AĞUSTOS 2026 · FARKINDALIK SERİSİ

TATİL SEZONU DOLANDIRICILIĞI

Sahte Rezervasyon ve Kampanya Tuzakları

Dolandırıcılar nasıl çalışıyor · Otelin rezervasyon hesabı nasıl ele geçiriliyor
Otel Wi-Fi ağlarının riskleri · Rezervasyon öncesi ve sonrası kontrol listesi
Nisan 2026 Booking.com veri ihlali · Dolandırıldıysanız ilk saatlerde ne yapmalı

SPARTA SİBER GÜVENLİK

Bu Sayıda

Sparta Siber Güvenlik, kuruluşların siber güvenlik ihtiyaçları için 2013 yılında kurulmuştur. Bugüne kadar 1000'in üzerinde siber güvenlik eğitimi, danışmanlık ve sızma testi projesi gerçekleştirmiştir. Bu farkındalık serisiyle, hem bireylerin hem de kurumların gündelik hayatta karşılaştığı güncel siber tehditleri aylık olarak ele alıyoruz.

Bu ay, yaz sezonuyla birlikte artan sahte rezervasyon dolandırıcılığını inceliyoruz. Kullanılan yöntemleri, en bilinen rezervasyon sitelerinden birinde yaşanan bir hesap ele geçirme vakasını ve yetkili kurumların uyarılarını bir araya getirdik.

Rezervasyon öncesinde ve sonrasında atılabilecek somut adımlara da yer verdik. Ayrıca yirmi yılı aşkın tecrübeye sahip bir siber güvenlik uzmanının bu konudaki gözlemlerini son sayfalarda bulacaksınız.

GİRİŞ

Bu Yaz Neler Değişti

Yaz sezonunun hareketlenmesiyle birlikte, özellikle popüler tatil bölgelerinde sahte rezervasyon vakaları belirgin şekilde artıyor. Dolandırıcılar otel ve villa işletmelerinin adını kullanarak gerçeğine çok benzeyen web siteleri ve sosyal medya hesapları oluşturuyor.

Tatilcilerden kapora veya konaklama ücretini doğrudan banka hesabına göndermelerini istiyorlar. Ödeme yapıldıktan sonra iletişim kesiliyor. Tatilciler tesise ulaştıklarında adlarına herhangi bir rezervasyon yapılmadığını öğreniyor.

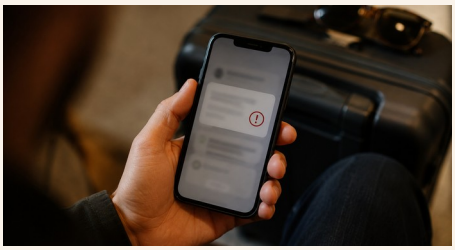
> **Sahte rezervasyon girişimlerinde geçen yıla göre yaklaşık yüzde 10 artış yaşandı.**
>
> ALİŞİR ŞAHİN · BODER BAŞKAN YARDIMCISI

Benzer vakalar yalnızca Türkiye'ye özgü değil. İlerleyen sayfalarda, dünyanın en meşhur rezervasyon sitelerinden birinde işleyen ve çok daha teknik olan bir saldırı türünü de ele alıyoruz. Bu kez hedef alınan sahte bir site değil, otelin kendi hesabı.

Sektör temsilcileri bu durumun yalnızca bireysel mağduriyet yaratmadığını, tatil bölgesine ve turizm sektörüne duyulan güveni de zedelediğini vurguluyor. Bu sayıda dolandırıcıların kullandığı yöntemleri ve ailenizi veya ekibinizi nasıl koruyabileceğinizi anlatıyoruz.

YÖNTEMLER

Dolandırıcılar Nasıl Çalışıyor



Bu yaz sık karşılaşılan beş dolandırıcılık yöntemi öne çıkıyor. Çoğu vakada bu yöntemler tek başına değil, birkaçı bir arada kullanılıyor. Ortak noktaları, tüketiciye ödeme sonrasında başvurabileceği bir muhatap bırakmamaları.

Sahte site ve sosyal medya hesabı

Gerçek bir işletmenin adını taşıyan, gerçeğine çok benzeyen web sitesi ya da sosyal medya hesabı üzerinden rezervasyon alınması. Çoğu vakada alan adında yalnızca tek bir harf değiştiriliyor veya uzantı farklılaştırılıyor. Gerçek fotoğraflar da kullanıldığı için adres satırına bakmadan ayırt etmek neredeyse imkânsız.

