Como Saber se um Código QR É Seguro Antes de Abrí-lo (Guia Anti-Quishing)

O quishing é phishing por código QR. Saiba identificar os sinais de alerta antes de escanear e o que verificar antes de tocar em Abrir.

Autor: Lubor Šimůnek · Publicado: August 23, 2026 · Segurança
Versão online: https://appstoryo.com/pt/blog/qr-code-safe-quishing-guide



O que é quishing?

Quishing é phishing realizado por meio de códigos QR. Um atacante exibe um código que, ao ser escaneado, redireciona para uma página falsa criada para roubar credenciais, instalar malware ou simular pagamentos. O nome une 'QR' e 'phishing', e o golpe cresce porque as pessoas costumam confiar em QR codes sem questionar.

Por que códigos QR representam um risco especial

Com um link comum você pode passar o cursor por cima e ver o endereço antes de clicar. Com um QR você não consegue ver o destino até que o scanner decodifique o código — e muitos aplicativos de câmera abrem o navegador imediatamente, sem mostrar a URL. Esse instante é suficiente para que um site malicioso comece a rastrear o seu dispositivo.

Além disso, os QR codes passam despercebidos por filtros de spam: um filtro procura texto suspeito ou URLs conhecidas como maliciosas, mas uma imagem de QR parece totalmente inofensiva. Por isso ataques de phishing corporativo trocam cada vez mais hiperlinks por QR codes.

No mundo real o quishing aparece em adesivos sobre códigos legítimos em parquímetros, cardápios de restaurantes falsificados, avisos de entrega de encomendas deixados na caixa

de correio e instruções em carregadores públicos falsos que pedem para 'escanear para pagar'.

Sinais de alerta ANTES de escanear

- **Adesivo sobre um código original.** Um QR colado sobre outro é uma troca clássica. Puxe a ponta do adesivo — se descolar, não escaneie.
- **Linguagem de urgência em panfleto desconhecido.** 'Escaneie agora para resgatar seu prêmio' ou 'Sua encomenda está retida — escaneie para reagendar' são táticas de pressão.
- **E-mail ou carta não solicitados.** Uma comunicação inesperada de banco, transportadora ou órgão governamental com QR code como principal chamada à ação é um forte sinal de alerta.

O que verificar DEPOIS de escanear e ANTES de abrir

- **O domínio corresponde ao esperado?** Se escaneou um QR em um banco, a URL deve estar no domínio oficial.
- **É um encurtador de URL?** Serviços como bit.ly ou tinyurl.com ocultam o destino real. Use um expansor de URLs para revelar o endereço verdadeiro.
- **Domínios com erros ortográficos.** Atenção a paypa1.com ou g00gle.com — leia cada caractere com cuidado.
- **Subdomínios suspeitos.** login.seguro.amazon-entregas-br.com parece legítimo, mas o domínio real é amazon-entregas-br.com, não amazon.com.

Como o QR Code Reader Without Ads ajuda

QR Code Reader Without Ads exibe a URL completa antes de abrir qualquer link, dando-lhe tempo para analisar o endereço. Se parecer suspeito, basta não tocar em 'Abrir'. O aplicativo mantém um histórico local de escaneamentos no seu dispositivo, não coleta dados e não exibe anúncios. Disponível na App Store e no Google Play buscando 'QR Code Reader Without Ads'.

Baixe o QR Code Reader Without Ads grátis para iOS ou Android — sem anúncios, sem rastreamento e funciona totalmente offline.

Como citar: Lubor Šimůnek (2026). *Como Saber se um Código QR É Seguro Antes de Abrí-lo (Guia Anti-Quishing)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/pt/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.