QR CODE : quelle sécurité et quelles précautions à prendre ?

Le faux QR code fait l'objet de sanctions pénales.

Comment se prémunir contre les faux ?

- **Qu'est-ce qu'un QR code ?**

Le QR code (code Quick Response, code à réponse rapide) dit aussi Code QR, c'est ce petit carré déjà vu sur des affiches, sur des prospectus, sur la devanture d'un commerce, dans un restaurant ou encore sur des billets de train ou d'avion.

Ce code-barre en 2 dimensions amélioré à base de petits carrés noirs et blancs est devenu commun dans notre vie quotidienne. Il est notamment aujourd'hui utilisé pour vérifier un pass sanitaire via l'application TousAntiCovid Verif.

Avec un smartphone, il suffit de placer l'objectif de son appareil vers le QR code pour voir s'afficher une URL (adresse Web) qu'on est invité à valider pour voir directement apparaitre une page Web.

C'est un outil pratique qui facilite la vie et évite de taper de longues adresses. Mais c'est aussi une utilisation qui peut constituer une cybermenace avec des attaques ciblées vers les possesseurs de smartphones qui ne font pas attention, dont les professionnels qui l'utilisent pour contrôler les pass sanitaires.

- **Que pensent les internautes et mobinautes des QR code ?**

Les résultats d'une récente enquête de MobileIron, plateforme de sécurité mobile auprès de consommateurs font état de ces constats :

- 74 % des personnes interrogées estiment que les codes QR codes leur facilitent la vie (mais 51 % déclarent ne pas avoir de logiciel de sécurité sur leur smartphone),
- 47 % de ce même panel ont noté une augmentation de l'utilisation des QR codes,
- durant les 6 derniers mois, 38 % des répondants ont scanné un code QR dans un restaurant, un bar ou un café et 37 % pour un commerce de détail,
- 53 % des individus souhaitent que les codes QR soient davantage utilisés dans l'avenir,
- 66 % des répondants disent avoir des problèmes avec les QR codes, dont plus de 51 % qui indiquent en être conscients, mais les utilisent quand même,
- enfin, 51 % des personnes interrogées sont inquiètes quant la confidentialité et la sécurité des données concernant l'utilisation des QR codes.

- **Quelles attaques possibles avec des QR codes ?**

Les QR codes peuvent pointer vers des URL (adresses de sites, de pages, logiciels exécutables) malveillantes pour tenter d'avoir accès à des données d'un smartphone ou d'une tablette.

Il peut aussi d'agir de cyberattaques visant à ouvrir un site de phishing (hameçonnage), technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

Pour les QR codes, on appelle cela le QRishing. Cela peut aussi amener vers une URL courte (raccourcisseur d'URL) qui renvoie ensuite vers l'URL malfaisante.

Bref, les pirates cherchent à récupérer des informations confidentielles des utilisateurs.

Autres agissements malveillants possibles à partir d'un QR code :

- récupérer une liste de contacts de votre appareil afin de leur envoyer des messages par email ou téléphone,
- déclencher des appels téléphoniques vers des numéros surtaxés,
- envoyer des SMS malveillants,
- effectuer des paiements mobiles.

- **Comment se prémunir contre les attaques via QR code et rester vigilant ?**

Voici quelques règles à observer pour se protéger des faux QR codes :

- avant de scanner un QR code, s'assurer qu'il ne couvre pas un autre code,
- en cas de doute sur un QR code, ne pas le scanner,
- vérifier l'URL proposée sur la notification avant de cliquer sur la redirection. Si URL étrange ou très courte, quitter la notification,
- le QR code doit vous amener à une information souhaitée, si ce n'est pas le cas, fermez la page et effacer l'historique de son navigateur,
- si le QR code arrive vers une application de l'AppStore ou de Google Play, s'assurer que l'entreprise mentionnée sur cette page a bien développé l'application demandée,
- ne pas installer d'applications de sécurité à partir d'un lien scanné d'un QR code car c'est souvent un logiciel malveillant (malware) qu'on cherche à installer sur votre smartphone ou tablette,
- être méfiant sur les QR codes distribués sur des cartes, mentionnés sur des affiches lors d'évènements ou placés dans des lieux publics,
- pour les smartphones professionnels, ne pas mettre en place l'installation automatique d'applications,

- utiliser une authentification multifacteurs pour les applications d’entreprise,
- professionnels : il est fortement recommandé d'adopter une solution de défense contre les menaces mobiles.