AIRNITE

ZERO DAY

NUMÉRO 14/2026 · SÉCURITÉ INFORMATIQUE

Quishing : quand le QR code de l'horodateur ment

QR codes recouverts sur les horodateurs et les bornes de recharge, faux courriers bancaires avec QR code : les escrocs déplacent le phishing dans le monde réel. Comment fonctionne le quishing et comment entreprises et salariés se protègent.

Publié le: 21 novembre 2026 Temps de lecture: 5 min Auteur: Rédaction Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUATION EN CHIFFRES

août 2024
premiers courriers de quishing signalés
prétendu courrier de la Commerzbank (centre allemand de protection des consommateurs)

< 20
horodateurs piégés à Hanovre
alerte de la police de Basse-Saxe du 14/11/2024

easypark.live
fausse page d'application de stationnement
demandait les données de carte (police de Basse-Saxe)

2026
nouveaux courriers bancaires avec QR code
aussi au nom d'autres banques (Verbraucherzentrale)

Les QR codes sont pratiques : on scanne, on paie, c'est fait. C'est précisément ce qu'exploitent les escrocs. Au lieu d'un faux e-mail, ils collent un faux code sur un horodateur ou envoient un courrier bancaire d'apparence authentique. L'arnaque a un nom : le **quishing**, contraction de QR code et de phishing.

// Que s'est-il passé ?

En novembre 2024, la police de Basse-Saxe, en Allemagne, a lancé une alerte : à **Hanovre**, des inconnus avaient collé des autocollants soignés sur les vrais QR codes de plusieurs horodateurs – moins de 20. Ils menaient à une fausse page imitant l'application de stationnement easypark, qui demandait les **données de carte bancaire**.

Les centres allemands de protection des consommateurs recensent d'autres variantes. Les premières tentatives avec des QR codes dans des **courriers** leur ont été signalées fin août 2024 – un prétendu courrier de la Commerzbank adressé à une femme qui n'y avait même pas de compte. En septembre 2025 a suivi un autre faux courrier de la Commerzbank exigeant une « mise à jour de la banque en ligne », et en 2026 des courriers similaires sont arrivés au nom d'autres banques. S'y ajoutent des codes recouverts sur des **bornes de recharge**, de fausses affiches dans les **transports en commun** et de faux **avis de contravention** avec QR code.

// Comment fonctionne l'attaque ?

Le QR code cache l'adresse vers laquelle il mène. Qui le scanne ne voit souvent qu'une page ressemblant à celle du service de stationnement, de la banque ou de l'opérateur de transport. Il doit y saisir données de carte, accès bancaires ou informations personnelles. Comme le code est collé sur un vrai appareil ou figure dans un courrier crédible, la méfiance baisse.

La police cite des signes d'alerte sur la fausse page de stationnement : absence de trémas allemands (« ae » au lieu de « ä ») et durées de stationnement plus longues que ne le permet la zone. Ces détails passent facilement inaperçus au quotidien – surtout sur un petit écran de smartphone et dans la précipitation.

// Qui est concerné ?

Les consommateurs qui se garent, rechargent leur véhicule ou ouvrent le courrier de leur banque sont les premiers concernés. Pour les entreprises, le sujet compte doublement : leurs **salariés** scannent des QR codes au travail comme en privé et peuvent ainsi divulguer des identifiants. Et les entreprises qui utilisent elles-mêmes des QR codes – sur des appareils, bornes, factures ou affichages – peuvent devenir l'outil des escrocs si leurs codes sont recouverts.

// Que faire maintenant ?

Les recommandations des associations de consommateurs et de la police sont simples : ne scanner que des codes d'origine sûre, vérifier l'adresse de destination avant d'ouvrir, contacter l'expéditeur d'un courrier via un numéro trouvé soi-même et n'utiliser aux bornes que le code affiché à l'écran. Qui a déjà saisi ses données de carte doit faire opposition immédiatement et porter plainte. La check-list ci-dessous résume les étapes.

// Comment Airnite vous aide-t-il ?

En **formation**, Airnite apprend à vos équipes à reconnaître le phishing sous toutes ses formes – de l'e-mail au QR code en passant par l'appel téléphonique. En **conseil**, nous vérifions avec vous où votre entreprise utilise elle-même des QR codes et comment prévenir les manipulations. Avec des **tests d'intrusion** et des simulations de phishing, nous mesurons l'efficacité de la défense au quotidien.

> Remarque : les cas proviennent d'alertes de centres de consommateurs et de la police en Allemagne ; tous ne sont pas datés précisément. État de la recherche : 21 novembre 2026.

Check-list : ce qu'il faut faire maintenant

[+] Ne scanner un QR code que si son origine et son emplacement sont fiables ; repérer les autocollants posés sur le code d'origine.

[+] Utiliser un lecteur qui affiche l'adresse de destination avant ouverture et la vérifier attentivement.

[+] Pour un courrier avec QR code, contacter l'expéditeur via un numéro trouvé soi-même, jamais via les indications du courrier.

[+] Aux bornes de recharge, n'utiliser que le code affiché à l'écran ou l'application de l'opérateur.

[+] Après saisie de données de carte sur une page suspecte, faire opposition immédiatement et porter plainte.

[+] Contrôler régulièrement que les QR codes de l'entreprise sur affichages et appareils n'ont pas été recouverts.

Comment Airnite vous aide

- Formations – Votre équipe apprend nos outils et méthodes.
- Conseil – Un regard extérieur sur vos projets.
- Tests d'intrusion et sécurité – Attaques contrôlées avec rapport clair et plan d'action.

Vos équipes repéreraient-elles le faux code ?

Airnite forme vos équipes de manière concrète au phishing sous toutes ses formes – e-mail, téléphone, voix générée par IA et QR code – et vérifie, sur demande, la protection contre la falsification de vos propres QR codes sur emballages, factures ou affichages.

Demander un premier échange · Écrire un e-mail · Par WhatsApp

Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/quishing-faux-qr-codes/

Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.

1. **Verbraucherzentrale · „Quishing“: Falsche QR-Codes in Mails, Briefen, ÖPNV und Straßenverkehr** · état au 23/10/2025 · SOURCE PRIMAIRE
   Protection des consommateurs : cas de courriers bancaires, bornes de recharge, transports, contraventions, recommandations
   https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/quishing-falsche-qrcodes-in-mails-briefen-oepnv-und-strassenverkehr-98612

2. **Police de Basse-Saxe (polizei-praevention.de) · Gefälschter QR Code auf Parkscheinautomat führt zu Phishingseite im Aussehen von easypark** · 14/11/2024, mise à jour 21/11/2024 · SOURCE PRIMAIRE
   Police : horodateurs piégés à Hanovre, fausse page, signes d’alerte
   https://www.polizei-praevention.de/aktuelles/gefaelschter-qr-code-auf-parkscheinautomat-fuehrt-zu-phishingseite-im-aussehen-von-easypark.html

Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de