Facteurs relatifs à la sécurité à considérer pour les codes QR

Janvier 2024

ITSAP.00.141

Les codes à réponse rapide (QR pour *Quick response*) sont de petits carrés blancs avec des marques noires bidimensionnelles (2D) semblables à celles d'un code-barres. Les codes QR contiennent des renseignements déchiffrables par la lentille de la caméra de certains dispositifs électroniques. On les utilise de différentes façons comme, entre autres, scanner un code pour consulter un menu dans un restaurant ou accéder à un site Web afin d'obtenir de l'information supplémentaire.

On compte trois principaux types d'activités liées aux codes QR :

1. Consommation : Les utilisateurs peuvent scanner un code QR pour accéder à du contenu, comme le menu d'un restaurant ou d'autres documents. Il s'agit de l'activité la plus répandue.
2. Communication : Les utilisatrices et utilisateurs présentent leur code QR afin de valider leurs renseignements, comme une carte d'embarquement ou des billets de loterie. Il s'agit d'un usage de plus en plus courant.
3. Génération : Sans être aussi courante, elle peut se produire si une application nécessite un code pour effectuer une action, comme le jumelage d'une montre intelligente à un téléphone intelligent.

Actions des codes QR

Une fois numérisé, le texte décodé du code QR peut déclencher les actions suivantes:

- ouverture d'un site Web
- téléchargement d'une application
- connexion à un réseau wifi
- vérification d'informations
- création d'un contact
- envoi d'un courriel ou d'un message
- composition d'un numéro de téléphone

Les codes QR posent-ils des risques?

Les codes QR peuvent contenir des renseignements personnels. Ils peuvent également exécuter une action, comme l'ouverture d'un document PDF à remplir ou d'un formulaire en ligne qui vous invite à saisir des renseignements personnels. Lorsque ces renseignements ont été saisis, il suffit de scanner le code QR pour afficher les renseignements enregistrés dans votre dispositif électronique. De plus, certains formulaires en ligne créent un code QR une fois remplis.

Scanner un code QR peut vous faire courir les risques suivants :

- les sites Web faisant appel à des témoins de connexion peuvent faire le suivi de vos activités en ligne, ce qui pourrait donner lieu à la collecte et à l'utilisation de vos données à des fins de marketing sans votre consentement;
- la collecte de métadonnées qui vous sont associées, comme le type d'appareil que vous avez utilisé pour scanner le code QR, votre adresse IP, votre emplacement et les renseignements que vous saisissez lorsque vous vous trouvez sur le site Web;
- l'exposition de vos données financières, comme votre numéro de carte de crédit, si vous l'utilisez pour vous procurer des produits ou services sur le site Web.

Les actions effectuées par le code QR peuvent également présenter des risques en permettant, entre autres, aux auteures et auteurs de menace de tirer avantage du code QR pour infecter des appareils avec des maliciels, voler des renseignements personnels ou effectuer des fraudes par hameçonnage.

Les codes QR comme vecteurs d'attaque

- **Clonage:** Les auteurs de auteurs de menaces peuvent cloner un code QR de manière à ce qu'il redirige l'utilisatrice ou utilisateur vers un site malveillant ou infecte son dispositif avec un maliciel en vue d'en extraire les données personnelles.
- **Exploration:** Les auteurs et auteurs de menace utilisent les codes QR à des fins d'hameçonnage et d'attaques par maliciel. Des codes QR malveillants peuvent diriger les utilisatrices et utilisateurs vers des sites Web en apparence légitimes qui sont conçus pour voler les justificatifs d'identité, les données de cartes de crédit ou les identifiants de connexion d'entreprise, ou vers des sites Web à partir desquels des maliciels sont téléchargés automatiquement.
- **Publicités:** Les auteurs et auteurs de menace placent des codes QR dans des endroits publics dans l'espoir que les passants les scannent.
- **Hameçonnage par code QR (Quishing):** Les auteurs et auteurs de menaces peuvent placer un code QR dans un courriel d'hameçonnage, ou utiliser un tel code pour diriger les utilisateurs et utilisateurs vers un site Web d'hameçonnage qui les incite à dévoiler leurs renseignements personnels.
- **Applications de numérisation:** Les auteurs et auteurs de menaces peuvent avoir recours à des applications de numérisation par balayage de tierces parties pour diffuser des maliciels et accéder à certains paramètres de confidentialité des appareils mobiles des utilisateurs, comme l'affichage des connexions réseau ou la modification du contenu de stockage USB. Vous devriez utiliser la caméra intégrée à votre appareil ou une application de lecture de code sécurisée pour scanner les codes QR.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-141-2023F-PDF
ISBN 978-0-660-68426-0

