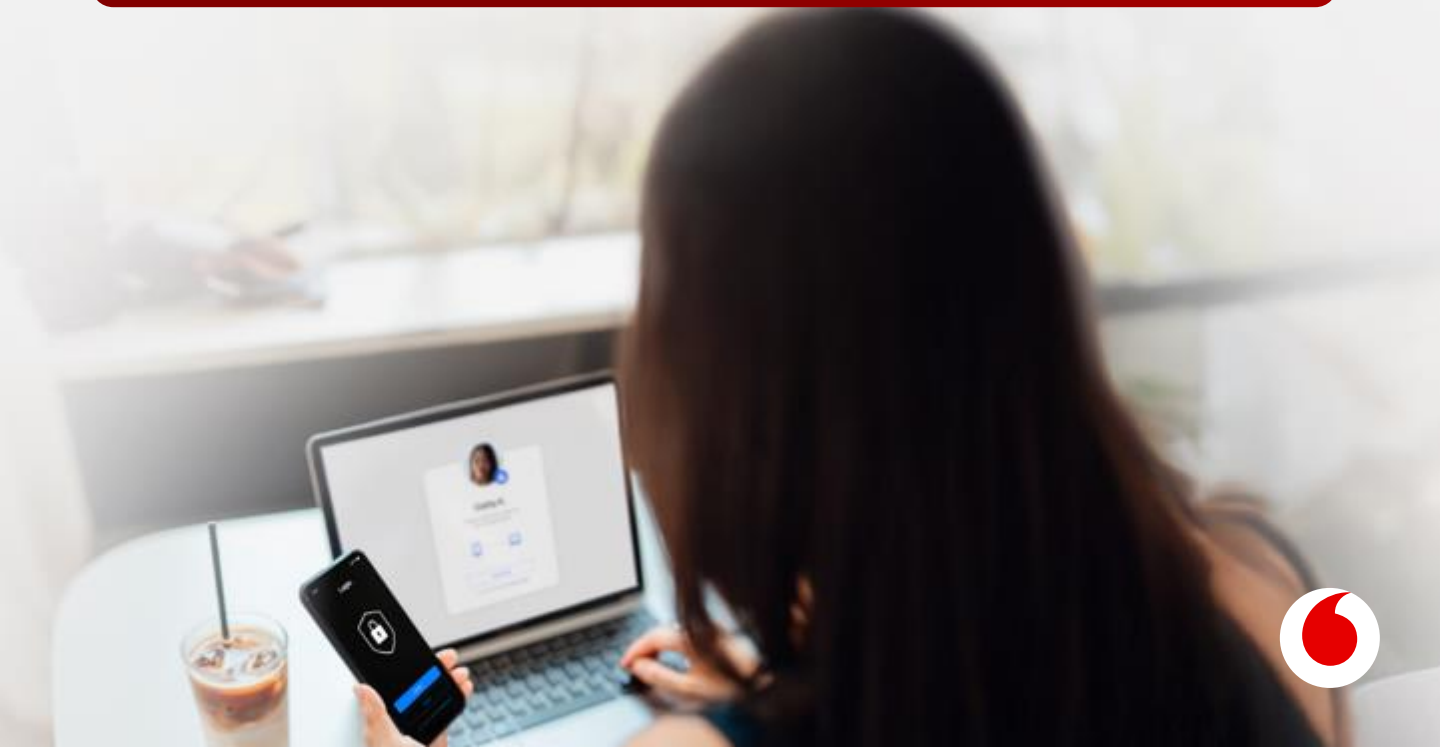
Bu üç alana odaklanmak, mobil güvenliği güçlendirmek için akıllı ve gerçekçi bir başlangıç noktasıdır. Bunları, mobil güvenlik zincirinizde en fazla güçlendirilmesi gereken üç temel halka olarak düşünebilirsiniz: insanlar ve verdikleri kararlar (oltalama saldırıları), yükledikleri uygulamalar (zararlı yazılımlar) ve cihazlarında çalışan yazılımlar (güncellemeler).

Vodafone Business olarak iyimseriz. Riskler gerçektir ancak çözümler her işletmenin erişebileceği kadar yakındır. Doğru farkındalık ve basit, proaktif adımlarla işletmeler; mobil teknolojilerin sunduğu verimlilikten ve esneklikten gereksiz güvenlik endişeleri yaşamadan faydalanabilir. Önemli olan bir olay yaşandıktan sonra tepki vermek değil, önceden harekete geçmektir.

Dikkatli bir yaklaşım, günlük güvenlik alışkanlıkları ve Vodafone gibi iş ortaklarının desteğiyle işletmeler güçlü bir mobil güvenlik yapısı oluşturabilir ve mobil öncelikli çalışma modelinin sunduğu avantajlardan güvenle yararlanabilir.

