19.12.2023

Alerte escroqueries : redoublez de vigilance !

Les autorités et les banques tirent la sonnette d'alarme pour signaler la recrudescence des tentatives de vol d'identifiants aux sessions d'e-banking des consommateurs. Les criminels disposent généralement de moyens professionnels et arrivent malheureusement trop souvent à leurs fins.

Plusieurs arnaques particulièrement soignées et au scénario identique occupent actuellement plusieurs établissements financiers et leurs clients.

D'une part, on assiste à une prolifération de copies apparemment authentiques de sites d'instituts financiers officiels (sites de phishing). Les victimes atterrissent généralement sur ces sites après avoir cliqué sur des liens contenus dans des emails de phishing ou affichés dans les résultats des moteurs de recherche. Lorsqu'un client bancaire saisit ses identifiants sur un de ces sites pirates, les données sont transmises en temps réel à la véritable page de connexion de la banque concernée. Dans l'étape suivante, le deuxième facteur de sécurité généré par le site légitime (p. ex. un QR code, une combinaison de chiffres ou une mosaïque) est également redirigé en temps réel sur le site pirate. Une fois que la victime, qui ne se doute de rien, a confirmé la connexion, les escrocs ont libre accès à son espace e-banking et à ses comptes bancaires. La procédure d'autorisation des virements effectués par les criminels suit ensuite le même schéma.

Un scénario d'arnaque très similaire a également été signalé sur les plateformes de petites annonces et de ventes aux enchères. Dans ce cas, l'escroc se présente au vendeur comme un client potentiel et lui demande ses coordonnées pour le paiement qu'il entend effectuer via un prestataire de paiements de type Paypal. Les données ainsi récoltées seront ensuite utilisées lors des prochaines étapes qui conduiront, là encore, à la prise de contrôle de la session d'e-banking du vendeur.

Dans un autre cas d'escroquerie, les criminels se font passer au téléphone pour des collaborateurs ou des responsables sécurité d'un institut bancaire pour obtenir des informations confidentielles telles que les identifiants à l'espace e-banking du client. Le numéro de téléphone est la plupart du temps maquillé pour tromper le client et endormir sa confiance. Cette arnaque repose là encore sur le modèle du phishing en temps réel, qui permet de contourner l'obstacle de l'authentification à deux facteurs.

Mais ce n'est pas tout : on enregistre actuellement une vague de fraudes à l'investissement. L'arnaque se présente souvent comme une offre d'emploi particulièrement lucrative ou par un scandale prétendument révélé par des personnalités célèbres. Après une première phase d'approche et de mise en confiance, les victimes sont souvent incitées à verser une petite somme d'argent sur un portail d'investissement présenté comme très rémunératif. Convaincues par la simulation des gains prétendument réalisés, elles sont ensuite incitées à effectuer des dépôts plus importants. Mais en réalité, les sommes d'argent atterrissent directement sur le compte bancaire des criminels.

Pour vous protéger contre le phishing...

- Pour vous connecter à un service de banque en ligne, ne cliquez jamais sur un lien reçu par email, SMS ou Messenger, ou que vous auriez obtenu après avoir scanné un QR code.

- Soyez méfiant à l'égard des pièces jointes de vos courriels et SMS.
- Ne révélez aucune information confidentielle au téléphone (p. ex. vos mots de passe).
- 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.
- En cas de doute, contactez toujours directement votre institut financier.

Pour vous protéger contre la fraude à l'investissement, il convient en revanche de suivre les règles suivantes :

- Ne vous laissez pas aveugler par des promesses de gains mirobolantes. Aucun prestataire de services financiers sérieux ne se hasardera jamais à promettre des gains exceptionnellement élevés sur du court-terme.
- Faites des recherches sur l'opérateur en question, sur Google par exemple, ou sur des forums et des sites de protection des consommateurs. Vérifiez que le prestataire dispose bien d'une autorisation de la FINMA (https://www.finma.ch/de/finma-public/bewilligte-institute-personen-und-produkte/) ou qu'il ne figure pas sur la liste noire de la FINMA (https://www.finma.ch/de/finma-public/warnliste/) , ni sur l'l'Investor Alerts Portal de l'OICV (https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal) . S'il s'agit d'un prestataire suisse, examinez l'extrait du registre du commerce des prestataires suisses sur www.zefix.ch (https://www.zefix.ch/de/search/entity/welcome) .
- En cas d'incertitude, n'hésitez pas à en parler au conseiller financier de votre banque.