L’arnaque au QR Code ou Quishing.

Qu’est-ce que le quishing ?

Vous connaissez certainement le phishing ce type d’arnaque reposant sur l’envoi de mails ou SMS frauduleux. Les cybercriminels se font passer pour une grande entreprise dans le but d’escroquer des entreprises en leur soutirant subtilement des données personnelles : mots de passe, informations bancaires, etc. De plus en plus en personnes averties, le public se méfie plutôt bien aujourd’hui des mails et sms.

En effet, la plupart savent qu'il ne faut plus cliquer sur un lien sommaire dans un e-mail et savent aussi comment vérifier si une URL est sûre. Les escrocs ont donc changé leur mode opératoire en utilisant les QR codes. Le QR code (en anglais code Quick Response) permet de rediriger vers un site, comme le fait un lien classique, en le scannant avec une appli dédiée sur son smartphone ou directement depuis l’appareil photo de celui-ci. Il est utilisé presque partout, sur des publications, affiches publicitaires, billets de spectacles ou événements, au restaurant, au supermarché ou encore dans un mail. Cette méthode c’est le quishing voisine au Phishing.

Comment cela fonctionne ?

Pour les pirates, les QR codes présentent l’intérêt d’être plus difficiles à détecter par les filtres anti-spam ou anti-phishing alors ils intègrent désormais des QR codes dans leurs campagnes de phishing par email. Certains vont même plus loin en entreprenant des démarches physiques en se rendant dans des enseignes où sont exposés des QR Code. Puis, ils collent leur propre QR Code frauduleux par-dessus l’original. Ensuite, un passant va le scanner et va être renvoyé vers un site similaire à l’original, sauf que celui-ci essaiera de lui soutirer de l’argent par exemple.

Comment s’en protéger ?

Le quishing peut être difficile à détecter et à ce jour, aucune technologie fiable ne permet de s’en prémunir totalement. La meilleure arme pour se prémunir du quishing, c’est donc la vigilance.

Cependant, il existe tout de même quelques bonnes pratiques à avoir pour réduire les chances de tomber dans le piège :

Vérifiez la source du QRCode !

Évitez de scanner les codes QR d’inconnus, surtout s’ils proposent des offres ou des réductions irrésistibles.

Si le message ou l’e-mail provient d’une source officielle ou d’un collègue, vérifiez auprès d’eux l’authenticité du courrier ou visitez leur site Web officiel.

Tenez-vous au courant !

Veille, sensibilisation, formation : les attaquants sont malins, ils ajustent sans cesse leur techniques d’attaques. Il est important de connaitre les derniers pièges en vogue !