ivanti

QRurb Your Enthusiasm 2021:

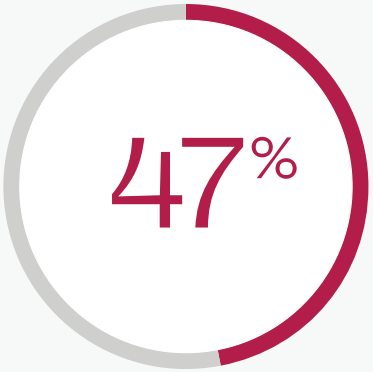
Pourquoi le QR code reste l'une des principales menaces de sécurité et comment réagir

Les QR codes : Comment ça a commencé et où va-t-on?

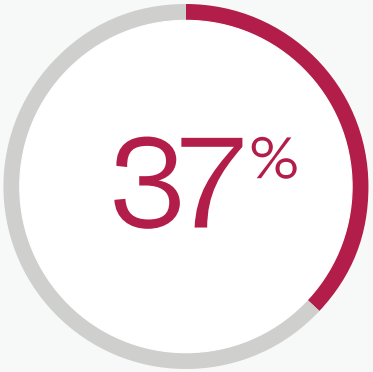
En 2020, nous avons publié des documents sur l'augmentation croissante (et les risques potentiels) des QR codes (Quick Response codes). Bien que les QR codes soient utilisés depuis des dizaines d'années, leur utilisation a explosé avec la pandémie de COVID-19, car les transactions sans contact sont devenues la norme dans le monde entier. Les consommateurs utilisent de plus en plus souvent les QR codes pour accéder à des sites Web, soumettre des commandes et réaliser des paiements, tandis que les autorités gouvernementales les utilisent pour faciliter le suivi des contacts et le traitement des visiteurs aux frontières. Les QR codes ont rendu possibles tous ces échanges sans argent liquide et sans papier au moment où le monde en avait le plus besoin.

Avance rapide jusqu'à 2021... Est-ce que quelque chose a changé, et quoi ?

Nous savons que les QR codes sont plus répandus que jamais. Pensez-y : les réseaux sociaux comme Facebook, Snapchat, Twitter, LinkedIn et Instagram permettent désormais à leurs utilisateurs de suivre instantanément un compte, simplement en scannant un QR code. En outre, l'on retrouve les QR codes presque partout en Chine, et leur adoption est également rapide en Corée du Sud et en Inde. Des solutions de paiement par QR code devraient aussi être déployées très bientôt au Ghana, en Russie et au Sri Lanka, et d'autres pays prévoient de mettre en place cette technologie dans l'année à venir.



des personnes interrogées savent qu'un QR code peut ouvrir une URL, contre 61% en septembre 2020.



des personnes interrogées savent qu'un QR code peut télécharger une application, soit moins que les 49% révélés par l'enquête précédente.

Quelles sont les prévisions en matière de sécurité des QR codes pour 2021 ?

Pour être honnête, d'après notre enquête, ce n'est pas fameux. Comme nous l'avons mentionné dans notre rapport de 2020, le danger ne réside pas dans le QR code proprement dit mais dans le manque d'information des consommateurs sur les opérations qu'un QR code peut réaliser à l'insu de l'utilisateur. Les habitudes risquées des consommateurs, associées à un manque fréquent de sécurité Zero Trust sur les périphériques mobiles, n'ont rien fait pour améliorer le paysage des menaces mobiles ces derniers mois.

En fait, notre enquête 2021 a révélé les tendances générales suivantes :

- L'utilisation des QR codes explose mais la connaissance de leurs capacités n'est pas du tout à la hauteur.
- Les scénarios d'utilisation des QR codes se sont multipliés et s'étendent désormais à la sphère privée, comme les transactions financières et l'accès aux organismes de santé.
- Ces deux tendances (augmentation de l'utilisation des QR codes et manque d'information des utilisateurs) représentent potentiellement un danger supplémentaire de fuites de données, à la fois pour les consommateurs et les entreprises.

Il est évident que les QR codes sont là pour longtemps, alors comment les professionnels de la sécurité IT peuvent-ils protéger leur entreprise de ces vulnérabilités ? Dans la suite de ce rapport, nous examinons plus en détail les tendances mondiales en matière de QR code et nous fournissons des informations pouvant servir aux entreprises à fortifier leurs stratégies de sécurité pour l'avenir.

Le monde est-il toujours attiré par les QR codes ?

