RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

ADOPTER LES BONNES PRATIQUES

LES MOTS DE PASSE

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. **Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.**

1 UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE SERVICE

Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

2 UTILISEZ UN MOT DE PASSE SUFFISAMMENT LONG ET COMPLEXE

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

3 UTILISEZ UN MOT DE PASSE IMPOSSIBLE À DEVINER

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré. Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

4 UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès. Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès. *Voir notre encadré sur Keepass au dos de cette fiche.*

5 CHANGEZ VOTRE MOT DE PASSE AU MOINDRE SOUPÇON

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

CRÉER UN MOT DE PASSE SOLIDE

LA MÉTHODE DES PREMIÈRES LETTRES
Un tiens vaut mieux que deux tu l'auras
1tvmQ2tl'A

LA MÉTHODE PHONÉTIQUE
J'ai acheté huit CD pour cent euros cet après-midi
ght8CD%E7am

Inventez votre propre méthode connue de vous seul !

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

KEEPASS

UN GESTIONNAIRE DE MOTS DE PASSE SÉCURISÉ ET GRATUIT

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires. **https://keepass.info**

6 NE COMMUNIQUEZ JAMAIS VOTRE MOT DE PASSE À UN TIERS

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

7 N'UTILISEZ PAS VOS MOTS DE PASSE SUR UN ORDINATEUR PARTAGÉ

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

8 ACTIVEZ LA « DOUBLE AUTHENTIFICATION* » LORSQUE C'EST POSSIBLE

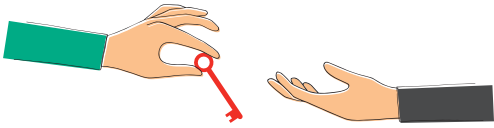
Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option . En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique. Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés. *Voir encadré.*

9 CHANGEZ LES MOTS DE PASSE PAR DÉFAUT DES DIFFÉRENTS SERVICES AUXQUELS VOUS ACCÉDEZ

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

- Outlook/Hotmail, Gmail, Yahoo Mail...
- Facebook, Instagram, LinkedIn, Snapshat, Tik Tok, Twitter...
- Skype, Teams, WhatsApp, Zoom...
- Amazon, eBay, Paypal...
- Apple iCloud, Dropbox, Google Drive, OneDrive...



10 CHOISISSEZ UN MOT DE PASSE PARTICULIÈREMENT ROBUSTE POUR VOTRE MESSAGERIE

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle. **Votre mot de passe de messagerie est donc un des mots de passe les plus importants à protéger**.

POUR ALLER PLUS LOIN

- **Par la CNIL :** Les conseils de la CNIL pour un bon mot de passe
- **Par l'ANSSI :** Sécurité des mots de passe

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

FRANCE ASSUREURS — FAIRE AVANCER LA SOCIÉTÉ EN CONFIANCE · kaspersky · LA POSTE GROUPE · signal spam

*Également appelée « authentification forte », « authentification multifacteurs », « 2FA », « vérification en deux étapes », « validation en deux étapes », « authentification à deux facteurs », « identification à deux facteurs », « vérification en deux temps »...

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

Version 2.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES **10 MESURES ESSENTIELLES** POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE

ADOPTER LES BONNES PRATIQUES

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés... Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. Comment se protéger au mieux face à ces risques ? **Voici 10 bonnes pratiques essentielles à adopter pour assurer votre sécurité numérique.**

1 PROTÉGEZ VOS ACCÈS AVEC DES MOTS DE PASSE SOLIDES

Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement en prévention, changez-les. Utilisez un gestionnaire de mots de passe et activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité.

2 SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT

En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages...). Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

3 APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS (PC, TABLETTES, TÉLÉPHONES...), DÈS QU'ELLES VOUS SONT PROPOSÉES

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner (mises à jour).

4 UTILISEZ UN ANTIVIRUS

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

5 TÉLÉCHARGEZ VOS APPLICATIONS UNIQUEMENT SUR LES SITES OFFICIELS

N'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streamings illégaux) qui pourraient également installer un virus sur vos matériels.

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

6 MÉFIEZ-VOUS DES MESSAGES INATTENDUS

En cas de réception d'un message inattendu ou alarmiste par messagerie (*e-mail*), SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par hameçonnage (*phishing*) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.

7 VÉRIFIEZ LES SITES SUR LESQUELS VOUS FAITES DES ACHATS

Si le commerce en ligne facilite les achats et offre l'opportunité de faire de bonnes affaires, il existe malheureusement de nombreux sites de vente douteux, voire malveillants. Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel, la crédibilité de l'offre et consultez les avis. Sans cette vérification, vous prenez le risque de vous faire dérober votre numéro de carte bancaire et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.

