RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

FRAUDE AU FAUX CONSEILLER BANCAIRE

La fraude au faux conseiller bancaire est une forme d'escroquerie dans laquelle l'escroc contacte la victime en prétendant être un agent du service anti-fraude de sa banque, dont il usurpe parfois le numéro de téléphone. L'escroc prétend avoir identifié des opérations suspectes en cours sur le compte de la victime. Pour les bloquer, il demande à la victime de lui donner des codes reçus par SMS ou de confirmer des actions sur son application bancaire. Ces actions permettent en réalité à l'escroc de valider des achats ou virements frauduleux. Les informations utilisées pour cibler la victime (identité, adresse, coordonnées de carte bancaire…) ont pu être obtenues par hameçonnage (*phishing*), piratage de compte, ou encore virus voleur de mots de passe sur un appareil de la victime (ordinateur, téléphone…), etc.

BUT RECHERCHÉ

Tromper la victime pour l**ui faire valider des opérations frauduleuses sur ses comptes bancaires.**

SI VOUS ÊTES VICTIME

MÉFIEZ-VOUS DES APPELS OU MESSAGES (SMS…) ALARMANTS qui vous informent d'opérations frauduleuses sur vos comptes et vérifiez l'information par vous-même en contactant votre banque par vos moyens habituels.

NE FOURNISSEZ JAMAIS DE MOTS DE PASSE, DE CODES ET NE VALIDEZ EN AUCUN CAS DES OPÉRATIONS DONT VOUS N'ÊTES PAS À L'ORIGINE même sous prétexte de les annuler.

FAITES OPPOSITION À VOTRE CARTE BANCAIRE SANS DÉLAI ET CHANGEZ LE MOT DE PASSE DE VOTRE COMPTE BANCAIRE EN LIGNE si les escrocs y ont accédé ou si vous le soupçonnez.

ALERTEZ VOTRE BANQUE des opérations frauduleuses identifiées pour en demander l'annulation.

CONSERVEZ LES PREUVES (numéros de téléphone, messages ou mails reçus, ordres de virement, relevés de paiements, etc.).

Si la fraude porte sur votre carte bancaire, **SIGNALEZ LES FAITS SUR LA PLATEFORME PERCEVAL.**

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez en fournissant toutes les preuves en votre possession.

RÉALISEZ UNE ANALYSE (SCAN) ANTIVIRALE COMPLÈTE DE VOS APPAREILS pour rechercher d'éventuelles infections qui auraient pu être à l'origine de la fraude.

Pour plus de conseils, **CONTACTEZ INFO ESCROQUERIES** au 0 805 805 817 (appel et service gratuits).

MESURES PRÉVENTIVES

Notez qu'aucun conseiller de votre banque ne vous demandera de lui communiquer votre mot de passe, des codes de confirmation ou encore d'effectuer des actions sur votre application bancaire pour de supposées fraudes en cours sur vos comptes.

Méfiez-vous des messages d'hameçonnage (mail ou SMS) qui vous amènent à communiquer des informations personnelles et/ou bancaires. Au moindre doute, contactez l'organisme concerné.

Appliquez de manière régulière et systématique les mises à jour de sécurité du système, des applications et des logiciels installés sur vos appareils.

N'installez des applications ou logiciels que depuis les sites ou magasins officiels au risque de télécharger une version infectée par un virus.

Utilisez un antivirus pour vous protéger des virus qui pourraient dérober vos informations personnelles et bancaires ou encore vos mots de passe.

Utilisez des mots de passe différents et complexes pour chaque site et application que vous utilisez. Activez la double authentification quand elle est disponible.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues contre leurs auteurs :

- **Escroquerie (article 313-1 du code pénal).** L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

- **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal).** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal).** Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V240201