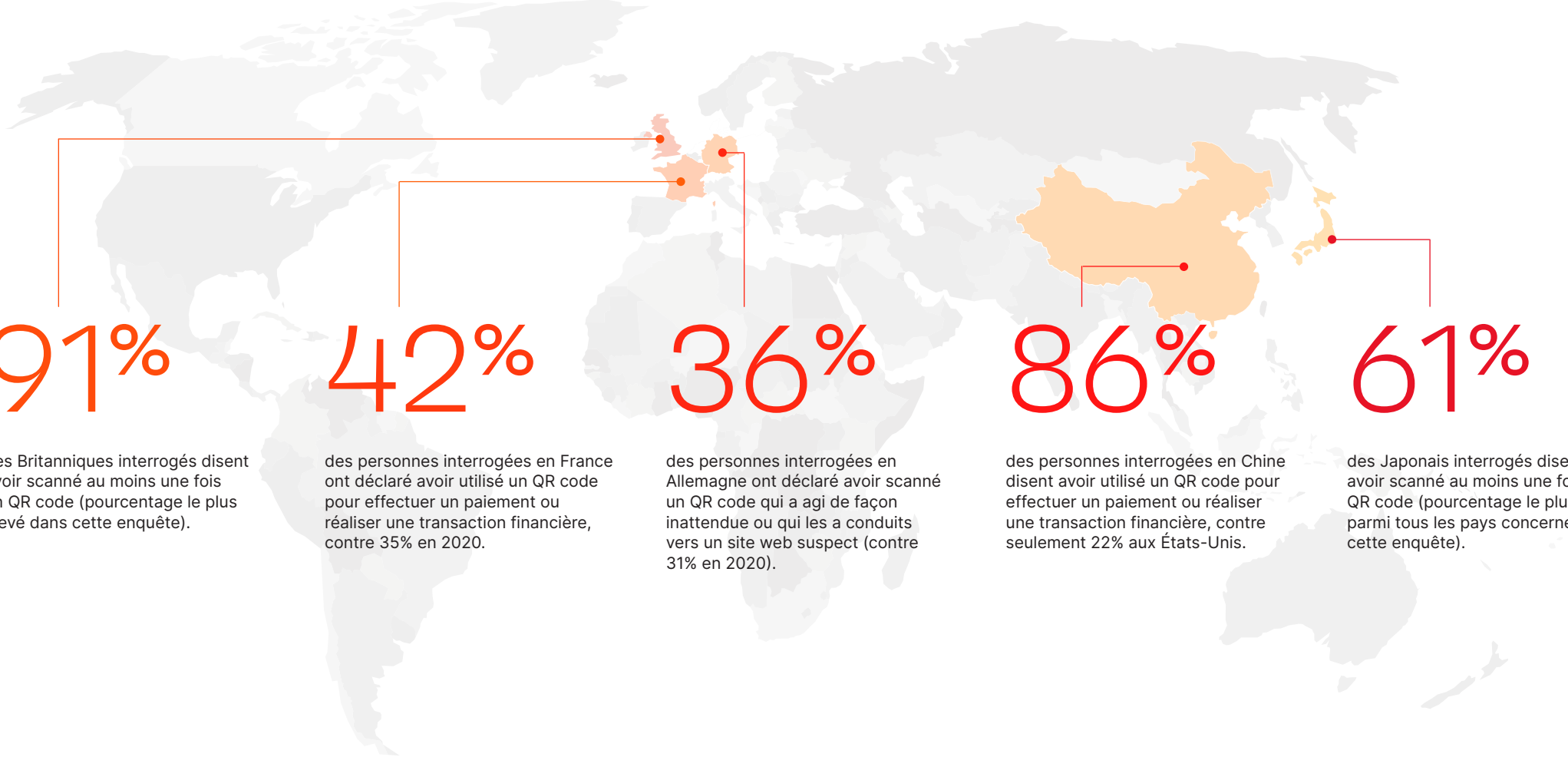
Parmi les pays inclus dans l'enquête, nous avons constaté que l'adoption des QR codes en Chine dépassait largement celle de tous les autres pays. Par exemple, la Chine a rapidement adopté le QR code pour toutes les activités, alors que les autres pays les utilisent principalement pour accélérer les transactions dans les restaurants, les bars et les cafés. Un point intéressant : plus de 40% des Chinois interrogés disent avoir scanné un QR code au cours des 6 derniers mois pour une opération financière (accès à leur compte bancaire, relevé de carte bancaire, distributeur). En comparaison, seulement 7% des Américains disent avoir utilisé des QR codes pour leurs transactions financières.

Ce qui est très curieux dans les résultats de cette année, c'est que le Japon (où le QR code a été inventé il y a des dizaines d'années pour accélérer les chaînes de montage automobiles) adopte plus lentement le QR code que les autres pays. En fait, seulement 61% des Japonais interrogés disent avoir au moins scanné une fois un QR code (pourcentage le plus faible parmi tous les pays concernés par cette enquête).

Le fait le plus notable, peut-être, est que l'utilisation des QR codes aux États-Unis semble ralentir. Moins d'un tiers des personnes interrogées disent avoir scanné un QR code au cours de la semaine écoulée, contre 39% en 2020.