8 MAÎTRISEZ VOS RÉSEAUX SOCIAUX

Les réseaux sociaux sont de formidables outils de communication et d'information collaboratifs. Ils contiennent toutefois souvent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains. Sécurisez l'accès à vos réseaux sociaux avec un mot de passe solide et unique, définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire, ne relayez pas d'informations non vérifiées (*fake news*).

9 SÉPAREZ VOS USAGES PERSONNELS ET PROFESSIONNELS

Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent ténue. Ces utilisations peuvent même parfois s'imbriquer. Matériels, messageries, « *clouds* »… Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement, que la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles (usages personnels et professionnels).

10 ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire…). Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).

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

Version 10

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

COMPRENDRE LES RISQUES

L'HAMEÇONNAGE

L'hameçonnage (***phishing*** en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

BUT RECHERCHÉ

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

SI VOUS ÊTES VICTIME

En cas de doute, **CONTACTEZ DIRECTEMENT L'ORGANISME CONCERNÉ** pour confirmer le message ou l'appel que vous avez reçu.

Si vous avez communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte bancaire, **FAITES OPPOSITION IMMÉDIATEMENT** auprès de votre organisme bancaire ou financier.

Si vous avez communiqué un mot de passe, **CHANGEZ-LE IMMÉDIATEMENT** ainsi que sur tous les autres sites ou services sur lesquels vous l'utilisiez (tous nos conseils pour gérer au mieux vos mots de passe).

CONSERVEZ LES PREUVES et, en particulier, le message d'hameçonnage reçu.

Si vous avez reçu un message douteux sans y répondre, **SIGNALEZ-LE À SIGNAL SPAM (SIGNAL-SPAM.FR).**

Vous pouvez également **SIGNALER UNE ADRESSE DE SITE D'HAMEÇONNAGE À PHISHING INITIATIVE (PHISHING-INITIATIVE.FR)** qui en fera fermer l'accès.

En fonction du préjudice subi (débits frauduleux, usurpation d'identité…) **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

Pour être conseillé en cas d'hameçonnage, contactez **INFO ESCROQUERIES AU 0 805 805 817** (numéro gratuit).

MESURES PRÉVENTIVES

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

En cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

Utilisez des mots de passes différents et complexes pour chaque site et application afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres-forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

Si le site le permet, **vérifiez les date et heure de dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.

Si le site vous le permet, **activez la double authentification pour sécuriser vos accès.**

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 :

- **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. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal)** : une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 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 trois ans d'emprisonnement et de 100 000 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 encourue est de cinq ans d'emprisonnement et de 150 000 euros.

- **Contrefaçon et usage frauduleux de moyen de paiement (articles L163-3 et L163-4 du code monétaire et financier)** : délit passible d'une peine d'emprisonnement de sept ans et de 750 000 euros d'amende.

- **Usurpation d'identité (article 226-4-1 du code pénal)** : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.

- **Contrefaçon des marques (logos, signes, emblèmes…) utilisées lors de l'hameçonnage, prévu par les articles L.713-2 et L.713-3 du Code de la propriété intellectuelle.** Délit passible d'une peine d'emprisonnement de trois ans et de 300 000 euros d'amende.

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

LE PIRATAGE DE COMPTE

COMPRENDRE LES RISQUES

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne. En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières : le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (***phishing*** en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.

BUT RECHERCHÉ

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

SI VOUS ÊTES VICTIME

Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

Dans vos paramètres de récupération de compte, **ASSUREZ-VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS**. Si ce n'est pas le cas, changez-les immédiatement.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE et choisissez-en un solide (voir notre fiche sur la gestion des mots de passe). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION.**

CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE avec le compte piraté.

Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

En fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Utilisez des mots de passes différents et complexes pour chaque site et application utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

Lorsque le site ou le service le permettent, **activez la double authentification** pour augmenter le niveau de sécurité.

Ne communiquez jamais d'informations sensibles (mots de passe) par messagerie, par téléphone ou sur Internet.

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Maintenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

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

Évitez les sites non sûrs ou illicites, tels ceux hébergeant des contrefaçons dont ces dernières peuvent contenir des logiciels malveillants (musique, films, logiciels, etc.) ou certains sites pornographiques.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

Si le site le permet, **vérifiez les date et heure de la dernière connexion à votre compte** afin de repérer d'éventuelles connexions anormales.