Var olmayan villa ve bungalov ilanı

Gerçekte mevcut olmayan veya ilanı verenin kiralama yetkisi bulunmayan konaklama yerlerinin kiraya verilmiş gibi gösterilmesi, genellikle ödeme sonrası ortaya çıkıyor.

Acele ettirici kampanya dili

“Son iki oda”, “bugüne özel yüzde 70 indirim” gibi ifadelerle hızlı ve düşünmeden ödeme yapılması için baskı oluşturulması, doğrulama adımlarının atlanmasını hedefliyor.

IBAN'a doğrudan kapora talebi

Konaklama bedelinin veya kaporanın, kurumsal bir hesap yerine doğrudan kişisel bir banka hesabına gönderilmesinin istenmesi, tek başına ciddi bir uyarı işaretidir.

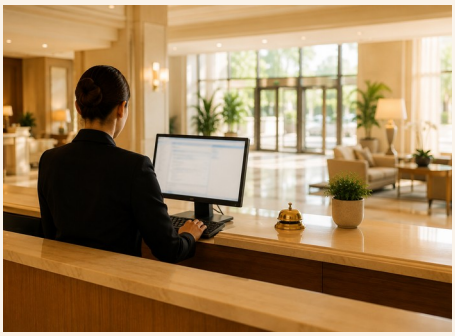
Kopyalanmış otel sayfası

Gerçek bir işletmenin fotoğraf ve açıklamalarının izinsiz kopyalanarak başka bir rezervasyon kanalında, çoğu zaman işletmenin haberi bile olmadan yeniden yayınlanması.

BOOKING.COM

Hesabınız Değil, Otelin Hesabı Ele Geçiriliyor

Yazar: Sinem Başaran



Booking.com, dünyanın önde gelen çevrimiçi rezervasyon platformlarından biri ve 220'den fazla ülke ve bölgede hizmet veriyor. Şirketin kendi verilerine göre 2010'dan bu yana platform üzerinden 6,8 milyar konaklama rezervasyonu yapıldı. Gezginler konaklamadan tatil evlerine, araç kiralamadan uçuş seçeneklerine kadar birçok ihtiyacını bu platform üzerinden karşılıyor.

Sistem hem bireysel kullanıcılar hem de oteller için büyük kolaylık sağlıyor, rezervasyon yönetimini hızlandırıyor ve otellere doğrudan müşteriyle iletişim imkânı veriyor. Ancak böylesine büyük bir platform olunca haliyle siber suçluların da hedefi haline geliyor.

Özellikle 2023 yılı itibarıyla, site üzerinde gerçekleştirilen siber saldırıların ve dolandırıcılıkların arttığına tanık oluyoruz. Güvenlik şirketi Secureworks, Ekim 2023'te incelediği bir olayda otel personeline Vidar adlı bilgi hırsızı yazılımın bulaştırıldığını ve otelin Booking.com yönetim paneli erişiminin çalındığını belgeledi. Aynı araştırma, ele geçirilen bu panel hesaplarının siber suç forumlarında 2.000 dolara kadar satıldığını ortaya koydu.

Aralık 2024'ten itibaren ise Microsoft'un Storm-1865 olarak takip ettiği ayrı bir grup, konaklama sektörünü ClickFix adı verilen yeni bir yöntemle hedef almaya başladı. Bu yöntemde kullanıcıya sahte bir hata mesajı gösteriliyor ve sorunu çözmesi için bir komutu kopyalayıp çalıştırması isteniyor. Microsoft kampanyayı Mart 2025'te belgeledi.

Booking.com'un kendisi de bu artışı doğruluyor. Şirketin internet güvenliği sorumlusu Marnie Wilking, Haziran 2024'te Toronto'daki Collision konferansında, üretken yapay zekanın yaygınlaşmasıyla birlikte seyahat dolandırıcılıklarının son bir buçuk yılda yüzde 500 ile 900 arasında arttığını söyledi.

Geçtiğimiz günlerde bir yakınımın başına da benzeri bir olay gelince bu konuyu araştırmaya karar verdim. Aşağıda saldırının nasıl işlediğini ve hem otel yöneticilerinin hem de müşterilerin ne yapabileceğini anlattım.