Le nombre des personnes disant avoir scanné un QR code au cours du dernier mois a baissé de 10 points : de 66% en 2020 à seulement 56% début 2021.

Même si les raisons de cette tendance à la baisse aux États-Unis restent inconnues, la confiance du grand public vis-à-vis des QR codes est globalement à la hausse… ce qui multiplie les occasions, pour les cybercriminels, d'exploiter ou d'abuser de cette technologie.



91%

des Britanniques interrogés disent avoir scanné au moins une fois un QR code (pourcentage le plus élevé dans cette enquête).

42%

des personnes interrogées en France ont déclaré avoir utilisé un QR code pour effectuer un paiement ou réaliser une transaction financière, contre 35% en 2020.

36%

des personnes interrogées en Allemagne ont déclaré avoir scanné un QR code qui a agi de façon inattendue ou qui les a conduits vers un site web suspect (contre 31% en 2020).

86%

des personnes interrogées en Chine disent avoir utilisé un QR code pour effectuer un paiement ou réaliser une transaction financière, contre seulement 22% aux États-Unis.

61%

des Japonais interrogés disent avoir scanné au moins une fois un QR code (pourcentage le plus faible parmi tous les pays concernés par cette enquête).

Une plus grande confiance augmente-t-elle le danger des QR codes ?

Même si notre enquête a révélé un niveau d'adoption différent selon le pays, la confiance vis-à-vis des QR codes a augmenté partout. Souvent, les consommateurs expriment moins d'inquiétudes et sont moins conscients des risques potentiels des QR codes. Par exemple, les personnes interrogées en 2021 étaient moins inquiètes des dangers pour la confidentialité (51%) et des risques de fuites de données (46%) qu'en 2020, où 58% des consommateurs s'inquiétaient de la confidentialité et plus de la moitié (51%), des conséquences financières. De plus, la connaissance générale des actions que peut effectuer un QR code, comme ouvrir une URL, envoyer un SMS ou révéler l'emplacement de l'utilisateur, a baissé pour toutes les catégories.

Comme près de la moitié (51%) des utilisateurs n'ont pas installé de système de sécurité sur leur périphérique mobile (ou ignorent si cela a été fait), les départements IT doivent vraiment faire de la protection contre les QR codes malveillants une priorité pour 2021.

Il n'est donc pas étonnant de voir que davantage de consommateurs utilisent les QR codes pour leurs activités privées, sans vraiment se soucier de la sécurité. En fait, 83% des personnes interrogées disent qu'elles ont utilisé un QR code pour effectuer un paiement (ou réaliser une transaction financière) au cours de l'année écoulée. Parmi ces personnes, 54% ont utilisé un QR code dans un but financier, rien que dans les 3 derniers mois. Cette augmentation dramatique pourrait être liée à une baisse des inquiétudes pour la sécurité, ainsi qu'à la normalisation des paiements sans contact pendant la pandémie.

Cependant, voici le résultat réellement inquiétant pour notre sécurité : même si l'utilisation des QR codes diminue sur l'ensemble des consommateurs, ces QR codes servent à accéder à des informations plus sensibles, comme les détails des cartes bancaires, les comptes bancaires et les dossiers de santé. En parallèle, les QR codes réalisent plus fréquemment des opérations que l'utilisateur n'attendait pas ou, pire encore, l'amènent à des sites Web malveillants. Si l'on y ajoute le fait que près de la moitié (51%) des utilisateurs n'ont pas installé de système de sécurité sur leur périphérique mobile (ou ignorent si cela a été fait), les départements IT doivent vraiment faire de la protection contre les QR codes malveillants une priorité pour 2021.

83%

des personnes interrogées disent qu'elles ont utilisé un QR code pour effectuer un paiement (ou réaliser une transaction financière) au cours de l'année écoulée. Parmi ces personnes, 54% ont utilisé un QR code dans un but financier, rien que dans les 3 derniers mois.

47%

des personnes interrogées savent qu'un QR code peut ouvrir une URL, contre 61% en septembre 2020 (soit une baisse de 14 points).

37%

des personnes interrogées savent qu'un QR code peut télécharger une application, soit une baisse de 12 points par rapport à 2020.

Quelle est l'évolution du paysage des menaces mobiles?

Comme notre enquête l'a montré, moins de la moitié des utilisateurs dans le monde disposent d'un outil de sécurité mobile sur leurs périphériques. Les cybercriminels sont également au courant. C'est pourquoi leurs tactiques ont évolué afin de cibler les utilisateurs mobiles, généralement moins sécurisés et plus distraits que les utilisateurs des PC d'entreprise. L'utilisation de QR codes pour lancer des attaques sur les périphériques mobiles, on en parlait déjà en 2013, et il était clair que des pirates liaient des QR codes à des sites Web incorporant du malware. Le site Web malveillant infecte le périphérique à l'aide d'un cheval de Troie, qui lance ensuite des attaques de surveillance et d'exfiltration des données pour envoyer ces informations aux serveurs du pirate.

