RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

KIT DE SENSIBILISATION
AUX RISQUES NUMÉRIQUES

DISPOSITIF NATIONAL D'ASSISTANCE
AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

www.cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

DANS CE KIT VOUS TROUVEREZ :

1/ Des fiches pour adopter les bonnes pratiques

- Les **mots de passe**
- La sécurité sur les **réseaux sociaux**
- La sécurité des **appareils mobiles**
- Les **sauvegardes**
- Les **mises à jour**
- La sécurité des **usages pro-perso**

2/ Des fiches pour comprendre les risques

- L'**hameçonnage**
- Les **rançongiciels**
- L'arnaque au **faux support technique**

3/ Et en complément...

- La présentation des **vidéos disponibles sur le site Internet**
- Un **quiz** pour tester vos connaissances
- Une **BD**
- Neuf **mémos**
- Une **affiche au format A2**

Ce contenu est le vôtre ! L'ensemble des contenus de ce kit de sensibilisation est diffusé sous licence ouverte Etalab 2.0. Vous êtes libres de :

- les **reproduire** et les **copier**
- les **adapter**, les **modifier**
- les **communiquer**, les **diffuser** et les **redistribuer**
- les **exploiter** en les incluant dans vos propres productions

sous réserve de mentionner la source de l'information (ici : Cybermalveillance.gouv.fr)
Voir www.etalab.gouv.fr/licence-ouverte-open-licence

RETROUVEZ LES CONTENUS DE PRÉVENTION ET D'ASSISTANCE AUX VICTIMES SUR :
WWW.CYBERMALVEILLANCE.GOUV.FR

ET SUR NOS RÉSEAUX SOCIAUX :

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

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

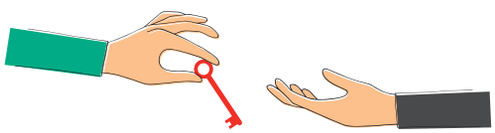
Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option . En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (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 :

Fédération Française de l'Assurance · kaspersky · LE GROUPE LA POSTE · 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

Licence Ouverte v2.0 (ETALAB)

Version 2.0

LA SÉCURITÉ **SUR LES RÉSEAUX SOCIAUX**

Les réseaux sociaux sont des outils de communication et d'information puissants et facilement accessibles. Aujourd'hui installés dans les usages personnels des internautes, mais aussi dans les usages professionnels des entreprises qui les utilisent comme vitrine de leur activité, ils n'échappent pas aux activités malveillantes. Escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… sont autant de dangers auxquels sont confrontés les utilisateurs de ces réseaux. **Voici 10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux.**

1 PROTÉGEZ L'ACCÈS À VOS COMPTES

Vos comptes de réseaux sociaux contiennent des informations personnelles sensibles (identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.), qui peuvent être convoitées par les cybercriminels. Pour vous assurer que personne ne puisse utiliser votre compte à votre insu ou usurper votre identité, protégez bien l'accès à votre compte en utilisant des mots de passe différents et suffisamment robustes. Si le service le propose, activez également la double authentification. En savoir plus sur les mots de passe.

2 VÉRIFIEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ

Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse e-mail…) et de vos publications sont souvent très ouverts. Vos données peuvent ainsi être partagées à tous les abonnés du réseau social. Il est généralement possible de restreindre cette visibilité en réglant la configuration de votre compte, afin de garder la maîtrise de ce que les autres utilisateurs voient de vos informations et de vos activités. Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous ne le sachiez.

3 MAÎTRISEZ VOS PUBLICATIONS

Les réseaux sociaux permettent de communiquer auprès d'une grande audience que vous ne pourrez jamais complètement maîtriser. Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez. Ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire. Faites également preuve de discernement lorsque vous évoquez votre travail car cela pourrait vous porter préjudice ainsi qu'à votre entreprise. Enfin, respectez évidemment la loi. *Voir encart.*

4 FAITES ATTENTION À QUI VOUS PARLEZ

Les cybercriminels utilisent notamment les réseaux sociaux pour commettre des escroqueries et voler des informations personnelles ou professionnelles. Soyez vigilants, car à leur insu, vos « amis » ou contacts peuvent également vous envoyer ou partager des contenus malveillants, surtout s'ils se sont fait pirater leur compte sans le savoir. Quelques conseils supplémentaires : n'envoyez jamais d'argent à quelqu'un sans avoir vérifié son identité au préalable, n'envoyez jamais de photos ou vidéos intimes à des contacts virtuels qui pourraient en profiter pour vous faire chanter et méfiez-vous des jeux concours, des gains inattendus, ou des « super affaires », qui peuvent cacher des escroqueries (hameçonnage).