Saldırı Yöntemleri: Otel Personelinin Bilgisayarlarının Zararlı Yazılımla Enfekte Edilmesi

Bu siber saldırıların temelinde, otel personelinin bilgisayarlarına zararlı yazılım bulaştırılması yer alıyor. Çok aşamalı bir yapıya sahip olan bu yöntem, öncelikli olarak otelin kendisinden ziyade müşterileri hedef alıyor.

BOOKING.COM · DEVAM

Şifre Çalma Yazılımı (Password Stealer) ile Saldırılar

Saldırganlar, admin.booking.com hesaplarını ele geçirmek için şifre çalma yazılımları kullanıyor. Bu zararlı yazılımlar, enfekte olan bilgisayarlardaki kayıtlı tüm şifreleri topluyor. Ancak bu durumda siber suçluların asıl ilgilendiği hedef, Booking.com hesapları oluyor.

Hedefli Kimlik Avı (Phishing) Saldırıları

Bu tür bir saldırı genellikle zararsız gibi görülen bir e-postayla başlıyor. Saldırganlar, kendilerini otelin eski bir müşterisi gibi tanıtarak kayıp belgeler konusunda yardım talep ediyor. E-postaların içeriği genellikle şu adımları içeriyor.

- **Masum Talep:** "Kayıp bir pasaportu arıyorum" gibi bir bahaneyle otel personelinden yardım isteniyor.
- **Sahte Bağlantı:** Yardıma yönelik bir dosya veya fotoğrafların yer aldığı söylenen bir bağlantı paylaşılıyor.
- **Zararlı Yazılım Yüklenmesi:** Bağlantıdaki dosya indirildiğinde, zararlı yazılım bilgisayara bulaşıyor ve kayıtlı şifreleri toplayarak siber suçlulara iletiyor.

Alternatif Bir Yöntem: Sahte Rezervasyonlar

Bazı durumlarda siber suçlular, sahte müşteri hesapları oluşturarak veya çalınmış müşteri hesaplarını kullanarak otel rezervasyonları yapıyor. Daha sonra, Booking.com'un dahili mesajlaşma sistemi aracılığıyla zararlı yazılım içeren bir dosya veya bağlantı gönderiyor. Bu yöntemde de, zararlı yazılım bulaşan bilgisayarlardaki şifreler ele geçiriliyor.

Ele Geçirilen Hesapların Kullanılması

Zararlı yazılımın topladığı bilgilerle admin hesapları ele geçirildikten sonra siber suçlular şu adımları izliyor.

1. **Rezervasyon Bilgilerinin İncelenmesi**
   Siber suçlular, otelin gelecekteki rezervasyon bilgilerine erişim sağlıyor. Bu bilgiler müşterilerin iletişim ve rezervasyon ayrıntılarını içerdiği için, son derece inandırıcı dolandırıcılık mesajları hazırlanmasına imkân veriyor.

2. **Sahte Mesajlar Gönderilmesi**
   Ele geçirilen hesaplar aracılığıyla, müşterilere profesyonelce hazırlanmış mesajlar gönderiliyor. Bu mesajlarda, müşterilerin ödeme bilgilerinde bir hata olduğu veya rezervasyonlarının iptal edileceği belirtiliyor.

3. **Taklit Web Siteleri**
   Müşteriler, Booking.com'u taklit eden sahte web sitelerine yönlendiriliyor. Bu siteler Booking.com'un tasarımını ve kullanıcı arayüzünü gerçekçi biçimde kopyalıyor, girilen ödeme bilgileri doğrudan siber suçluların eline geçiyor.

BOOKING.COM · DEVAM

İngiltere'nin resmi dolandırıcılık bildirim birimi Action Fraud'a göre, Haziran 2023 ile Eylül 2024 arasında bu tür Booking.com dolandırıcılığıyla ilgili 532 bildirim yapıldı ve 370 bin sterlin kayıp yaşandı.

13 NİSAN 2026

Booking.com veri ihlalini doğruladı

Booking.com, yetkisiz üçüncü kişilerin bazı misafir rezervasyon bilgilerine erişmiş olabileceğini doğruladı. Ad, e-posta, telefon numarası, rezervasyon ayrıntıları ve tesisle paylaşılan bilgiler etkilendi. Finansal bilgilere erişilmedi, ilgili rezervasyonların PIN kodları yenilendi. Erişimin hangi sistem üzerinden sağlandığı ve kaç müşterinin etkilendiği kamuoyuyla paylaşılmadı.