Vodafone olarak ağlarımızı bağımsız testlerden geçirerek ve sektör iş ortaklarımızla birlikte çalışarak güvenlik standartlarını sürekli yükseltmeye devam ediyoruz. Güvenliği ağın temel bir parçası haline getirirken, teknik olmayan saldırıların giderek artması kullanıcıların da güvenliğin sağlanmasında kritik bir rol üstlenmesini gerektiriyor.

Pedro Peixe Ribeiro, Siber Güvenlik Direktörü Security Vodafone Business



Neden Vodafone Business?

İşletmelerin, yapay zekâ destekli tehditlerin artması da dâhil olmak üzere günümüzün en büyük siber güvenlik zorluklarıyla mücadele edebilmesine yardımcı olmak için dünyanın önde gelen teknoloji sağlayıcılarıyla birlikte çalışıyoruz.

Küresel tehdit istihbaratı, gelişmiş teknolojiler ve uzman desteğini bir araya getirerek her ölçekteki işletmenin güvende kalmasına yardımcı oluyoruz. Çünkü her kuruluşun güçlü ve erişilebilir siber güvenlik çözümlerine sahip olması gerektiğine inanıyoruz.

Bu nedenle, işletmeler için Çalışan Güvenliği çözümlerimiz ile, çalışanlarınızı nerede olurlarsa olsunlar korumak üzere basit ve uygun maliyetli çözümler sunuyoruz.

Çalışan Güvenliği çözümlerimiz nelerdir?

Domain Risk Analizi

Web domain'inizi sürekli izleyerek güvenlik açıklarını gerçek zamanlı olarak tespit eder ve giderilmesine yardımcı olur.

Güvenlik Farkındalığı ve Eğitim

Sosyal Mühendislik Hizmetimiz, oltalama simülasyonu ve farkındalık eğitimleri gibi kullanıcı davranışlarından faydalanan siber saldırı risklerini azaltmanıza ve ekiplerinizin daha güçlü güvenlik alışkanlıkları geliştirmesine yardımcı olur.

E-posta ve Bulut Güvenliği

Trend Micro ve Microsoft çözümleriyle cihazlar, e-posta sistemleri, bulut uygulamaları ve web erişimi için kapsamlı koruma sağlar.

Mobil Tehdit Yönetimi

Lookout Mobile Security, mobil tehditlere karşı koruma sağlamak için dünyanın en büyük yapay zekâ destekli veri kümelerinden yararlanır.

Ayrıca şunları da sunuyoruz

Yönetilen Güvenlik Hizmetleri

Vodafone Business Siber Güvenlik ürün portföyü içindeki birçok çözüm için yönetim hizmeti de sunuyoruz, böylece tüm güvenlik süreçlerini tek başınıza yönetmek zorunda kalmazsınız.

Ağ Güvenliği

Bağlantılarınızı ve IT altyapınızı güvence altına almak üzere, güvenlik duvarı (Firewall), DDoS Atak Önleme Hizmeti ve IPS gibi gelişmiş ağ güvenliği hizmetleri sunuyoruz.

İş Ortaklarımıza Teşekkürler

Microsoft Lookout TREND MICRO FORTINET

Daha fazla bilgi ve işletmenize özel siber güvenlik çözümleri için Vodafone Business'i ziyaret edin.

vodafone business

Nasıl Güvende Kalırsınız?

- Resmî kanallar üzerinden doğrulama yapın.
- Şifrelerinizi ve çok faktörlü kimlik doğrulama (MFA) kodlarınızı asla paylaşmayın.
- Aciliyet hissi yaratan taleplerde durup düşünün; bu önemli bir uyarı işareti olabilir.
- Şüpheli gördüğünüz her durumu şirketinizin IT veya güvenlik ekiplerine bildirin.

E-posta

Acil işlem gerekiyor!

→ **"Şifreniz ele geçirildi sıfırlamanız gerekiyor."**

Dikkat edilmesi gereken işaretler

- Tanımadığınız gönderici
- Beklenmedik bağlantılar (linkler)
- Aciliyet yaratan dil ve ifadeler

Kısa Mesaj (SMS)

Gönderiniz gecikti.

→ **"Doğrulamak için hemen tıklayın!"**

Dikkat edilmesi gereken işaretler

- Tanımadığınız numara
- Kısaltılmış bağlantılar (URL'ler)
- Aciliyet içeren ifadeler

Telefon Araması

IT ekibinden arıyorum...

→ **"Kodunuzu 30 saniye içinde paylaşın!"**

Dikkat edilmesi gereken işaretler

- Baskı kurmaya çalışma
- Hassas bilgi talebi
- Tanımadığınız arayan kişi

Sosyal Medya

Fotoğraftaki siz misiniz?

→ **"Görmek için tıklayın, aksi takdirde hesabınız silinecektir."**

Dikkat edilmesi gereken işaretler

- Sahte profiller
- Beklenmedik özel mesajlar
- Şüpheli görünen bağlantılar