MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

FICHE CYBER

Fraude au faux conseiller bancaire

Statut : **En cours**
Secteurs affectés : **Tous**
Zones géographiques touchées : **France**
Objectif : **Lucratif**

SYNTHÈSE

La fraude au faux conseiller bancaire consiste pour un attaquant à contacter par téléphone une victime en se faisant passer pour un conseiller bancaire légitime, afin de lui soutirer des fonds en effectuant des achats en ligne ou en lui faisant valider des virements bancaires sur différents comptes. Les escrocs, aux profils très variés, adaptent leurs attaques exploitant des évolutions technologiques et sociétales. Leurs motivations sont principalement financières, et ceux-ci ciblent les personnes physiques.

EN QUOI CONSISTE CE PHÉNOMÈNE CYBERCRIMINEL ?

Les escroqueries représentent la part la plus importante des phénomènes cybercriminels sur l'année 2022. Parmi celles-ci, la **fraude au faux conseiller bancaire** constitue une **menace croissante** mettant en péril la s**écurité financière des usagers**. Celle-ci consiste pour un attaquant à se faire passer pour un conseiller bancaire légitime afin d'obtenir de la part de la victime, ses **informations sensibles**, **identifiants bancaires**, **codes PIN ou autres détails financiers**, afin de réaliser des paiements en ligne ou des virements, en exploitant de manière abusive la crédulité de la victime.

Si cette menace n'est pas nouvelle, celle-ci reste bien présente et ce, en raison de plusieurs facteurs. **Les escrocs**, toujours créatifs, **ajustent leurs stratégies pour exploiter les avancées technologiques et sociétales**. Ceux-ci profitent de l'accès simple et rapide à de nombreuses données de leurs victimes en ligne notamment sur le ***darkweb*** ou sur des **forums cybercriminels** qu'ils obtiennent gratuitement ou contre plusieurs dizaines d'euros. Lors de l'appel, les escrocs sont souvent déjà en possession de **l'identité, l'adresse, le numéro de téléphone, les coordonnées bancaires et les numéros des cartes bancaires de leur victime.**

D'autre part, **les innovations technologiques** facilitent le travail de ces cybercriminels qui peuvent aisément **modifier leurs voix** et profiter d'un **quasi anonymat**. D'autres techniques de ***spoofing*** permettent également aux attaquant de faire apparaitre le numéro officiel de la banque sur le téléphone de la victime, trompant à nouveau sa vigilance. Des acteurs malveillants mettent à disposition *via* des applications de messagerie instantanée des **outils de spoofing** « clé en main » ainsi que du texte (script de communication) pour communiquer avec la victime et revendiquent parfois plus **de 90% de taux de réussite**. Ces techniques autrefois réservées à des attaquants aguerris ont tendance à se démocratiser.

Les profils de ces acteurs malveillants opérant ce type d'attaque sont désormais **très variés**, du **groupe d'attaquants expérimentés** et **organisés** à **l'attaquant isolé et opportuniste**. Leurs motivations résident principalement dans **la recherche de gains financiers rapides**, au détriment de clients peu avertis.

QUE DIT LA LOI ?

Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite
- article 226-18 du code pénal
- cinq ans d'emprisonnement et 300 000 euros d'amende.

Escroquerie
- article 313-1 du code pénal
- cinq ans d'emprisonnement et 375 000 euros d'amende.

Accès frauduleux à un système de traitement automatisé de données (STAD)
- article 323-1 du Code pénal
- trois ans d'emprisonnement et 100 000 euros d'amende. Lorsqu'il y a suppression ou modification de données contenues dans le système, ou une altération du fonctionnement de ce système, la peine est portée à cinq ans d'emprisonnement et à 150 000 euros d'amende.

MODE OPERATOIRE

1. APPEL

L'escroc contacte la victime par téléphone en se faisant passer pour un conseiller bancaire. Il indique à la victime qu'elle a été victime d'une fraude à la carte bancaire.

2. MISE EN CONFIANCE

L'escroc indique à la victime qu'il va annuler les opérations frauduleuses. Pour gagner en crédibilité, il lui demande de vérifier ses informations personnelles.

3. COMPROMISSION

L'escroc demande à la victime de lui communiquer les codes de confirmation qu'elle reçoit par SMS et de valider les opérations sur l'application bancaire.

4. OPÉRATIONS FRAUDULEUSES

Grace à ces opérations, l'escroc réalise des paiements en ligne et/ou des virements bancaires sur des comptes frauduleux.

5. ENVOI D'UN COURSIER

L'escroc invite la victime à faire opposition sur ses cartes bancaires et à les remettre à un coursier qui se présentera à son domicile.

ACTES PREPARATOIRES

RECUPERATION DE DONNEES

Les escrocs récupèrent ou acquièrent des données personnelles de leurs victimes notamment sur le *darkweb* pour mener à bien leurs attaques et gagner en crédibilité lors de l'échange avec la victime.

ANONYMAT

Les escrocs peuvent s'appuyer sur des technologies modernes pour modifier leurs voix, usurper un numéro de téléphone (*spoofing*) et se rendre quasiment anonymes.

SCRIPT DE COMMUNICATION

Les escrocs préparent un discours de nature à créer un effet de surprise et exercent une pression psychologique insistant notamment sur l'urgence à agir, pour induire les victimes en erreur.

COMMENT S'EN PREMUNIR ?

- ✖ Votre banque ne vous demandera jamais de réaliser des opérations bancaires *via* les outils d'authentification mis à votre disposition sur votre application bancaire.
- ✖ Ne communiquez jamais vos codes de confirmation.
- ✖ Si vous avez un doute, raccrochez et contactez immédiatement votre banque pour vérifier que vous avez le bon interlocuteur.
- ✖ Si vous avez été victime de ce type de fraude, modifiez vos codes d'accès à votre espace bancaire, contactez votre banque et déposez plainte sans délai dans une brigade de gendarmerie ou un commissariat de police.

SOURCES

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417968/
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418192/
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/fraude-faux-conseiller-bancaire#protection-fraude-faux-conseiller-bancaire