Qu'est-ce qu'un code QR ?

Le code QR est un type de code-barres que l'on peut scanner avec n'importe quel Smartphone et qui, grâce à un agencement unique de points pixélisés distribués sur une surface carrée, peut contenir des informations interprétables par Android ou IOS.

Bien que pratiques et conviviaux, les codes QR pollués (utilisés pour des fins malveillantes) sont devenus le fer de lance des pirates pour piéger les utilisateurs.

QR est l'abréviation de Quick Response

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

Quels types d'informations peut-on inclure dans un code QR ?

L'agencement unique de points pixélisés distribués sur la surface carrée du code QR peuvent contenir :

Contenu textuel

Il peut contenir des informations relatives à une personne, une entreprise ou un service.

Liens hypertextes

Ces liens sont souvent utilisés pour envoyer l'utilisateur vers le site web ou les ressrouces de l'entreprise ou le créateur du code QR

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

Comment les pirates exploitent-ils les codes QR ?

1 Le pirate crée une page frauduleuse ou un logiciel malveillant (malware).

Une fois ces ressources mises en ligne, le pirate peut utiliser les outils de raccourcissement des liens URL pour obfusquer (cacher ou dissimuler) les noms complets des liens qui pointent vers sa ressource. 2

3 Le pirate crée le code QR dans lequel il va inclure le lien qui pointe vers la page frauduleuse ou le logiciel malveillant (malware).

Après avoir créé le code QR , le pirate va tenter de le viraliser (diffuser) en le mettant dans des endroits publics (Stations de métro, parcs, grandes surfaces...) afin de piéger le maximum de victimes. 4

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

Quels sont les risques d'une attaque par code QR ?

Le code QR "pollué" peut contenir un lien qui pointe vers une page frauduleuse ou un lien de téléchargement d'un logiciel malveillant qui peut :

Pirater les comptes des réseaux sociaux enregistrés au niveau du smartphone

Envoyer des emails et des SMS aux contacts enregistrés sur le smartphone

Réaliser des achats et des opérations financières en exploitant les paramètres des cartes bancaires enregistrés au niveau du smartphone

Modifier la liste de contacts et réaliser des appels téléphoniques

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

Comment se protéger contre cette technique d'attaque ?

Ne jamais scanner un code QR sans être sûr de la véracité de sa source.

Lorsqu'on scanne un code QR, il faut vérifier que les informations qu'il affiche soient concordantes avec le service ou l'entreprise que l'on souhaite consulter.

Si jamais le code QR scanné pointe vers une application, il faut vérifier la source de cette dernière et consulter l'avis des APP Store (Google store, Microsoft Store...) en vérifiant les informations qui y sont relatives (ratings, vérification de sécurité, source, et développeur).

Installer un antivirus sur vos équipements mobiles (Smartphones et tablettes) afin de minimiser les risques liés aux malwares.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam