Comment Savoir si un QR Code Est Sûr Avant de l'Ouvrir (Guide Anti-Quishing)

Le quishing est l'hameçonnage par QR code. Apprenez à repérer les signaux d'alerte avant de scanner et ce qu'il faut vérifier avant de toucher Ouvrir.

Auteur: Lubor Šimůnek · Publié: August 23, 2026 · Sécurité
Version en ligne: https://appstoryo.com/fr/blog/qr-code-safe-quishing-guide



Qu'est-ce que le quishing?

Le quishing est une forme d'hameçonnage (phishing) qui utilise des QR codes. Un attaquant affiche un code qui, une fois scanné, redirige vers un site frauduleux conçu pour voler des identifiants, installer un logiciel malveillant ou simuler une page de paiement. Le terme mêle 'QR' et 'phishing', et cette menace est en pleine expansion car les gens font confiance aux QR codes presque instinctivement.

Pourquoi les QR codes présentent un risque particulier

Avec un lien classique, vous pouvez passer la souris dessus et lire l'URL avant de cliquer. Avec un QR code, vous ne voyez pas la destination tant que votre scanner ne l'a pas décodée — et beaucoup d'applications d'appareil photo ouvrent directement le navigateur sans afficher l'adresse. Cet instant suffit à un site malveillant pour commencer à pister votre appareil.

Les QR codes contournent également les filtres anti-spam : un filtre recherche du texte suspect ou des URL connues comme dangereuses, mais une image de QR code paraît totalement inoffensive. C'est pourquoi les e-mails d'hameçonnage remplacent de plus en plus leurs hyperliens par des QR codes, en particulier dans les attaques visant les entreprises.

Dans la vie réelle, le quishing se manifeste par des autocollants placés sur des codes légitimes (horodateurs, menus de restaurant), des faux avis de livraison dans les boîtes aux lettres, et de fausses bornes de recharge publiques invitant à 'scanner pour payer'.

Signaux d'alerte AVANT de scanner

- **Autocollant posé sur un code original.** Un QR code collé par-dessus un autre est un remplacement classique. Soulevez le coin : s'il se décolle, ne scannez pas.
- **Langage d'urgence sur un prospectus inconnu.** 'Scannez maintenant pour réclamer votre lot' ou 'Votre colis est retenu — scannez pour reprogrammer' sont des tactiques de pression.
- **E-mail ou courrier non sollicité.** Une communication inattendue d'une banque, d'un transporteur ou d'un organisme officiel avec un QR code comme principal appel à l'action est un signal fort.

Ce qu'il faut vérifier APRÈS avoir scanné et AVANT d'ouvrir

- **Le domaine correspond-il à ce que vous attendez?** Si vous avez scanné un QR dans une banque, l'URL doit figurer sur le domaine officiel.
- **Est-ce un raccourcisseur d'URL?** Des services comme bit.ly ou tinyurl.com masquent la vraie destination. Utilisez un service d'expansion d'URL pour révéler l'adresse réelle.
- **Domaines mal orthographiés.** Méfiez-vous de paypa1.com ou g00gle.com — lisez chaque caractère attentivement.
- **Sous-domaines suspects.** login.secure.amazon-livraisons-fr.com semble légitime, mais le vrai domaine est amazon-livraisons-fr.com, pas amazon.com.

Comment QR Code Reader Without Ads aide

QR Code Reader Without Ads affiche l'URL complète avant d'ouvrir quoi que ce soit, vous laissant le temps d'analyser le lien. Si l'adresse semble suspecte, il vous suffit de ne pas appuyer sur 'Ouvrir'. L'application conserve un historique local sur votre appareil, ne collecte aucune donnée et n'affiche pas de publicités. Disponible sur l'App Store et sur Google Play en cherchant 'QR Code Reader Without Ads'.

Téléchargez QR Code Reader Without Ads gratuitement sur iOS ou Android — sans publicité, sans pistage, et l’appli fonctionne entièrement hors ligne.

Citer comme: Lubor Šimůnek (2026). *Comment Savoir si un QR Code Est Sûr Avant de l'Ouvrir (Guide Anti-Quishing)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/fr/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.