mémo

COMPRENDRE LES RISQUES

LE PIRATAGE DE COMPTE

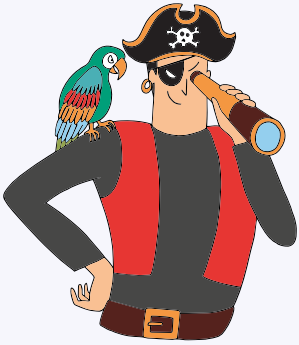
CYBERCRIMINEL

VOL DE DONNÉES

Vous constatez une activité anormale ou inquiétante sur vos comptes ou applications (messagerie, réseaux sociaux, sites administratifs, banques, sites e-commerce…) ? Vous êtes peut-être victime d'un piratage de compte !

BUT
Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.)

TECHNIQUE
Prise de contrôle d'un ou plusieurs comptes en ligne, suite à un mot de passe trop simple, communiqué sans le savoir suite à un message frauduleux ou utilisé sur plusieurs sites dont l'un a été piraté.



VICTIME

COMMENT RÉAGIR ?

- Changez votre mot de passe piraté sur tous les sites ou comptes sur lesquels vous pouviez l'utiliser
- Vérifiez que les coordonnées de récupération de votre compte (e-mail, téléphone) n'ont pas été modifiées
- Prévenez votre banque
- Prévenez tous vos contacts de ce piratage
- Sauvegardez les preuves
- Déposez plainte si le préjudice le justifie

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

SES MISSIONS

1. **ASSISTANCE AUX VICTIMES** D'ACTES DE CYBERMALVEILLANCE
2. **INFORMATION ET SENSIBILISATION** À LA SÉCURITÉ NUMÉRIQUE
3. **OBSERVATION ET ANTICIPATION** DU RISQUE NUMÉRIQUE

QUI EST CONCERNÉ ?

- PARTICULIERS
- COLLECTIVITÉS TERRITORIALES
- ENTREPRISES

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

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

mémo

COMPRENDRE LES RISQUES

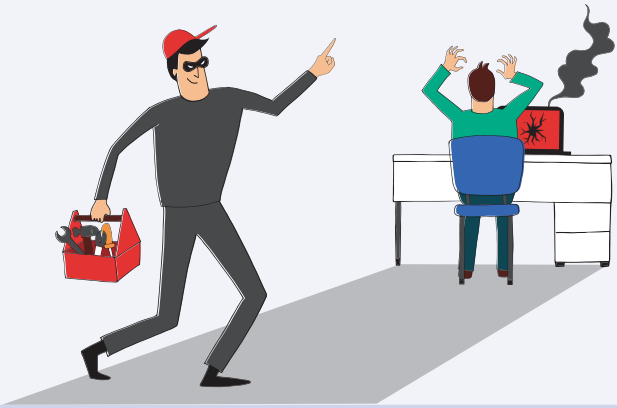
LES **FAUX SUPPORTS TECHNIQUES**

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT
Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants.

TECHNIQUE
Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).



COMMENT RÉAGIR ?

- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

LIENS UTILES

Internet-signalement.gouv.fr

Info Escroqueries
0 805 805 817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

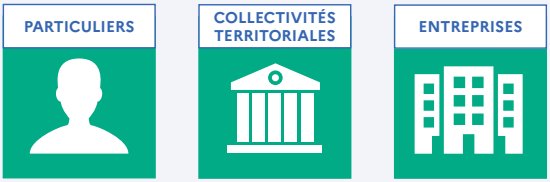
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

SES MISSIONS

1. **ASSISTANCE AUX VICTIMES** D'ACTES DE CYBERMALVEILLANCE
2. **PRÉVENTION ET SENSIBILISATION** À LA SÉCURITÉ NUMÉRIQUE
3. **OBSERVATION ET ANTICIPATION** DU RISQUE NUMÉRIQUE

QUI EST CONCERNÉ ?



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

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

COMPRENDRE LES RISQUES

LA FRAUDE À LA CARTE BANCAIRE

La fraude à la carte bancaire désigne l'utilisation frauduleuse des coordonnées de la carte bancaire d'une personne à son insu alors que celle-ci est pourtant toujours en possession de sa carte. Trouver l'origine précise d'une telle fraude est souvent difficile. En effet, pour obtenir les coordonnées de la carte bancaire de la victime, le fraudeur peut utiliser de nombreuses méthodes comme l'hameçonnage (***phishing*** en anglais) à travers un message incitant la victime à fournir ses coordonnées, le piratage d'un compte en ligne de la victime sur lequel les coordonnées de la carte seraient inscrites (commerce en ligne, réseaux sociaux…), le piratage d'un équipement informatique de la victime (ordinateur, téléphone…), l'utilisation d'une fuite de données d'un site en ligne sur lequel la victime aurait laissé les coordonnées de sa carte, le piégeage d'un distributeur de billets ou même lors d'un paiement chez un commerçant malhonnête qui aurait pu photographier la carte.

BUT RECHERCHÉ

Dérober les coordonnées bancaires de la victime pour en faire un usage frauduleux (achats en ligne, etc.)

SI VOUS ÊTES VICTIME

FAITES IMMÉDIATEMENT OPPOSITION À VOTRE CARTE BANCAIRE en cas de fraude.

