OUCH! Janvier 2024

Votre bulletin mensuel sur la sensibilisation à la sécurité

QR codes

Aperçu

Vous êtes-vous déjà demandé à quoi servent ces carrés de points ou ces barres appelés "codes QR" ? Vous les avez très probablement vus sur des sites web, imprimés sur des affiches, utilisés comme tickets mobiles ou sur des tables de restaurant. Comment fonctionnent-ils et y a-t-il des risques à craindre ? Découvrons tout ça ensemble.

QR code pointant vers le site web de SANS OUCH.

Comment marchent les QR codes ?

Le QR code est l'abréviation de "Quick-Response code" (code de réponse rapide). Il s'agit d'un code lisible par une machine, généralement constitué d'une matrice de carrés noirs et blancs (il peut également exister dans d'autres couleurs et contenir des images d'arrière-plan). Ces carrés peuvent être facilement créés à l'aide de générateurs de QR codes et sont utilisés pour encoder des informations telles que l'URL d'un site web, les coordonnées d'un contact par courrier électronique ou d'autres types de données. Les QR codes sont comparables aux codes-barres, mais ils sont plus polyvalents. La plupart des appareils photo des téléphones portables reconnaissent et décodent les informations codées dans un code QR. En d'autres termes, lorsque vous essayez de prendre une photo d'un QR code avec l'appareil photo de votre appareil, celui-ci décode le QR code et vous demande si vous souhaitez agir sur les informations qu'il contient, comme ouvrir un lien vers un site web.

Quel est le danger ?

Les QR codes peuvent être difficiles à interpréter par les gens, ce qui permet aux cyberattaquants d'encoder plus facilement des informations susceptibles d'être malveillantes ou de causer des dommages. Par exemple, un QR code peut vous envoyer sur un site web malveillant qui tente de récolter vos informations personnelles, comme vos mots de passe ou vos numéros de carte de crédit, ou peut-être même d'installer un logiciel malveillant sur votre appareil. En outre, les QR codes peuvent prendre des mesures supplémentaires, telles que l'ajout d'un contact à votre liste de contacts ou la composition d'un courrier électronique en votre nom. Le QR code en lui-même n'est pas une menace, mais l'information ou l'action qu'il déclenche peut l'être.

Supposons par exemple que vous vous trouviez en ville ou dans un aéroport et qu'une affiche sur un mur fasse la promotion d'un produit qui vous intéresse. L'affiche comporte un QR code que vous pouvez utiliser pour obtenir rapidement plus d'informations. Ce que vous ne réalisez pas, c'est que quelqu'un a recouvert le QR code de l'affiche d'un autocollant représentant un autre QR code. En regardant l'affiche, vous ne vous méfiez pas, sans vous rendre compte que le QR code qui y figure a été remplacé par un criminel. Lorsque vous scannez le QR code pour en savoir plus sur le produit, vous êtes dirigé vers un site web contrôlé par le criminel pour lancer une attaque.

Que puis-je faire pour éviter cela ?

- Soyez prudent avant de faire confiance à un QR code et de le scanner. D'abord, demandez-vous : Est-ce que je peux faire confiance à la source ? Faites-vous confiance à l'affiche, au restaurant ou au site web qui affiche le QR code ? Si quelqu'un laissait sur votre voiture un prospectus comportant un QR code, pourriez-vous lui faire confiance ?
- Une fois que vous avez scanné un QR code, votre appareil vous demande si vous souhaitez agir sur les informations qu'il lit avant de faire quoi que ce soit. Par exemple, si le QR code est un lien vers un site web, votre appareil vous demandera si vous souhaitez visiter le site avant de vous y rendre. Prenez le temps d'examiner l'appel à l'action ou le lien lui-même et assurez-vous que vous vous sentez à l'aise en le consultant.
- Confirmez que vos appareils mobiles sont toujours mis à jour et qu'ils utilisent la dernière version de leur système d'exploitation. Cela permet de s'assurer qu'il dispose des dernières fonctionnalités de sécurité. Le moyen le plus simple est d'activer les mises à jour automatiques sur votre appareil.
- Il n'est pas nécessaire d'installer des applications mobiles spéciales pour décoder les QR codes, vous devriez pouvoir utiliser simplement l'appareil photo intégré de votre appareil. Si un site web vous demande de télécharger une application spécialisée pour scanner les QR, il s'agit très probablement d'un faux.
- Réfléchissez à deux fois avant de fournir des informations confidentielles ou personnelles à un site web auquel vous avez accédé via un QR code visible par le public.

Les QR codes sont un moyen pratique d'accéder à toutes sortes de nouvelles informations et capacités. Quelques mesures simples peuvent vous aider à en tirer le meilleur parti, en toute sécurité.

Rédacteur Invité

Abdulmajeed AlAbdulhadi est consultant en systèmes IT/OT à Saudi Aramco et a plus de 27 ans d'expérience. Il est auditeur certifié des systèmes d'information (CISA) et gestionnaire certifié de la sécurité de l'information (CISM) et a obtenu un brevet de cybersécurité de l'office américain des brevets (10 693 906).

Ressources

Attaques de messagerie / Smishing: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Hameçonnage vocal - Attaques ou arnaques téléphoniques: https://www.sans.org/newsletters/ouch/vishing
Sécuriser vos appareils mobiles : https://www.sans.org/security-awareness-training/ouch-newsletter/2018/securing-your-mobile-devices/

Traduit pour la communauté par : Juliette Busson