Association Loisirs et culture

✓ *Des arnaques du côté des QR codes.*
✓ *Ce qu'il faut faire lorsque l'on identifie une arnaque.*
✓ *Quand on pense être victime d'un acte de cyber malveillance.*

Jean Marie Herbaux

Table des matières

Ils se sont multipliés au point de devenir incontournables avec la pandémie. Les codes sont depuis utilisés pour l'affichage des menus des restaurants jusqu'aux transactions sans contact en passant par des applications de partage de contacts.
Les QR-Codes sont pratiques puisqu'il suffit de dégainer le smartphone et d'utiliser une application spécifique ou bien Google Lens, pour pouvoir accéder au contenu proposé par le QR-Code.
Comme toujours, ce qui marche bien attire les escrocs. Il est maintenant temps de se méfier de ces petits carrés noirs et blancs

L'action déclenchée par la lecture d'un QR code dépend de l'application qui interagit avec ledit code. Les codes peuvent être utilisés pour naviguer vers un site web, télécharger un fichier, ajouter un contact, se connecter à un réseau Wi-Fi et même effectuer des paiements.

1. Comment les QR codes peuvent être exploités ?

Voici comment les cybercriminels peuvent détourner les codes pour voler vos données et votre argent :

1. Lorsque vous pointez sur un QR code

vous pouvez très bien être redirigé vers un site web malveillant afin de vous voler des informations sensibles. C'est exactement le même principe que pour du phishing par e-mail ou pas SMS.

2. Le scannage du QR code peut engendrer le *téléchargement*

d'un fichier malveillant sur votre appareil. Pour cela, les attaquants vont falsifier un QR code pour vous inciter à télécharger un fichier PDF malveillant ou une application mobile malveillante, au lieu d'un menu ou d'une application dédiée à une activité.

3. Les QR codes peuvent *déclencher des actions* directement sur votre appareil

ces actions dépendent de l'application qui les lit. Cependant, il existe certaines actions de base que tout lecteur QR est capable d'interpréter. Il s'agit notamment de la connexion de l'appareil à un réseau Wi-Fi, de l'envoi d'un e-mail ou d'un SMS avec un texte prédéfini, ou de l'enregistrement des informations de contact sur votre appareil. Bien que ces actions ne soient pas malveillantes en soi, elles peuvent être utilisées pour connecter un appareil à un réseau compromis ou envoyer des messages en votre nom.

4. Détourner un paiement :

La plupart des applications financières permettent aujourd'hui d'effectuer des paiements au moyen de codes QR contenant des données appartenant au destinataire de l'argent. Un attaquant pourrait modifier ce QR avec ses propres données et recevoir des paiements sur son compte. Il pourrait également générer des codes avec des demandes de collecte d'argent pour vous tromper.

5. Dans cet exemple

il s'agit d'une discussion sur une transaction via la messagerie du site Leboncoin. La personne cherche à faire payer un bien qui n'existe pas à partir du scan d'un faux code QR qui se fait passer pour celui du site. Seule la méfiance permettra d'éviter l'arnaque.

2. Ce qu'il faut faire lorsque l'on identifie une arnaque

6. Rendez-vous sur un site communautaire de dénonciation contre les escroqueries sur Internet. Je vous conseille par exemple *Signal Arnaque*
   https://www.signal-arnaques.com/scam/add
   Il suffit de saisir des mots clés qui correspondent au nom de la boutique en ligne.