Dès l'identification d'un débit frauduleux sur votre compte bancaire, **ALERTEZ VOTRE BANQUE AU PLUS VITE POUR EN DEMANDER LE REMBOURSEMENT.**

SIGNALEZ LA FRAUDE BANCAIRE AUPRÈS DE LA PLATEFORME PERCEVAL du ministère de l'Intérieur.

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

METTEZ À JOUR VOS ÉQUIPEMENTS pour corriger les failles de sécurité qu'aurait pu utiliser le fraudeur pour en prendre le contrôle.

RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN) de vos appareils pour supprimer les virus qui auraient pu être à l'origine de la fraude à la carte bancaire.

ASSUREZ-VOUS QU'AUCUN DE VOS COMPTES EN LIGNE NE SOIT PIRATÉ. Au moindre doute, changez les mots de passe et activez la double authentification si disponible. Choisissez des mots de passe différents et complexes pour chacun de vos comptes.

MESURES PRÉVENTIVES

Ne communiquez jamais vos coordonnées bancaires par messagerie, par téléphone ou sur Internet.

Conservez précieusement votre carte bancaire et son code confidentiel.

Vérifiez régulièrement votre compte bancaire pour identifier tout débit suspect.

Pour des achats ponctuels sur un site Internet, **n'enregistrez pas vos coordonnées bancaires** et supprimez-les si vous ne l'utilisez plus. Vérifiez également la notoriété du site Internet avant de réaliser un achat (recherche sur Internet ou d'avis par exemple).

Privilégiez les moyens de paiement sécurisés (e-Carte Bleue, Paylib, etc.). Contactez votre banque pour connaître les solutions qu'elle propose.

Si vous n'avez pas réalisé d'achat, **soyez vigilant aux demandes de validation** qui prennent souvent la forme de numéro à communiquer et qui pourraient vous amener à valider des transactions dont vous n'êtes pas l'auteur.

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute (tous nos conseils pour gérer vos mots de passe). **Activez la double authentification** si disponible.

Mettez régulièrement à jour votre appareil, votre système d'exploitation ainsi que les logiciels et applications installés.

Après avoir vérifié que votre antivirus est en état de fonctionnement et à jour, **faites régulièrement une analyse antivirale complète (scan)** de votre appareil et supprimez les virus.

Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate

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 :

- En cas d'utilisation frauduleuse de coordonnées de carte bancaire : l'**escroquerie**. **L'article 313-1 du code pénal** dispose que : « *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* ». Ce délit est passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

- En cas de piratage d'un système informatique (ordinateur, téléphone mobile, tablette…) : l'**infraction d'atteinte à un système de traitement automatisé de données (STAD)** peut être retenue. **Les articles 323-1 à 323-7 du code pénal** disposent notamment que : « *le fait d'accéder ou de se maintenir frauduleusement* » *dans un STAD,* « *la suppression ou la modification de données contenues dans le système* », « le fait […] d'extraire, de détenir, de reproduire, de transmettre […] les données qu'il contient » ou l'« *altération du fonctionnement de ce système* » sont passibles de trois à cinq ans d'emprisonnement et de 100 000 à 150 000 euros d'amende.

- Dans le cas de la fabrication d'une carte bancaire contrefaite : l'**infraction de faux et usage d'une contrefaçon d'un moyen de paiement** peut être retenue. **L'article 163-3 du Code monétaire et financier** dispose que : « *Est puni d'un emprisonnement de cinq ans et d'une amende de 375 000 euros le fait pour toute personne : 1. De contrefaire ou de falsifier un chèque ou un autre instrument mentionné à l'article L. 133-4 ; 2. De faire ou de tenter de faire usage, en connaissance de cause, d'un chèque ou un autre instrument mentionné à l'article L. 133-4 contrefaisant ou falsifié ; 3. D'accepter, en connaissance de cause, de recevoir un paiement au moyen d'un chèque ou d'un autre instrument mentionné à l'article L. 133-4 contrefaisant ou falsifié.* »

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

V230417

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

mémo

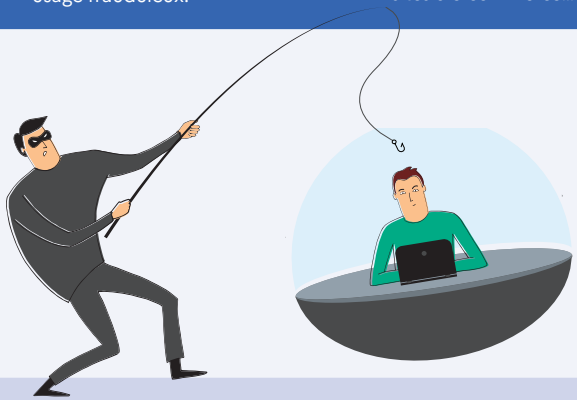
L'HAMEÇONNAGE

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT
Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE
Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…



COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel
- Au moindre doute, contactez directement l'organisme concerné pour confirmer

COMMENT DÉTECTER UN MESSAGE D'HAMEÇONNAGE ?

7 points de contrôle qui doivent vous alerter :

- Une notification de la messagerie ou de l'antivirus
- Un nom d'émetteur inhabituel
- Une adresse d'expédition fantaisiste
- Un objet de message succinct ou alarmiste
- Un message aguicheur ou inquiétant
- Des fautes de français surprenantes
- Une incitation à ouvrir un lien ou une pièce-jointe

PLUS D'INFORMATIONS SUR :
www.cybermalveillance.gouv.fr