CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

FACTEURS RELATIFS À LA SÉCURITÉ À CONSIDÉRER POUR LES CODES QR

JANVIER 2022

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 sont de plus en plus utilisés depuis le début de la pandémie de COVID-19, notamment parce qu'ils rendent possibles des transactions sans contact, par exemple les restaurants remplacent leurs menus en papier par un code QR qui, une fois scanné, mène à une version électronique du menu. On utilise aussi les codes QR dans le cadre du dépistage de la COVID-19 et de la recherche des contacts. Les codes QR sont désormais utilisés pour prouver que l'on est vacciné, ce qui accroît le potentiel de vulnérabilités exploitables par les auteurs de menaces qui veulent accéder à vos renseignements personnels.

COMMENT FONCTIONNENT LES CODES QR?

Les codes QR contiennent des renseignements déchiffrables par la lentille de la caméra de certains dispositifs électroniques. On compte trois principaux types d'activités liées aux codes QR:

1. La consommation est l'activité la plus répandue. Les utilisateurs peuvent scanner un code QR pour accéder à du contenu, p. ex. le menu d'un restaurant ou autres documents.
2. Le partage de renseignements est aussi un usage de plus en plus commun. Les utilisateurs présentent leur code QR pour que l'on confirme leurs renseignements (p. ex. carte d'embarquement, billet de loterie, preuve de vaccination).
3. La génération n'est pas aussi courante, mais peut se produire si une application nécessite un code pour effectuer une action, comme l'association d'une montre intelligente à un téléphone intelligent.

Actions des codes QR

Une fois scanné, 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 comporter 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 consignés 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:

- Suivi de vos activités en ligne par des sites Web utilisant des témoins de connexion. Vos données pourraient être recueillies et utilisées à des fins de marketing sans votre consentement.
- Collecte des 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 informations que vous saisissez lorsque vous êtes sur le site Web.
- Divulgation 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, p. ex. en permettant aux auteurs de menaces d'exploiter des codes QR en vue d'infecter des appareils avec des maliciels, de voler des renseignements personnels ou d'effectuer des fraudes par hameçonnage.

Les codes QR comme vecteurs

- **Clonage:** Les auteurs de menaces peuvent cloner un code QR qui redirige l'utilisateur vers un site malveillant ou qui infecte son dispositif électronique à l'aide d'un maliciel en vue d'en extraire les données personnelles.
- **Exploitation:** Les auteurs de menaces utilisent les codes QR à des fins d'hameçonnage et d'attaques par maliciel. Des codes QR malveillants peuvent diriger les utilisateurs vers des sites Web qui ont l'air légitimes, mais 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 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 de menaces peuvent placer un code QR dans un courriel d'hameçonnage, ou utiliser un code QR pour diriger les utilisateurs vers un site Web d'hameçonnage qui incite ces derniers à dévoiler leurs renseignements personnels.
- **Applications de numérisation par balayage:** Les 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. Utilisez la caméra intégrée à votre appareil ou une application de lecture de code sécurisée pour scanner les codes QR.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-141-2022F-PDF
ISBN 978-0-660-41544-4

ASSUREZ VOTRE PROTECTION

RENSEIGNEMENTS PERSONNELS

- Utilisez le mode de navigation privée sur vos appareils et considérez l'utilisation d'un navigateur avec des fonctionnalités anti-pistage.
- Méfiez-vous 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.

APPAREILS ÉLECTRONIQUES

- Configurez votre appareil pour 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.

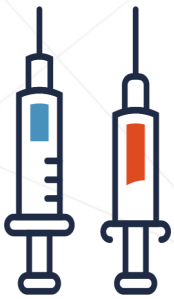
CODES QR PERSONNALISÉS

- Conservez vos codes QR personnalisés (p. ex. preuve de vaccination, carte d'embarquement) dans un dossier sécurisé.
- Veillez à ce que votre code QR soit scanné uniquement par une application sécurisée et vérifiée (p. ex. application provinciale de vérification des preuves de vaccination).

À ÉVITER

- Empêchez vos appareils d'exécuter automatiquement les actions des codes QR.
- Évitez de scanner un code QR publié dans un lieu public (p. ex. station d'autobus, publicités affichées dans la rue).
- Ne scannez pas de code QR se trouvant sur une étiquette qui pourrait recouvrir un autre code QR. Demandez à un membre du personnel de préalablement confirmer la légitimité du code QR. Il est possible que l'entreprise ait simplement mis à jour son code QR.
- Ne scannez pas de codes QR reçus par courriel ou message texte à moins de savoir qu'ils proviennent d'une source légitime.
- N'utilisez jamais d'applications de numérisation de codes QR provenant d'entreprises ou d'institutions méconnues.
- Ne faites jamais prévaloir la commodité au profit de la sécurité. Saisissez l'URL d'un site Web pour afficher le contenu (p. ex. un menu de restaurant en ligne) au lieu de scanner un code QR.

PREUVE DE VACCINATION



Le gouvernement du Canada a aidé les provinces et les territoires à mettre en œuvre une preuve de vaccination standardisée à l'aide de codes QR. La preuve de vaccination peut être utilisée au niveau national pour accéder à des établissements comme les restaurants, sites sportifs et cinémas. Elle sert aussi dans le cadre des voyages à l'étranger.

La preuve de vaccination comprend un code QR SMART Health Card qui contient des informations personnelles, notamment votre nom, votre date de naissance et vos antécédents de vaccination contre la COVID-19 (date de vaccination, nom du vaccin et nombre de doses reçues). Votre nom et votre date de naissance figurant sur la preuve de vaccination sont associés à une pièce d'identité avec photo émise par le gouvernement. Le code QR permet un traitement rapide ainsi que la validation d'une signature numérique pour détecter les contrefaçons.

En suivant les conseils énumérés ci-dessus pour sécuriser vos appareils, protéger vos informations et adopter de bonnes pratiques de cybersécurité lors de la numérisation ou de la création de codes QR, vous protégerez les informations sensibles contenues dans vos carnets de vaccination et autres codes QR personnalisés.

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**.