Le « quishing », la nouvelle forme de menace cyber

De plus en plus répandus, les QR codes sont des images codifiées contenant des informations qui redirigent l'utilisateur vers un site ou une application. Ils sont principalement utilisés pour éviter la saisie manuelle souvent fastidieuse de liens sur les appareils mobiles par exemple. S'ils sont très pratiques, ces outils technologiques sont également devenus un moyen d'action pour les cybercriminels. En effet, Cybermalveillance.gouv.fr a relevé que les QR codes frauduleux (appelés quishing en anglais) se multiplient sous la forme de fausse contravention envoyée au domicile ou sur les pare-brise de véhicules stationnés, de faux avis de passage de La Poste déposés dans les boîtes aux lettres ou encore de faux QR codes collés sur des parcmètres ou sur des bornes de recharge de véhicules électriques.

Apprendre à identifier des liens frauduleux

Le site Cybermalveillance.gouv.fr tient toutefois à rassurer les utilisateurs : l'utilisation des QR codes frauduleux reste encore relativement mineure puisqu'elle requiert une distribution physique (peu de QR codes sont, en effet, envoyés par mail puisqu'ils nécessitent la lecture par un autre appareil), ce qui limite la diffusion en masse. Mais leur développement est réel et il est indispensable pour les

utilisateurs d’apprendre à identifier des liens frauduleux, par exemple lorsqu’ils sont masqués par un QR code qui n’est pas immédiatement lisible. Comme tout lien contenu dans un message, il convient de vérifier d’abord la vraisemblance et de s’abstenir de l’ouvrir au moindre doute.

Pour en savoir plus : www.cybermalveillance.gouv.fr