Réduction des risques associés à l'utilisation des codes QR

Comment protéger vos renseignements :

- Utilisez le mode de navigation privée sur vos appareils et considérez l'utilisation d'un navigateur avec des fonctionnalités anti-pistage.
- Faites preuve de vigilance et vérifiez attentivement l'adresse URL du site Web si l'on vous demande un mot de passe ou des justificatifs d'identité après avoir scanné un code QR.
- Vérifiez les paramètres du navigateur pour désactiver les témoins de connexion et le stockage des données du site.
- Fournissez le minimum de renseignements personnels demandés lorsque vous remplissez des formulaires en ligne.
- Renseignez-vous sur la politique de confidentialité de l'entreprise si vous scannez son code QR pour vous connecter ou accéder à un service.
- Signalez les fraudes et incidents de cybersécurité à votre service de police local, au centre antifraude du Canada, ou au Centre canadien pour la cybersécurité.

Comment protéger vos appareils :

- Configurez votre appareil de manière à exiger une autorisation et une vérification avant de lancer l'action du code QR. .
- Fermez votre navigateur Web si le code QR que vous avez scanné a ouvert un site suspect.
- Activez les mises à jour automatiques sur vos appareils.

Comment protéger vos codes QR personnalisés :

- Conservez vos codes QR personnalisés , comme une carte d'embarquement, dans un dossier sécurisé.
- Veillez à ce que votre code QR soit scanné uniquement par une application sécurisée et vérifiée comme l'application d'une compagnie aérienne ou d'un aéroport.

Actions à éviter

- Autoriser vos appareils à exécuter automatiquement les actions des codes QR.
- Scanner un code QR publié dans un lieu public, comme une station d'autobus ou des publicités affichées dans la rue.
- Scanner un code QR se trouvant sur une étiquette qui pourrait recouvrir un autre code QR. Avant de procéder, demandez à une ou un membre du personnel de confirmer la légitimité du code QR. Il est possible que l'entreprise ait simplement mis à jour son code QR.
- Scanner des codes QR reçus par courriel ou message texte à moins de savoir qu'ils proviennent d'une source légitime.
- Utiliser des applications de numérisation par balayage de codes QR provenant d'entreprises ou d'institutions méconnues.
- Faire passer la commodité avant la sécurité. Saisissez l'adresse URL d'un site Web pour afficher le contenu (par exemple, un menu de restaurant en ligne) au lieu de scanner un code QR.

Les codes QR en action

En 2020, le gouvernement du Canada a soutenu les provinces dans la mise en œuvre des codes QR comme certificat officiel des vaccins contre la COVID-19. Même si les passeports vaccinaux ne sont plus exigés dans la plupart des établissements, les codes QR ont toujours la cote. On les utilise souvent pour le paiement sans contact, sur les aliments emballés, sur les cartes professionnelles et pour se connecter à des réseaux Wi-Fi. N'oubliez pas qu'il est important de procéder à une vérification avant de scanner un code QR.

Les demandes de passeport utilisent également les codes QR. Au moment de soumettre votre demande de passeport, vous devez remplir un formulaire, que ce soit sous forme électronique ou par écrit. Remplir électroniquement le PDF générera un code QR unique à votre demande. Faites preuve de vigilance lorsque vous choisissez cette méthode. Bien qu'elle facilite la saisie des données, elle permet également à la personne qui scanne votre demande d'accéder à votre information. Affaires mondiales Canada recommande de vider le cache du navigateur et du visualiseur d'Adobe Acrobat sur votre ordinateur après avoir imprimé le formulaire de votre demande pour atténuer les risques. Cliquez ici pour en apprendre plus sur le code-barres bidimensionnel (code-barres 2D) utilisé sur les formulaires de demande de passeport.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.