- Olayın hemen öncesinde, gerçek rezervasyon ayrıntıları içeren WhatsApp oltalama mesajları bildirildi. Rezervasyonunuzu bilen bir mesaj, doğru olduğu anlamına gelmiyor.
- Bağlantıya tıklamak yerine uygulamayı veya adresi kendiniz açıp rezervasyonunuzu kontrol edin.
- Sizi platform dışına veya harici bir ödeme sayfasına yönlendiren talebe yanıt vermeyin.

Peki Ne Yapmalı?

Oteller İçin

- **Parola Yönetimi:** Parolaları tarayıcıda kaydetmeyin, parola yöneticisi kullanın.
- **Cihaz Güvenliği:** Tüm iş cihazlarında antivirüs bulundurun ve güncel tutun.
- **Çalışan Bilinci:** Şüpheli e-posta ve dosyalar konusunda personeli düzenli eğitin.
- **Düzenli Kontroller:** Güncellemeleri aksatmayın, bilinen açıkları kapatın.

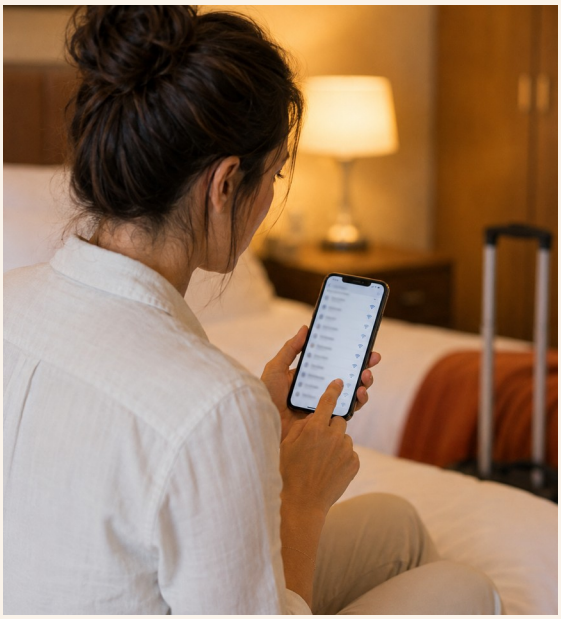
Müşteriler İçin

- **Bağlantıyı Kullanmayın:** Mesajdaki bağlantı yerine uygulamayı veya adresi kendiniz açarak rezervasyonunuzu kontrol edin.
- **Adres Satırını Okuyun:** Orijinal adresle uyuşmayan bağlantılara tıklamayın. Ödeme sizi platform dışına çıkarıyorsa durun.
- **İki Faktörlü Doğrulama:** Parolanız sızsa bile hesabın ele geçirilmesini zorlaştırır.

AĞ GÜVENLİĞİ

Otelin Kablosuz Ağına Bağlanırsak Başımıza Ne Gelebilir?

Tatilde oda anahtarını alır almaz yaptığımız ilk işlerden biri otelin Wi-Fi ağına bağlanmak oluyor, ama bu ağlar göründüğünden çok daha az güvenli olabiliyor. Bazı kötü niyetli kişiler, otelin gerçek ağıyla aynı veya çok benzer isimde sahte bir ağ oluşturabiliyor.



Telefonunuz veya bilgisayarınız bu sahte ağı gerçeğinden ayırt edemeyebiliyor, özellikle daha önce bağlandığınız ağlara otomatik bağlanma özelliği açıksa. Böyle bir ağa bağlandığınızda, o ağı kuran kişi sizinle internet arasına bir nevi girmiş oluyor, yani gönderdiğiniz ve aldığınız bilgilerin bir kısmını görebiliyor.

Sahte ağlar sizi taklit giriş sayfalarına yönlendirebiliyor, hangi servislere bağlandığınızı izleyebiliyor ve güvenli bağlantı kullanmayan uygulama ya da sitelerde aktarılan bilgileri ele geçirebiliyor. Güvenli bağlantı kullanan sitelerde içerik şifreli kalıyor, ancak sahte giriş sayfaları ve yönlendirmeler hâlâ ciddi risk oluşturuyor. Otelin gerçek ağına bağlansanız bile risk tamamen ortadan kalkmıyor, çünkü birçok otelde ağ altyapısı güncellenmemiş oluyor.

