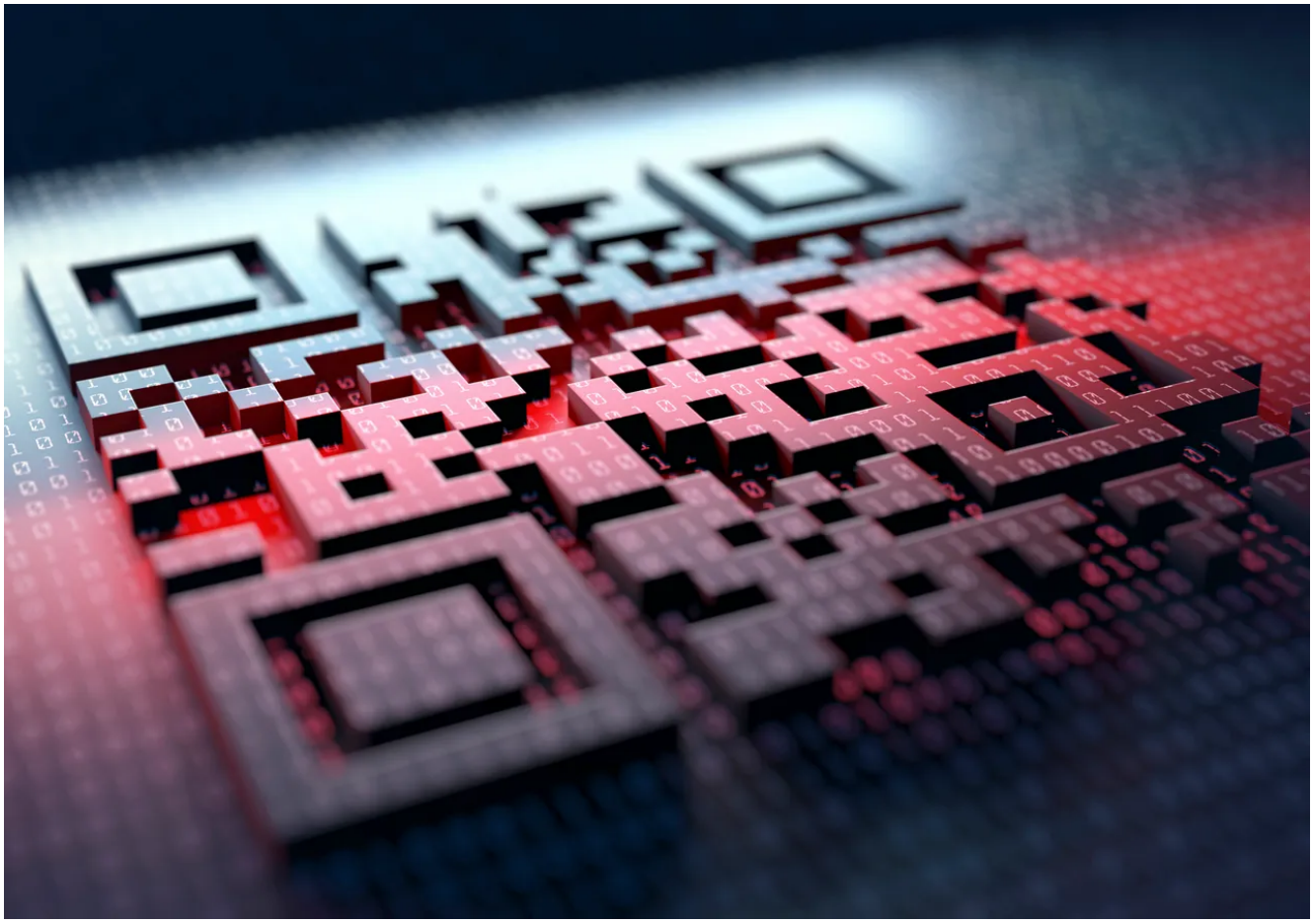
www.zdnet.com /article/quishing-is-the-new-phishing-what-you-need-to-know/

"Quishing" est le nouvel hameçonnage et ce que vous devez savoir

NDLR: Quishing signifie une combinaison des mots " code QR et Phishing " qui veut dire hameçonnage

La cybercriminalité semble toujours trouver un nouveau moyen de tirer parti des technologies modernes et maintenant les codes QR sont la prochaine chose.

Écrit par Jack Wallen, rédacteur collaborateur ⋮



KTSDESIGN/SCIENCE PHOTO LIBRARY/Getty Images

Je me souviens qu'il y a quelques Super Bowls, le réseau d'hébergement affichait une publicité d'entreprise qui n'était rien de plus qu'un code QR.
Même à l'époque, j'ai dit à ma femme : « Oh, mon garçon, ça pourrait devenir moche. » Le fait est que, comme toute chose, les codes QR semblent toujours inoffensifs... jusqu'à ce qu'ils ne le soient plus.

À lire aussi : Les meilleurs services VPN : testés et examinés par des experts

Les amis, nous sommes arrivés à ce point où les codes QR ont commencé à être utilisés comme armes dans les attaques de phishing.

C’est-à-dire qu’il faut s’arrêter.

Tout d’abord, un peu de retour en arrière.