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

Déconnectez-vous systématiquement de votre compte après utilisation pour éviter que quelqu'un puisse y accéder après vous.

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 :

- **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 trois ans d'emprisonnement et de 100 000 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 encourue est de cinq ans d'emprisonnement et de 150 000 euros.

Dans le cas d'un piratage d'un compte de messagerie :
- **Atteinte au secret des correspondances (article 226-15 du code pénal)** : délit passible d'une peine d'emprisonnement d'un an et de 45 000 euros d'amende.

Dans le cas de collecte de données à caractère personnel quel que soit le compte :
- **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.

Si le compte a été détourné pour usurper votre identité :
- **Usurpation d'identité par voie de télécommunication (article 226-4-1 du code pénal)** : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

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

LES RANÇONGICIELS

Un rançongiciel (***ransomware*** en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

BUT RECHERCHÉ

Extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Certaines attaques visent juste à endommager le système de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

SI VOUS ÊTES VICTIME

DÉBRANCHEZ LA MACHINE D'INTERNET ou du réseau informatique.

En entreprise, **ALERTEZ IMMÉDIATEMENT VOTRE SERVICE OU PRESTATAIRE INFORMATIQUE.**

NE PAYEZ PAS LA RANÇON réclamée car vous n'êtes pas certain de récupérer vos données et vous alimenteriez le système mafieux.

CONSERVEZ LES PREUVES: message piégé, fichiers de journalisation (logs) de votre pare-feu, copies physiques des postes ou serveurs touchés. À défaut, conservez les disques durs.

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

Professionnels : **NOTIFIEZ L'INCIDENT À LA CNIL** s'il y a eu une violation de données personnelles.

IDENTIFIEZ LA SOURCE DE L'INFECTION et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

APPLIQUEZ UNE MÉTHODE DE DÉSINFECTION ET DE DÉCHIFFREMENT, lorsqu'elle existe*. En cas de doute, effectuez une restauration complète de votre ordinateur. Reformatez les postes et/ou serveurs touchés et réinstallez un système sain puis restaurez les copies de sauvegarde des fichiers perdus lorsqu'elles sont disponibles.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS. Vous trouverez sur www.cybermalveillance.gouv.fr des professionnels en sécurité informatique susceptibles de pouvoir vous apporter leur assistance.

** Le site suivant peut fournir des solutions dans certains cas: https://www.nomoreransom.org/fr/index.4html*

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Tenez à jour l'antivirus et configurez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.

N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.

Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés (tous nos conseils pour gérer vos mots de passe).

Éteignez votre machine lorsque vous ne vous en servez pas.

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 :

- De tels procédés relèvent de l'**extorsion de fonds** et non de l'escroquerie. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou de ses fichiers – obligeant à une remise de fonds non volontaire. L'article 312-1 du code pénal dispose que : « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende* ».

- L'infraction d'**atteinte à un système de traitement automatisé de données (STAD)** peut aussi 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 sept ans d'emprisonnement et de 100 000 à 300 000 euros d'amende.
  – La tentative de ces infractions est punie des mêmes peines (article 323-7 du code pénal).
  – Lorsque ces infractions ont été commises en bande organisée (article 323-4-1 du code pénal), la peine peut être portée à dix ans d'emprisonnement et à 300 000 euros d'amende.

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

V230417

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

LE CYBERHARCÈLEMENT

Le cyberharcèlement consiste en des agissements malveillants répétés, dans un cadre public ou restreint, qui peuvent prendre différentes formes : intimidations, insultes, menaces, rumeurs, publication de photos ou vidéos compromettantes, etc. Ils peuvent être le fait d'une seule personne ou de plusieurs individus et se dérouler sur les réseaux sociaux, messageries, forums, blogs, etc. Les conséquences du cyberharcèlement peuvent être dramatiques pour les victimes : dépression, décrochage scolaire ou professionnel, troubles psychologiques ou émotionnels, violence, suicide, etc. Le cyberharcèlement est puni par la loi qui prévoit de lourdes sanctions contre ses auteurs.

BUT RECHERCHÉ

Le cyberharcèlement a pour objectif **l'atteinte et la dégradation des conditions de vie de la personne** qui en est victime.

SI VOUS ÊTES VICTIME

NE RÉPONDEZ PAS aux commentaires ou aux messages malveillants. Vous risqueriez d'empirer la situation en y montrant de l'intérêt.

PARLEZ-EN À UN TIERS DE CONFIANCE (parent, ami, enseignant…) car il est important de ne pas garder cela pour soi et ne pas rester isolé.