Ne Yapmalı

- Wi-Fi ağına bağlanmadan önce ağ adını cihazdaki listeden değil, resepsiyondan sözlü olarak doğrulayın.
- Otel Wi-Fi'sindeyken bankacılık işlemi yapmaktan kaçının, hassas işlemler için mobil verinizi tercih edin.
- Mümkünse bir VPN uygulaması kullanarak bağlantınızı daha güvenli hale getirin.
- Cihazınızın bilinen ağlara otomatik bağlanma özelliğini kapatın.

SAHADAN

Sahada Neler Yaşanıyor

Villa ve bungalov kiralamalarında da benzer bir tablo görülüyor. Tüketici hakları kuruluşlarına ulaşan şikayetlerin önemli bir kısmı bu iki kategoride toplanıyor. İşletmeler, bu dolandırıcılıkların kendi bilgileri ve iradeleri dışında gerçekleştirildiğini belirtiyor. Mağduriyet yalnızca tatilciyle sınırlı kalmıyor, işletmelerin itibarını da etkiliyor.

BODER Başkan Yardımcısı Alişir Şahin, turizmin güven üzerine kurulu bir sektör olduğunu hatırlatarak yaşanan her dolandırıcılık olayının destinasyonların ve sektörün itibarına zarar verdiğini vurguluyor. Şahin ayrıca sahte rezervasyon yöntemlerinin her yıl daha profesyonelleştiğini, dolandırıcıların artık yalnızca otel fotoğraflarını değil logoları ve kurumsal kimlikleri de birebir kopyaladığını belirtiyor.

Yetkililer Ne Diyor

Emniyet birimleri, tatil dönemlerinde artan sahte rezervasyon girişimlerine karşı vatandaşları düzenli olarak uyarıyor. Seyahat acentesinin kaydını TÜRSAB'ın acenta arama sistemini veya Kültür ve Turizm Bakanlığı'nın seyahat acentası sorgulama sayfasını kullanabilirsiniz. Konaklama tesisleri TÜRSAB kapsamında değil, turizm işletme belgeleri Kültür ve Turizm Bakanlığı kayıtlarından doğrulanır. Uyarılarda öne çıkan üç temel kontrol şöyle.

YETKİLİ UYARISI

Güvenli rezervasyon için üç temel kontrol

Ödeme yapmadan önce kısa bir duraklama, büyük bir mağduriyeti önleyebilir.

Fiyatı Doğrula

Aşırı düşük fiyatları ve cazip teklifleri bağımsız kaynaklardan karşılaştırın.

Kaydı Kontrol Et

Acentenin TÜRSAB, tesisin Bakanlık kaydını resmi kanallardan doğrulayın.

Güvenli Öde

Ödemeyi kurumsal ve güvenli sistemler üzerinden yapın, doğrulanamayan IBAN'lardan kaçının.

KONTROL LİSTESİ

Rezervasyon Öncesi ve Sonrası

Rezervasyon Yapmadan Önce

- Seyahat acentesinin TÜRSAB kaydını, konaklama tesisinin ise Kültür ve Turizm Bakanlığı kaydını bir önceki sayfadaki araçlarla doğrulayın.
- Piyasa fiyatının çok altındaki tekliflere ve “hemen ödeyin” baskısına karşı temkinli olun.
- Sosyal medyada gördüğünüz ilanı işletmenin resmi web sitesiyle karşılaştırın.
- Yalnızca site içi yorumlara değil, bağımsız değerlendirmelere de bakın.
- İşletmenin telefon numarasını arayarak rezervasyonu sözlü teyit edin.

Rezervasyon Sırasında ve Sonrasında

- Ödemeyi yalnızca güvenli ödeme sistemleri üzerinden yapın, doğrulanamayan bir IBAN'a ödeme yapmayın.
- Rezervasyon onayını, sözleşmeyi ve faturayı yazılı olarak alın ve saklayın.
- Mümkün olduğunda kredi kartıyla ödeme yapın, şüpheli işlemlerde harcama itirazında bulunabilirsiniz.
- Tesise varmadan birkaç gün önce rezervasyonunuzu tekrar teyit edin.
- Herhangi bir tutarsızlık fark ederseniz ödeme öncesinde işlemi durdurun.

Dolandırıldığınızı Fark Ettiyseniz

Bir dolandırıcılık durumuyla karşılaştığınızda hızlı ve etkili bir şekilde hareket etmek önemlidir. İlk saatlerde izlenecek adımlar şöyle.