Peu de choses ont changé depuis, sauf que les QR codes sont bien plus répandus en 2021 qu'en 2013, et utilisés pour davantage de transactions. Si l'on y ajoute le manque général d'information des consommateurs sur le fonctionnement des QR codes, l'on voit qu'ils sont un outil de choix pour les pirates.

Aujourd'hui, les utilisateurs peuvent sans le savoir scanner des QR codes frauduleux, les amenant à un site Web d'aspect légitime, mais qui les invite à entrer des données comme leur nom d'utilisateur, leur mot de passe, les détails de leur carte bancaire, leur ID de connexion d'entreprise, etc.

Le cybercriminel utilise ensuite ces données pour accéder aux comptes de l'utilisateur ou aux applications et données d'entreprise stockées sur le périphérique. Comme les chevaux de Troie du passé, les QR codes de 2021 peuvent toujours servir à télécharger un logiciel malveillant sur un périphérique mobile à l'insu de l'utilisateur.

Même si les techniques ont changé et continuent d'évoluer, le but est le même : accéder à des données précieuses. C'est pourquoi il est plus important que jamais de mettre en place les fondations d'une sécurité mobile capable de vous protéger de ces menaces changeantes.

Une bonne protection nécessite une sécurité mobile et la formation des utilisateurs

Il n'est pas étonnant que les pirates continuent à utiliser des QR codes pour accéder aux périphériques, aux applications et aux données mobiles. Les principales raisons sont que les QR codes sont bon marché et qu'ils sont faciles à générer et à exploiter. En combinant la formation des consommateurs, une bonne hygiène de sécurité et une plateforme de sécurité mobile robuste, vous pouvez limiter - voire même éliminer totalement - ces risques.

Ce que les utilisateurs peuvent faire

- Ne jamais faire confiance à un e-mail provenant d'un expéditeur inconnu (c'est toujours une bonne pratique de sécurité).
- Traiter les QR codes inconnus comme les URL inconnues, puisque c'est presque la même chose.
- S'assurer que le QR code est un original et qu'aucun autre n'a été collé dessus, s'il s'agit d'un code physique, comme dans un magasin.
- Utiliser le logiciel de lecture de QR code pour examiner l'URL avant de cliquer dessus.

Ce que les entreprises peuvent faire

Comme nous l'avons dit, l'utilisateur ne sait généralement pas si son périphérique mobile dispose d'un outil de sécurité. Et franchement, c'est très bien comme ça. Les collaborateurs distants doivent pouvoir rester productifs sans avoir sans cesse à mettre à jour un logiciel de sécurité ou à saisir leur mot de passe pour accéder aux applications et données de l'entreprise.

La sécurité mobile Zero Trust, qui vérifie chaque périphérique, utilisateur, application, URL, réseau et Cloud, est indispensable. Elle vous protège de l'hameçonnage et autres exploitations malveillantes qui exploitent des QR codes pour contourner les logiciels antivirus traditionnels. Plus précisément, les entreprises ont besoin d'une plateforme complète de gestion des périphériques mobiles et de sécurité, capable de découvrir, gérer et sécuriser tous les périphériques qui accèdent aux ressources de l'entreprise.

Si vous pouvez voir et protéger tous les périphériques de votre Everywhere Workplace, vous pourrez vous protéger des attaques par hameçonnage, ainsi que des menaces qui visent les périphériques, les applications et le réseau, même si les périphériques ne sont pas connectés au réseau. De plus, en promouvant l'utilisation de l'authentification multifacteur (MFA), les entreprises peuvent aussi éliminer les mots de passe, qui sont l'une des principales causes de fuites de données en cas d'hameçonnage.

ivanti

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr

I. [Report overview]
II. En septembre 2020, MobileIron (racheté par Ivanti en décembre 2020) a mené une enquête ambitieuse auprès d'environ 4 500 consommateurs aux États-Unis, au Royaume-Uni, en Allemagne, aux Pays-Bas, en France, et en Espagne. (Vous trouverez les résultats de cette enquête ici.) Début 2021, Ivanti a complété cette enquête pour inclure des consommateurs en Chine et au Japon, à la place de l'Espagne et des Pays-Bas qui figuraient dans l'enquête initiale. Cette dernière enquête offre une image plus large de l'utilisation des codes QR au-delà des États-Unis et de l'Europe centrale pour donner aux professionnels de la sécurité davantage de détails sur les tendances mondiales en matière de QR code.