Pour ceux qui n’ont pas entendu ce terme, l’hameçonnage est un type d’ingénierie sociale que les attaquants utilisent pour tromper les gens afin qu’ils révèlent ou transmettent des informations sensibles (telles que des noms d’utilisateur et des mots de passe) ou même qu’ils installent des logiciels malveillants.

À lire aussi : Comment activer le mode DNS privé sur Android (et pourquoi vous devriez)

L’hameçonnage existe depuis très longtemps et a pris de nombreuses formes au fil des ans.
Dans ce tour de passe-passe, les attaques utilisent des codes QR, c’est-à-dire des quishing.

Considérez le code QR diffusé pendant le Super Bowl.
Maintenant, imaginez que l’entreprise derrière cette publicité avait une intention malveillante (juste pour être clair, l’entreprise derrière cette publicité *n’avait pas* d’intention malveillante).
Disons, par exemple, que le code QR affiché pendant la publicité ouvre le navigateur de votre téléphone et télécharge et installe automatiquement un rançongiciel.
Compte tenu du nombre de personnes qui regardent le Super Bowl, le résultat de cette attaque aurait pu être désastreux.

À lire aussi : Qu’est-ce que le dark web ? Voici tout ce qu’il faut savoir avant d’y accéder

C’est ce qu’on appelle l’hésitation.
Tromper une personne (ou un certain nombre de personnes) en lui faisant croire quelque chose est inoffensif (ou nécessaire), mais la véritable intention est loin d’être innocente.
L’objectif est d’accéder à vos informations, de voler vos identifiants de compte bancaire et bien plus encore.

Pourquoi est-ce un problème ?

Les codes QR sont partout : dans les restaurants, les transports en commun, les publicités, les enseignes, les murs, les salles de bains, les publicités et même les entreprises expédient leurs produits avec des codes QR, afin que les consommateurs puissent accéder aux manuels sur leurs téléphones.

Nous venons tous d’accepter le code QR.
Et, à cette fin, nous leur faisons confiance.
Après tout, à quel point un simple code QR peut-il être nocif ?
La réponse à cette question est... très.
Et les cybercriminels comptent sur l’idée que la plupart des consommateurs supposent toujours que les codes QR sont inoffensifs.
Ces mêmes criminels comprennent également que leurs cibles les plus faciles sont celles qui utilisent des téléphones portables.
Pourquoi?
Parce que la plupart des systèmes d’exploitation de bureau incluent une protection contre l’hameçonnage.
Les téléphones, en revanche, sont beaucoup plus vulnérables à ces attaques.

À lire aussi : 9 principales menaces de sécurité mobile et comment les éviter

À l'heure actuelle, la plupart des attaques de quishing impliquent des criminels qui envoient un code QR par courriel.
Le plus souvent, ces courriels servent d'appel aux utilisateurs pour qu'ils vérifient les comptes et que l'utilisateur en question doit agir dans un certain délai, sinon son compte sera verrouillé ou fermé.
L'idée est qu'un utilisateur verrait le code QR dans son e-mail de bureau et le scannerait avec son téléphone.
Une fois scanné, le code QR ferait des ravages sur l'appareil.

Bien sûr, ce n'est pas la seule façon dont un auteur de menace pourrait utiliser un code QR pour duper les gens et les amener à tomber dans le piège de leur escroquerie. Comme je l'ai dit, les codes QR sont partout.
Qu'est-ce qui empêche un cybercriminel de placarder des codes QR partout, sachant qu'un spectateur innocent scannerait le code pour déclencher une attaque planifiée ?

Que pouvez-vous faire ?

La chose la plus simple que vous puissiez faire est de ne pas scanner les codes QR... en particulier ceux de sources inconnues.
La *seule* fois où je scanne un code QR, c'est après avoir vérifié la source.
Même dans ce cas, je ne le numériserai que si je dois absolument le faire.

Si vous recevez un courriel avec un code QR, la première chose à faire est de vérifier la validité de l'expéditeur.
Par exemple, si vous recevez un courriel avec un code QR qui prétend provenir de l'entreprise X, mais que vous regardez le courriel de l'expéditeur et qu'il provient de Gmail ou d'un domaine aléatoire (inconnu), il y a de fortes chances qu'il s'agisse d'une attaque de quishing.

À lire aussi : Qu'est-ce que Facebook Protect ? Voici pourquoi vous serez peut-être obligé de l'activer

Mon meilleur conseil est qu'un code QR dans un courriel ne doit jamais être scanné.
Les entreprises légitimes vous enverront toujours des instructions pour faire ce que vous devez faire.
Et la plupart des entreprises n'enverront certainement pas de code QR pour que vous puissiez vérifier votre compte.
Qu'en est-il des codes QR aléatoires que vous rencontrez dans le monde ?
Ne le faites pas.
Si vous laissez votre curiosité prendre le dessus sur vous, vous risquez de ne pas en subir les conséquences.

Tout comme les SMS provenant de sources inconnues, ces codes QR pourraient cacher des intentions dangereuses.
Donc, à moins d'être sûr à 100% de la source d'un code QR, ne le scannez jamais avec votre téléphone.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231030
"C'est ensemble qu'on avance"