DOLANDIRILDIYSANIZ

İlk saatlerde izlenecek müdahale akışı

Önce finansal zararı sınırlayın, ardından hesapları güvene alın ve resmi bildirimleri tamamlayın.

1. **Bankayı Ara** — Ödemenin durdurulmasını veya kartın bloke edilmesini isteyin.
2. **Kanıt Sakla** — Mesajları, dekontları ve ekran görüntülerini kaydedin.
3. **Şifreleri Gözden Geçir** — Sahte sayfaya parola girdiyseniz aynı parolalı hesapları güncelleyin.
4. **Resmî Başvuru Yap** — Cumhuriyet Başsavcılığına ya da en yakın polis veya jandarma birimine
5. **Platformu Bildir** — Kullanılan hesabı ve gerçek işletmeyi bilgilendirin.
6. **Hesabı İzle** — Kart ve banka hesaplarındaki şüpheli işlemleri takip edin.

ACİL · İlk iki adım en kısa sürede

KAYIT VE BİLDİRİM · Resmi başvuruları geciktirmeyin

UZMAN GÖRÜŞÜ

Yirmi Yıllık Saha Tecrübesi Ne Gösteriyor

Yazar: Alper Başaran

Yirmi yılı aşkın süredir bu işi yapıyorum ve tatil dolandırıcılığı vakalarında en sık duyduğum cümle şüphesiz şu: "Ben aslında dikkatli biriyimdir." Mağdurların büyük çoğunluğu dikkatsiz insanlar değil, dikkatsiz bir anlarında yakalanmış insanlar oluyor.

Buraya kadar yöntemleri ve alınacak önlemleri anlattık. Bu bölümde bir adım geri çekilip başka bir soruya cevap vermek istiyorum: bu kadar basit görünen bir dolandırıcılık, nasıl hâlâ etkili olabiliyor?

Karşınızdaki kişi size oda satmıyor, sizden zaman satın alıyor

Bu konudaki yaygın varsayımlardan biri, dolandırıcının bir sahte ilan hazırlayıp şansını denediğidir. İşin aslı, bunun çoğunlukla istatistiksel bir yaklaşımla ortaya çıktığıdır. Sahte bir site kurmanın maliyeti neredeyse sıfıra indi. Hazır şablonlar, dakikalar içinde yayına alınan ödeme sayfaları ve kiralık altyapılar var. Bu sayede çok ufak maliyetlerle yapılabilir hale geldi. Bunun sonucunda dolandırıcılar, ikna oranlarını yükseltmeye çalışmaktansa daha çok kişiye ulaşmayı tercih ediyor.

Bunu okuyacak pek çok kişi gibi siz de belki içinizden "canım, sitenin sahte olduğu belli, ne saf insanlar var" diye düşünebilirsiniz. Doğrudur, sahte siteler çok yoğun çalışmalar sonucunda yüzde 100 gerçekçi hale getirilmeye çalışılmıyor zaten. Sizin kadar dikkatli ve bilgili olmayan birini, ya da sizin gibi dikkatli birinin boş bir anını yakalamaya çalışıyorlar. Dolandırıcılar dikkatli bireyleri hedef almıyor, hatta çoğu örneğe baktığımda sayfaları bilerek yalapşap yaptıklarını bile düşünüyorum. Böylece dikkatli kişiler hemen çıkıyor, kalanlar ise daha kolay hedef oluyor.

İkinci ve daha az konuşulan nokta ise zamanlama. Erken rezervasyonla önceden ödenip ağustosta kullanılan bir tatil, dolandırıcıya haftalarca fark edilmeme süresi verir. Bu tür dolandırıcılıkların yaz aylarında artmasının bir sebebi de tatil heyecanı kadar bu zaman farkı olabilir. Erken rezervasyon dönemleri bu yüzden tüketici için avantajlı olduğu kadar saldırgan için de verimli bir dönemdir.

Yirmi yılda değişen şey saldırganın zekâsı değil, maliyetler oldu. Eskiden emek isteyen sahtecilik, bugün birkaç dakikalık bir işleme dönüştü.

