Le QR code : usages, bons réflexes et arnaques

...Ou comment scanner en confiance et repérer les faux QR codes.

Guide d'après le support « QR code : usages et arnaques » de l'atelier Part'âges numériques.

- Où croise-t-on des QR codes ?
- Du scan à l'action
- Les bons réflexes
- Le « quishing » : l'hameçonnage par QR code
- Les signaux d'alerte
- Pour s'entraîner

Où croise-t-on des QR codes ?

Restaurants Menus, commande et paiement à table.	**Paiement** Chez un commerçant ou entre particuliers.	**Wi-Fi** Connexion sans taper le mot de passe.
Billetterie Train, avion, concert, musée.	**Produits** Fiches, avis, notices.	**Publicité** Affiches et flyers renvoyant vers un site.

Du scan à l'action

1. Capture	2. Décodage	3. Aperçu	4. Action
L'appareil photo détecte le motif.	Le téléphone le traduit en lien ou texte.	Le lien s'affiche à l'écran.	Vous choisissez d'ouvrir ou non.

Le risque : vouloir ouvrir sans avoir lu le lien.

> Le téléphone peut proposer d'ouvrir le lien avant que vous ayez vraiment vérifié où il mène : c'est là que se loge le risque.

Les bons réflexes

1. **Lisez l'aperçu du lien** avant de l'ouvrir : le nom de domaine correspond-il à l'enseigne ? Prenez 2 secondes.
2. Utilisez l'**appareil photo natif** du téléphone plutôt qu'un scanner peu connu.
3. Avant de payer, vérifiez le **cadenas** et le **nom du site**.
4. Gardez le téléphone et ses applications **à jour**.

Le « quishing » : l'hameçonnage par QR code

Le **quishing** (QR code + phishing) consiste à remplacer ou à coller un faux QR code pour piéger la victime : faux site de paiement, fausse page de connexion, application malveillante.

- Un **autocollant** collé sur un vrai QR code (borne de parking, menu de restaurant).
- Un QR code reçu par **mail ou SMS** d'un faux livreur ou d'une fausse administration.
- Un **flyer** annonçant un cadeau ou une réduction trop belle.

Les signaux d'alerte

Signaux d'alerte	Réflexes rassurants
QR code isolé, collé ou imprimé sans lien avec son support	QR code intégré à un support officiel (ticket, emballage, site vérifié)
Urgence : « offre limitée », « compte bloqué »	Aucune urgence : vous prenez le temps de vérifier
Lien différent du site officiel (fautes, nom étrange)	Nom de domaine cohérent avec l'enseigne
Demande de mot de passe ou de coordonnées bancaires	Aucune demande de données sensibles
QR code reçu d'un inconnu par SMS ou mail	Expéditeur connu et message attendu

Pour s'entraîner, à son rythme

1. Scannez un QR code sans l'ouvrir : lisez l'aperçu du lien.
2. Repérez un QR code dans la rue : est-il collé sur un autre ?
3. Retrouvez les quatre étapes d'un scan.

À retenir

- Lisez le lien avant d'ouvrir.
- Appareil photo natif, téléphone à jour.
- Méfiance envers un QR code collé, reçu ou pressant.
- Jamais de mot de passe ni de carte sur un lien douteux.

Petit lexique

Quishing	Hameçonnage par faux QR code.
Aperçu du lien	Adresse affichée avant l'ouverture.
Domaine	Le nom du site dans l'adresse.

Sources : support de cours de l'atelier Part'âges numériques (Niveau 1, « Les smartphones »).