MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Groupement de gendarmerie départementale de la Somme

28 janvier 2025

ALERTECYBERGEND80

Hier, un **samarien** a déposé plainte dans la brigade de gendarmerie de son secteur après avoir été victime d'une **fraude au faux conseiller bancaire**. Dans un premier temps, un **email frauduleux** semblant provenir de sa banque l'a incité à cliquer sur un lien menant à un **faux site**, visuellement identique en tous points à celui de son établissement bancaire. Sur ce faux site, il a saisi ses **identifiants bancaires** et son **mot de passe**.
Un **faux employé** de banque l'a ensuite contacté par téléphone pour lui signaler des transactions suspectes. Sous la **pression** et la **confiance** accordée à l'interlocuteur, il a transmis des **codes de sécurité** reçus par SMS. En conséquence, son compte bancaire a été vidé de plus de **12 000 euros.**

DÉCRYPTAGE ÉTAPE PAR ÉTAPE

L'e-mail d'hameçonnage

- Mimétisme parfait : Le mail était conçu pour ressembler trait pour trait à une communication officielle de la banque. L'adresse de l'expéditeur, le logo, la mise en page, tout était fait pour inspirer confiance.
- Le lien piège : Le lien "mon compte" ne dirigeait pas vers le véritable site de la banque, mais vers une fausse plateforme créée par les hackers. Cette plateforme était une réplique exacte du site légitime, de quoi tromper même les plus vigilants.

La collecte d'informations :

- Identifiants et mot de passe : En saisissant ses informations de connexion sur le faux site, la victime a offert aux hackers les clés de son compte bancaire.
- Informations personnelles : Le numéro de compte, la date de naissance et d'autres informations personnelles ont permis aux hackers de renforcer leur crédibilité et de gagner la confiance de leur victime.

L'appel téléphonique :

- Usurpation d'identité : En se faisant passer pour un employé de la banque, le hacker a pu entrer en contact direct avec la victime et poursuivre son escroquerie.
- La pression psychologique : En évoquant des virements suspects, le hacker a créé un sentiment d'urgence chez la victime, la poussant à agir rapidement et à lui faire confiance.

L'obtention des codes de sécurité :

- La promesse d'annuler les transactions : En prétendant pouvoir annuler les virements frauduleux, le hacker a incité la victime à lui communiquer les codes de sécurité reçus sur son téléphone.
- La répétition : En demandant plusieurs codes à différents moments, le hacker a maximisé ses chances de vider complètement le compte de sa victime.

POUR ÉVITER DE TOMBER DANS CE GENRE DE PIÈGE, IL EST ESSENTIEL DE RESTER VIGILANT ET DE SUIVRE QUELQUES CONSEILS SIMPLES

- **Ne cliquez jamais** sur des liens dans des emails non sollicités ;
- **Vérifiez toujours** l'adresse web du site sur lequel vous vous connectez ;
- **Ne communiquez jamais** vos informations personnelles par téléphone ou par email.