UZMAN GÖRÜŞÜ · DEVAM

Sahada tekrar eden kalıplar

Bazı örneklerde sorunu yaratanla çözenin aynı kişi olduğu görülüyor. Tam güvenemedikleri ilanı teyit etmek için ilandaki numarayı arıyorlar. Karşılarına son derece profesyonel bir karşılama mesajı ve devamında tipik bir çağrı merkezi muhatabı çıkıyor. Bu durumda doğrulama sanılan şey doğrulama değildir. "Aradım, telefona çıktılar" cümlesini kaç kere duyduğumu hatırlamıyorum. Ama aranan numara, ilanın üzerindeki numaradır.

Sahte bir belgeyi kendi üzerindeki bilgiyle doğrulamak gibi düşünün. Geçerli tek yöntem, bilgiyi bağımsız bir kaynaktan yeniden bulmaktır: resmî kayıt, platformun kendi uygulaması, işletmenin arama motorundan ayrıca teyit edilen kurumsal sayfası.

Zarar, ödemeyi yapanla sınırlı kalmıyor. Aile, arkadaş grubu veya kurumsal seyahat organizasyonlarında ödemeyi genellikle tek bir kişi yapar. O kişi hem maddi kaybı hem de sosyal sorumluluğu tek başına taşır. Bildirim oranlarının bu kadar düşük olmasının sebeplerinden biri de bu olabilir: mağdur, olayı bildirmeden önce kendini savunmak zorunda hisseder.

Kontrol listeleri neden tek başına yetmiyor

Önceki sayfalarda bir kontrol listesi verdik ve o listenin her maddesi doğru. Ama gördüğümüz şu: listeler sakin bir masada, tek bir karar verici için yazılır. Gerçek karar ise telefonda, akşam saatlerinde, "bu fiyat kaçmasın" baskısıyla ve çoğu zaman yanınızdaki birine cevap yetiştirirken verilir.

Asimetrik bir durum daha var. Dolandırıcı yalnızca bir maddede sizi ikna etmek zorundadır, siz ise hiçbir maddede yanılmamak zorundasınız.

> **Dolandırıcı yalnızca bir maddede sizi ikna etmek zorundadır, siz ise hiçbir maddede yanılmamak zorundasınız.**
>
> ALPER BAŞARAN

Bu yüzden kontrol listelerini "karar anında bakılacak bir belge" olarak değil, "arama başlamadan önce konulmuş bir kural" olarak kullanmak gerekiyor. Aradaki fark küçük görünür ama sonucu belirler. Ailelere ve kurumlara önerdiğim üç kural şu:

1. **Platform dışına çıkılmaz**
   İşlem bilinen ve güvenilir bir platform dışında yapılmaz, bunun istisnası olmamalıdır. İstisna talebinin gelmesi zaten uyarı işaretidir.

2. **Tek kişi onaylamaz**
   Belli bir tutarın üzerindeki ödemeyi tek kişi onaylamaz. İkinci bir kişinin sadece "bu ilanı nerede gördün?" diye sorması, vakaların önemli bir kısmını durdurur.

UZMAN GÖRÜŞÜ · DEVAM

3 **İlk saatlerde ödeme yapılmaz**

Hiçbir ödeme, talep edildiği ilk saatlerde yapılmaz. Bir gece bekleyen teklif, çoğu zaman kendini ele verir.

Bu üç kuralın ortak özelliği bilgi değil, süre kazandırmalarıdır. Meşru bir işletme sizin yirmi dört saat beklemenize itiraz etmez. Baskının yönü, teklifin içeriğinden daha güvenilir bir göstergedir.

İşletme tarafında gördüğüm yapısal zaaflar

Otel, acente ve villa ile bungalov işletmelerine verdiğimiz danışmanlıklarda, sorunun neredeyse hiçbir zaman "bilinçsiz personel" olmadığını söyleyebilirim. Sorun süreçlerin tasarımındadır.

