Association Loisirs et culture

La fraude au QR code : nos conseils pour identifier et éviter les arnaques

Jean Marie Herbaux

Table des matières

La fraude au QR code ou « quishing » est une forme d'arnaque numérique en plein essor qui repose sur l'utilisation de QR codes frauduleux pour tromper les utilisateurs. Comment repérer ce nouveau fléau qui peut mettre en péril la sécurité de vos données personnelles et financières ?

1. Qu'est-ce que le quishing ?

Le quishing, contraction de « QR code » et « phishing », est une technique de fraude numérique. Elle consiste à utiliser des QR codes modifiés ou falsifiés pour rediriger les victimes vers des sites web malveillants.
Ces faux QR codes peuvent être apposés sur des affiches, des flyers, ou même intégrés dans des emails. Une fois scannés, ils conduisent l'utilisateur vers une page demandant des informations personnelles, des identifiants ou des données bancaires, souvent sous des prétextes anodins.

2. Où trouve-t-on ces QR codes frauduleux ?

Face à l'augmentation des arnaques au QR code, il est crucial de comprendre que les faux QR codes peuvent se trouver à n'importe quel endroit, voici quelques emplacements courants :

a. Affiches publicitaires :

dans les lieux publics (pharmacie, supermarché,…) ou les transports en commun, des affiches avec de faux QR codes peuvent être utilisées pour piéger les passants.
Restaurants et cafés : des menus ou des flyers avec des QR codes modifiés sont parfois apposés sur les tables.

b. Emails et réseaux sociaux :

des messages contenant de faux QR codes peuvent sembler provenir d'organisations légitimes, mais conduisent en réalité vers des sites frauduleux.

c. Distributeurs automatiques et terminaux de paiement

des stickers avec des QR codes malveillants peuvent être apposés sur ces machines (borne de recharge pour voiture électrique, par exemple).

d. Fausses amendes de stationnement :

des fausses amendes qui comportent un QR code frauduleux laissées sur le pare-brise des véhicules.

3. Quels sont les risques associés au quishing ?

En scannant un QR code frauduleux, l'utilisateur peut involontairement télécharger des logiciels malveillants (malwares) qui peuvent compromettre la sécurité de son appareil et de ses données personnelles. Cela inclut la perte de données sensibles, qui peuvent être des informations confidentielles personnelles ou professionnelles, exposant ainsi la victime à des risques supplémentaires tels que le chantage ou la violation de la confidentialité professionnelle.
En outre, ces fraudes au QR code conduisent souvent à l'utilisation de ces informations pour effectuer des transactions financières frauduleuses, telles que des prélèvements ou des achats non autorisés, impactant la victime.

4. Les dangers associés au quishing sont multiples et souvent très graves.

Ce type d'arnaque peut conduire au vol d'identité, où les informations personnelles récupérées sont utilisées pour usurper l'identité de la victime. La fraude au QR code peut également entraîner des

complications juridiques et financières considérables pour la personne affectée. Ces risques soulignent l'importance de rester vigilant et informé sur les méthodes employées par les fraudeurs dans le cadre du quishing.
La fraude au QR code est passible de sanctions pénales. Les individus ou groupes impliqués dans la création et la diffusion de QR codes malveillants peuvent faire face à des amendes significatives.

5. Comment éviter le quishing ?

a. Éviter de scanner des QR Codes de source inconnue :

toujours s'assurer de l'origine / la légitimité du support du QR code. Méfiez-vous des QR codes trouvés dans des lieux publics ou sur des supports suspects.

b. Ne jamais fournir d'informations sensibles :

ne pas entrer de données personnelles ou financières après avoir scanné un QR code, à moins d'être absolument sûr de sa sécurité.

c. Mettre à jour régulièrement son smartphone et les logiciels de sécurité :

garder son smartphone et ses applications de sécurité à jour pour se prémunir contre les menaces les plus récentes, ces logiciels vous avertissent en cas de risque. N'hésitez pas à en télécharger un si vous n'en disposez pas.

d. Utiliser un scanner / lecteur de QR Code Sécurisé :

certains smartphones ou applications offrent des fonctions de sécurité supplémentaires qui permettent de prévisualiser l'adresse web intégrée. Vérifiez le lien du site internet qui apparaît avant de cliquer ou de saisir des données.

6. En cas de fraude avérée :

si vous êtes victime de la fraude au QR code et avez saisi des informations personnelles, contactez votre banque immédiatement, faites opposition et portez plainte.