



UN SIMPLE MENU DE RESTO PEUT-IL PIRATER VOTRE TÉLÉPHONE ?

« QUISHING », LE PIÈGE DU FAUX QR CODE !

Aujourd'hui, que ce soit au bureau ou dans notre vie quotidienne, nous scannons des **QR codes** partout : menus de restaurant, bornes de recharge, horodateurs ou e-mails professionnels.

Nous sommes donc **tous concernés**, à titre **privé** comme **professionnel**. Les cybercriminels l'ont bien compris et détournent cet usage universel : c'est le **Quishing** (QR Code Phishing).



DÉCRYPTAGE : COMMENT FONCTIONNE L'ARNAQUE ?

- 1. LE PIÈGE PHYSIQUE :** Un escroc colle un banal autocollant imprimé avec son propre QR Code par-dessus un vrai (sur une borne de paiement, un horodateur, une terrasse de café ou une affiche).
- 2. LE PIÈGE NUMÉRIQUE :** Vous recevez un e-mail d'apparence légitime (banque, RH, outil de travail) vous demandant de scanner un QR Code pour valider une connexion MFA ou mettre à jour un dossier.
- 3. LE VOL DE DONNÉES :** Une fois scanné, le code vous redirige vers un faux site qui aspire vos identifiants de connexion, vos données bancaires ou installe un virus sur votre smartphone.



CONSEILS PRÉVENTIFS : LES BONS RÉFLEXES !

- Ouvrez l'œil, passez le doigt :** Dans l'espace public, observez et touchez le QR Code. S'il s'agit d'un sticker collé par-dessus le panneau d'origine, ne le scannez pas.
- Inspectez l'URL :** Avant de cliquer sur le lien généré par l'appareil photo, vérifiez attentivement l'adresse Web (orthographe, domaine officiel).
- Méfiez-vous des e-mails :** Une entreprise ou un service IT demande rarement de scanner un QR Code reçu par e-mail pour accéder à un compte.
- Paielements publics :** Privilégiez les applications officielles ou les terminaux de paiement classiques plutôt que les QR Codes sur la voie publique.



**UN DOUTE ? NE SCANNEZ PAS.
LA PRUDENCE EST VOTRE MEILLEUR BOUCLIER !**