- **Rezervasyon personelinin işi, tanımadığı kişilerden gelen dosyaları açmaktır.** Bu çalışana "şüpheli ek açma" demek, işini yapmamasını istemektir. Kalıcı çözüm eğitimle sınırlı kalmaz, riski başka yere taşımaktır. Misafir belgelerinin açıldığı cihaz ile rezervasyon paneline girilen cihazın ayrılması bile etkili önlemlerden biri olabilir.
- **Asıl kaybedilen şey parola değil, oturumdur.** Bir olaydan sonra yalnızca parola değiştirmek çoğu zaman yetersiz kalır, aktif oturumların da sonlandırılması gerekir. Aksi hâlde saldırgan iki faktörlü doğrulamaya hiç takılmadan içeride kalmaya devam eder.
- **Ortak hesaplar en sık rastladığım yapısal zaaf.** Panele "rezervasyon@" gibi paylaşılan bir hesapla girilen her işletmede, bir sorun yaşandığında kimin ne yaptığını bilme imkânı yoktur. Kişiye özel kullanıcı tanımlamak maliyetsizdir ve olay sonrası incelemenin tamamını mümkün kılar.
- **Dışarıdan yürütülen sosyal medya ve rezervasyon yönetimi.** Hesaplara erişimi olan ajans bilgisayarları çoğu envanterde yer almaz. İşletme kendi tarafını güvenceye alsa bile kapı açık kalabilir.

Kimsenin sormadığı soru şu: "Şu anda rezervasyon panelimize benden başka biri giriş yapmış olsa, bunu fark eder miydik?" Küçük ve orta ölçekli işletmelerin büyük bölümünde bu sorunun cevabı hayırdır. Giriş bildirimlerini açmak ve aktif oturumları düzenli olarak gözden geçirmek, bu cevabı evete çevirir.

Son olarak: mesajı değil, yolu doğrulayın

Uzun süredir sıradan kullanıcının elindeki en pratik tespit yöntemi dildi. Bozuk cümleler, garip çeviriler, tutmayan kurumsal ton. İnsanlara "yazıma dikkat edin" derdik ve bu gerçekten işe yarardı. Üretken yapay zekâ bunu ortadan kaldırdı. Bugün karşınıza çıkan mesaj kusursuz bir Türkçeyle, doğru kurumsal üslupla ve size ait gerçek bilgilerle yazılabiliyor.

Bunun sonucu olarak mesajın içeriğine bakarak karar verme dönemi kapandı. Artık bakılması gereken şey içerik değil, yoldur: mesaj hangi kanaldan geldi, sizi nereye yönlendiriyor, ödeme hangi sistemden geçiyor, bu adımı siz mi başlattınız yoksa size mi getirildi. İçerik taklit edilebilir, izlenen kurumsal süreç edilemez.

Bu Yaz Güvenli Tatil Dileriz

Çalışanlarınıza yönelik siber güvenlik farkındalık eğitimleri ve kurumsal güvenlik değerlendirmeleri için bizimle iletişime geçebilirsiniz.

Sparta Siber Güvenlik Teknolojileri · 0 312 909 33 02
www.sparta.com.tr · sparta@sparta.com.tr

KAYNAKÇA

Turizm Ekonomi, Alişir Şahin (BODER) açıklaması, 23 Temmuz 2026.

Samsun Ekspres, "Yaz Sezonunda Sahte Rezervasyon Alarmı", 23 Temmuz 2026.

Haber7 Ekonomi, "Tatil Dolandırıcılığı Alarmı, Sahte Rezervasyon Tuzakları Patladı", 22 Temmuz 2026.

Gazetevatan, "Tatil Planı Yapanlar Dikkat, Sahte Rezervasyon Tuzağı", 22 Temmuz 2026.

Star, "Türkiye'de Tatil Tuzağı, Sahte Rezervasyon Vurgunu Büyüyor", 22 Temmuz 2026.

Haberler.com, "Ankara Emniyeti'nden Tatil Dolandırıcılığı Uyarısı", 23 Temmuz 2026.

Sinem Başaran, "Booking.com Üzerinden Dolandırılmak", LinkedIn, 2026.

Secureworks Counter Threat Unit, "Vidar Infostealer Steals Booking.com Credentials in Fraud Scam", Kasım 2023.

Krebs on Security, "Booking.com Phishers May Leave You With Reservations", 1 Kasım 2024.

Microsoft Threat Intelligence, "Phishing Campaign Impersonates Booking.com", 13 Mart 2025.

Action Fraud (UK National Fraud and Cyber Crime Reporting Centre), Booking.com Scam Alert.

Marnie Wilking (Booking.com), Collision Konferansı konuşması, Toronto, Haziran 2024. BBC tarafından haberleştirildi.

Lorenzo Franceschi-Bicchierai, "Booking.com confirms hackers accessed customers' data", TechCrunch, 13 Nisan 2026.

The Guardian, Booking.com veri ihlali haberi, 13 Nisan 2026.

TÜRSAB, Acenta Arama ve Dijital Doğrulama Sistemi.

Yasal Uyarı