Bir QR Kodu Açmadan Önce Güvenli Olup Olmadığını Anlama (Quishing Rehberi)

Quishing, QR kod ile gerçekleştirilen kimlik avı saldırısıdır. Taramadan önce tehlike işaretlerini ve 'Aç'a dokunmadan önce neyi kontrol etmeniz gerektiğini öğrenin.

Yazar: Lubor Šimůnek · Yayınlanma Tarihi: August 23, 2026 · Güvenlik
Çevrimiçi sürüm: https://appstoryo.com/tr/blog/qr-code-safe-quishing-guide



Quishing Nedir?

Quishing, QR kodlar aracılığıyla yapılan kimlik avı (phishing) saldırısıdır. Saldırgan, tarandığında sizi kimlik bilgilerini çalmak, kötü amaçlı yazılım yüklemek veya sahte bir ödeme sayfası göstermek için tasarlanmış kötü niyetli bir siteye yönlendiren bir QR kodu oluşturur. Terim 'QR' ile 'phishing'i birleştirmektedir ve insanlar QR kodlara neredeyse düşünmeden güvendiğinden bu saldırı türü hızla yaygınlaşmaktadır.

QR Kodların Özel Bir Risk Oluşturmasının Nedeni

Normal bir bağlantıda tıklamadan önce üzerine gelip URL'yi görebilirsiniz. QR kodda ise tarayıcı çözümleyene kadar hedefi göremezsiniz — çoğu kamera uygulaması da adresi göstermeden tarayıcıyı anında açar. Bu kısa an, kötü amaçlı bir sitenin cihazınızı izlemeye başlaması için yeterlidir.

QR kodlar spam filtrelerini de tamamen atlatır: filtreler şüpheli metin veya bilinen zararlı URL'leri arar, ancak QR kod görseli tamamen zararsız görünür. Bu yüzden kimlik avı e-postaları özellikle kurumsal saldırılarda eski bağlantılarını QR kodlarla giderek daha fazla değiştirmektedir.

Gerçek dünyada quishing şu şekillerde karşınıza çıkar: park sayaçlarındaki meşru kodların üzerine yapıştırılan etiketler, sahte restoran menüleri, posta kutularına bırakılan sahte kargo bildirimleri ve 'ödeme yapmak için tarayın' diyen sahte kamu şarj istasyonları.

Taramadan ÖNCE Dikkat Edilmesi Gereken Uyarı İşaretleri

- **Orijinal kodun üzerindeki etiket.** Başka bir QR kodun üzerine yapıştırılmış QR etiketi klasik bir değişimdir. Köşeyi hafifçe kaldırın — soyuluyorsa taramayın.
- **Bilinmeyen bir broşürdeki aciliyet dili.** 'Hemen tarayın ve ödülünüzü alın' veya 'Paketiniz beklemede — yeniden planlamak için tarayın' baskı taktikleridir.
- **İstenmeyen e-posta veya mektup.** Bir bankanın, kargo firmasının veya devlet kurumunun QR kodu birincil eylem çağrısı olarak kullandığı beklenmedik iletişim güçlü bir uyarı işaretidir.

Taradıktan SONRA ve Açmadan ÖNCE Kontrol Edilecekler

- **Alan adı beklediğinizle eşleşiyor mu?** Bir bankada QR tarattıysanız URL resmi alan adında olmalıdır.
- **URL kısaltıcı kullanılıyor mu?** bit.ly veya tinyurl.com gibi hizmetler gerçek hedefi gizler. Ziyaret etmeden önce bir URL genişletici hizmeti kullanarak gerçek adresi öğrenin.
- **Yanlış yazılmış veya sahte alan adları.** paypa1.com (L harfi yerine 1 rakamı) veya g00gle.com (O harfi yerine 0 rakamı) gibi adreslere dikkat edin. Her karakteri dikkatlice okuyun.
- **Şüpheli alt alan adları.** login.secure.amazon-kargo-tr.com meşru görünür, ancak gerçek alan adı amazon-kargo-tr.com olup amazon.com değildir.

QR Code Reader Without Ads Nasıl Yardımcı Olur?

QR Code Reader Without Ads herhangi bir şeyi açmadan önce tam URL önizlemesini gösterir ve bağlantıyı incelemeniz için size zaman tanır. Adres şüpheli görünüyorsa 'Aç'a dokunmamanız yeterlidir. Uygulama, cihazınızda yerel bir tarama geçmişi tutar, veri toplamaz ve reklam göstermez. App Store veya Google Play'de 'QR Code Reader Without Ads' aratarak bulabilirsiniz.

QR Code Reader Without Ads uygulamasını iOS veya Android için ücretsiz indirin — reklamsız, izlemesiz ve tamamen çevrimdışı çalışır.

Kaynak gösterimi: Lubor Šimůnek (2026). *Bir QR Kodu Açmadan Önce Güvenli Olup Olmadığını Anlama (Quishing Rehberi)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/tr/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.