7. Si vous voyez une proposition de ristourne en cas de virement bancaire, n'allez pas plus loin. Et si vous souhaitez en avoir le cœur net, passez la commande sans payer en utilisant de faux noms et coordonnées, ainsi qu'une adresse mail bidon et copiez l'IBAN affiché pour passer commande. Rendez-vous sur le site https://wise.com/fr/iban/checker
et collez l'IBAN dans le champ de vérification d'IBAN et validez. Vous allez pouvoir voir la banque concernée. S'il s'agit d'une banque comme PFS CARD SERVICES IRELAND LIMITED, c'est clairement une arnaque.
8. Prenez le temps de signaler sur le site *Signal Arnaque* https://www.signal-arnaques.com/scam/add
pour que la communauté soit au courant. Vous permettrez aux autres d'éviter les arnaques.
Faites un signalement sur Pharos *https://www.internet-signalement.gouv.fr/PharosS1/*
le portail officiel de signalement des contenus illicites du gouvernement. La procédure est assez rapide et concerne aussi bien les spams, les escroqueries, que l'incitation à la haine, les trafics, la pédophilie ou les mises en danger des personnes.

3. Que faire si vous pensez être victime d'un acte de cyber malveillance ?

Il y a les arnaques et il y a aussi les cyberattaques. Pour ces deux délits, le gouvernement a mis au point un outil de diagnostic appelé cyber malveillance. On le trouve à l'adresse https://www.cybermalveillance.gouv.fr/diagnostic/accueil
Ce service est gratuit et délivré exclusivement en ligne. Il permet d'identifier votre problème et vous propose des conseils personnalisés pour pouvoir y faire face. Il suffit de répondre à plusieurs questions qui décrivent votre problème. Vos réponses permettront à l'outil de vous proposer un diagnostic personnalisé. Notez qu'aucune information à caractère personnel ne vous sera demandée pour obtenir votre diagnostic.
Des conseils y sont également délivrés pour résoudre votre problème. Le site oriente vers les différents services compétents en fonction de la situation. Il est aussi possible d'être mis en relation avec des prestataires spécialisés de proximité référencés par le site et susceptibles de pouvoir vous aider dans la résolution de votre problème. Par contre, il faut bien avoir conscience que ces prestations annexes pourront vous être facturées par la société qui vous prendra en charge.

4. Comment déposer plainte après une arnaque en ligne

Les pratiques commerciales abusives, mensongères ou trompeuses, visant particuliers et entreprises, vont monter en puissance en 2023. De nombreux sites internet très bien conçus sont créés chaque jour avec pour unique objectif d'escroquer le visiteur.
Et cela fonctionne plutôt bien, puisque d'après une note de l'Observatoire national de la délinquance et des réponses pénales (ONDRP) publiée en 2020, plus de la moitié des victimes d'escroqueries en France se font piéger en ligne. Ce chiffre, non encore mis à jour, a dû exploser depuis avec les confinements. Alors comment réagir face aux arnaques ?

Nouveau la plainte en ligne pour les cyber escroqueries Cela n'était pas possible avant, mais depuis peu pour les arnaques en ligne, il est possible de porter plainte via le site internet https://www.service-public.fr/
Le site couvre l'essentiel des scénarios :

- escroquerie,

- chantage via Internet
- Messagerie électronique piratée
- Phishing,

Le formulaire de choix est guidé. Il convient d'abord de créer un compte ou d'utiliser le service France Connect qui permet de vous identifier facilement via votre numéro de sécurité sociale, ou bien vos identifiants pour vous connecter au services des impôts en ligne. Le reste est très simple. Si vous avez réalisé des captures d'écran, ce que je conseille de faire, même chez un commerçant ayant pignon sur rue, vous pouvez les ajouter à la plainte. Toute information, comme par exemple un RIB, un numéro de téléphone, surtout un mobile est intéressant à indiquer. À l'issue de la plainte, vous pouvez signer votre déclaration à l'aide du pointeur de la souris. Vous recevrez ensuite par e-mail, une confirmation de votre plainte, ainsi que sa référence. À tout moment, vous pouvez la modifier ou la compléter, c'est très rapide à faire.
Une réponse sur les suites données à votre démarche devrait vous parvenir dans les huit jours par e-mail. Bien entendu, la procédure classique du dépôt de plainte en commissariat ou gendarmerie reste possible.