23.10.2020

Tentatives de phishing actuellement en recrudescence

Les messages de phishing par email et par SMS ont de nouveau fortement augmenté depuis la fin de l'été. Les escrocs affinent de plus en plus leurs techniques. Ne vous laissez pas tromper !

Les cybercriminels font preuve non seulement d'excellentes compétences techniques, mais aussi d'ingéniosité. Alors que les messages de phishing liés au coronavirus étaient particulièrement répandus pendant le confinement, les escrocs inventent toujours de nouveaux scénarios pour piéger les utilisateurs crédules, notamment des prétendus blocages de comptes et de carte de crédit, des livraisons de colis bloquées, des bons d'achat gagnés et des remboursements de services de télécommunications.

Le problème est que ces messages frauduleux, qui arrivent généralement par email ou par SMS, sont de plus en plus crédibles. Le texte est écrit dans un allemand/français impeccable et les cyberarnaqueurs s'adressent souvent à leurs victimes au moyen de leur adresse mail, voire même directement par leur nom. L'adresse de l'expéditeur aussi est généralement falsifiée, et le site web auquel renvoie le lien présente souvent un https et un nom de domaine, ce que des profanes considèrent comme autant de marques de fiabilité. Dans le but de tromper les plus expérimentés, les escrocs préfèrent parfois les pièces jointes malveillantes aux liens.

La prudence est donc de mise, mais pas de panique : quelques règles de conduite simples permettent de se protéger efficacement contre toutes ces tentatives d'arnaque.

- Ne cliquez jamais sur un lien reçu par email, SMS ou Messenger, ou que vous auriez obtenu après avoir scanné un code QR, pour vous connecter à un service de banque en ligne.
- Ne remplissez jamais de formulaires envoyés par courriel et dans lesquels on vous demande d'indiquer vos identifiants de connexion.
- Traitez les pièces jointes de vos courriels et SMS avec méfiance.
- Ne révélez au téléphone aucune information confidentielle comme vos mots de passe par exemple.
- Tapez toujours manuellement l'adresse de la page d'accueil du site du fournisseur de services ou de la banque dans la barre d'adresse de votre navigateur.
- Lorsque la page d'accueil s'affiche, vérifiez la connexion SSL (https:// et symbole du cadenas) et contrôlez l'adresse Internet dans la barre d'adresse du navigateur pour vous assurer que vous êtes bien sur le bon site.
- En cas de doute, contactez toujours directement votre institut financier.

Vous trouverez d'autres informations utiles dans notre article sur le phishing (https://www.ebas.ch/phishing) .