CONSERVEZ LES PREUVES (captures d'écran, messages et informations liées aux auteurs du cyberharcèlement) qui pourront vous servir pour signaler les faits.

VERROUILLEZ VOS COMPTES DE RÉSEAUX SOCIAUX en modifiant leurs paramètres de confidentialité pour en restreindre la visibilité et bloquez les auteurs des messages harcelants.

SIGNALEZ LES FAITS, CONTENUS OU COMPORTEMENTS ILLICITES AUPRÈS DES PLATEFORMES CONCERNÉES. Exemples de liens de signalement : Facebook, Twitter, LinkedIn, Instagram, Snapchat, TikTok, WhatsApp, YouTube.

DEMANDEZ À CE QUE LES CONTENUS HARCELANTS NE SOIENT PLUS RÉFÉRENCÉS par les moteurs de recherche : Bing, Qwant, Google, Yahoo, autres.

SIGNALEZ LES FAITS SUR LA PLATEFORME DÉDIÉE DU MINISTÈRE DE L'INTÉRIEUR en cas d'injure, de diffamation, de menace, d'incitation à la haine, à la discrimination, à la violence ou de mise en danger : Internet-signalement.gouv.fr.

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.

POUR PLUS DE CONSEILS ET D'ASSISTANCE, CONTACTEZ LE 3018 (service et appel gratuit), ligne nationale d'écoute et de conseil anonyme et confidentielle destinée aux personnes confrontées à des situations de cyberharcèlement et qui peut également intervenir auprès des réseaux sociaux pour faire supprimer des contenus préjudiciables.

MESURES PRÉVENTIVES

Vérifiez les paramètres de confidentialité de vos comptes en ligne qui sont souvent visibles par tous par défaut. Restreignez la visibilité de vos informations personnelles et de vos publications aux seules personnes que vous autorisez dans les paramètres de configuration de vos réseaux sociaux.

Ne renseignez votre profil qu'avec le minimum d'informations nécessaires. Mesurez l'utilité de communiquer toute information qui n'est pas obligatoire (date de naissance, lieu de résidence…).

Maîtrisez vos cercles de connaissances en distinguant les différents groupes ou personnes avec lesquels vous échangez et ce que vous partagez avec eux.

Faites attention à qui vous parlez et soyez vigilant face aux demandes de contact d'inconnus ou de personnes que vous ne connaissez pas vraiment ou encore celles dont l'identité a pu être usurpée.

Maîtrisez vos publications qui peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez.

Soyez vigilant lorsque vous communiquez des informations personnelles, intimes ou sensibles. De même s'il s'agit d'informations concernant d'autres personnes.

Faites preuve de discernement avec certaines informations relayées et vérifiez-les. Elles peuvent être partiellement ou totalement fausses, délibérément ou non, et avoir de graves conséquences pour vous ou les personnes qui en sont le sujet.

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 :

- Le cyberharcèlement est une forme de **harcèlement moral** défini par l'**article 222-33-2-2 du Code pénal**. Il désigne « le fait de harceler une personne par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale » [...] «lorsqu'ils ont été commis par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique ». Le cyberharcèlement est puni de deux ans d'emprisonnement et de 30 000 euros d'amende ; si la victime est mineur, les peines sont de trois ans d'emprisonnement et de 45 000 euros d'amende.
  À noter que l'infraction est constituée qu'elle soit le fait d'une seule ou d'un groupe de personnes, et, dans ce dernier cas, alors même que chacune de ces personnes n'a pas agi de façon répétée.

Selon la forme et les moyens des agissements de l'auteur ou des auteurs de cyberharcèlement :

- L'**injure ou la diffamation publique** (**article 32 de la Loi du 29 juillet 1881**) : délit passible d'une amende de 12 000 euros.

- L'**atteinte au droit à l'image** (**articles 226-1**, **226-2**, **226-2-1 du Code pénal**) : le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
  Lorsque les faits sont commis par le conjoint de la victime ou qu'ils présentent un caractère sexuel, les peines sont portées à deux ans d'emprisonnement et à 60 000 euros d'amende.

- La **diffusion de contenu à caractère pornographique d'un mineur** (**article 227-23 du Code pénal**) : délit passible de 5 ans d'emprisonnement et de 75 000 euros d'amende.

- L'**usurpation d'identité** (**article 226-4-1 du Code pénal**) : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 euros d'amende.
  Lorsque les faits sont commis par le conjoint de la victime, ils sont punis de deux ans d'emprisonnement et de 30 000 euros d'amende.

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

V230422