5 CONTRÔLEZ LES APPLICATIONS TIERCES

Certaines applications proposent d'interagir avec votre compte de réseau social. Il peut s'agir de jeux, de quiz, de programmes alternatifs pour gérer votre compte. Ces applications demandent des autorisations qu'il faut examiner avec attention car une fois données, ces applications peuvent avoir accès à vos informations personnelles, vos contacts, vos publications, vos messages privés… Ne les installez que depuis les sites ou magasins d'applications officiels, sinon vous risquez de donner l'accès à votre compte à un programme infecté par un virus. Si l'application vous semble trop intrusive dans les autorisations qu'elle demande, ne l'installez pas. Enfin, pensez à désinstaller ces applications ou en révoquer les droits si vous ne vous en servez plus.

RESPECTEZ LA LOI

Internet n'est pas une zone de non-droit et l'anonymat n'y est pas absolu : les propos incitant à la haine ou à la violence, la pédophilie, le cyberharcèlement, l'atteinte au droit à l'image ou au droit d'auteur… sont punis par la loi.

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

LE SAVIEZ-VOUS ?

En vertu de la loi n° 2018-493 du 20 juin 2018 – Article 20, **un mineur peut consentir seul à un traitement de ses données à caractère personnel à partir de quinze ans.** Avant cet âge, le consentement du titulaire de l'autorité parentale est requis.

6 ÉVITEZ LES ORDINATEURS ET LES RÉSEAUX WIFI PUBLICS

Utiliser un ordinateur en libre accès ou un réseau WiFi public est risqué car ils peuvent être piégés ou contrôlés par un cybercriminel. Lorsque vous vous connectez à votre compte de réseau social par ce moyen, vous pouvez vous faire voler votre mot de passe et donc vous faire pirater votre compte. Évitez dans la mesure du possible de renseigner des informations sensibles ou personnelles sur un matériel ou un réseau qui n'est pas le vôtre. Si vous y êtes contraint malgré tout, pensez à bien vous déconnecter de votre compte après utilisation pour empêcher que quelqu'un puisse y accéder après vous.

7 VÉRIFIEZ RÉGULIÈREMENT LES CONNEXIONS À VOTRE COMPTE

La plupart des réseaux sociaux offrent des fonctionnalités qui vous permettent de voir les connexions ou sessions actives sur votre compte depuis les différents appareils que vous utilisez pour y accéder. Consultez régulièrement ces informations. Si vous détectez une session ou une connexion inconnue ou que vous n'utilisez plus, déconnectez-la. Au moindre doute, considérez qu'il peut s'agir d'un piratage et changez immédiatement votre mot de passe (voir conseil n° 1).

8 FAITES PREUVE DE DISCERNEMENT AVEC LES INFORMATIONS PUBLIÉES

Les réseaux sociaux sont de formidables et rapides outils d'information, mais n'importe qui peut aussi y publier n'importe quelle information, sans aucune vérification. Certaines informations peuvent donc être partiellement ou totalement fausses, parfois délibérément. Avec la puissance des réseaux sociaux, ces fausses informations (appelées *fake news* en anglais) peuvent avoir de graves conséquences sur les personnes qui en sont victimes. Aussi, avant de considérer ou relayer une information, efforcez-vous d'en vérifier la véracité.

9 UTILISEZ EN CONSCIENCE L'AUTHENTIFICATION AVEC VOTRE COMPTE DE RÉSEAU SOCIAL SUR D'AUTRES SITES

Pour s'y connecter, certains sites Internet vous proposent d'utiliser votre compte de réseau social. Cette fonctionnalité peut sembler pratique car elle évite de créer un compte et un mot de passe supplémentaires, mais cela signifie que vous allez communiquer au réseau social des informations sur ce que vous faites sur le site concerné, et à l'inverse que vous allez peut-être donner au site des droits d'accès sur votre compte de réseau social. De plus, si votre compte de réseau social était un jour piraté, le cybercriminel pourrait automatiquement accéder à tous ces sites en usurpant votre identité. Aussi, avant d'utiliser cette fonctionnalité, ayez bien conscience des risques et vérifiez attentivement les autorisations que vous délivrez.

10 SUPPRIMEZ VOTRE COMPTE SI VOUS NE L'UTILISEZ PLUS

Pour éviter que vos informations ne soient récupérées par des tiers ou que votre compte ne soit utilisé à votre insu, notamment pour usurper votre identité, supprimez-le si vous ne l'utilisez plus.

QUE FAIRE EN CAS DE PROBLÈME ?

- **Réagir en cas de piratage de votre compte de réseau social** – Les conseils de la CNIL : www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux
- **Demander la suppression d'une publication gênante ou compromettante sur les réseaux sociaux** – Les conseils de la CNIL : www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer
- **Signaler une situation de cyber harcèlement** : contacter Net Écoute gratuitement au 0800 200 000 et sur www.netecoute.fr
- **Signaler un contenu illicite sur les réseaux sociaux** – Internet Signalement/Pharos (ministère de l'Intérieur) : www.internet-signalement.gouv.fr

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :
CO vea · e-Enfance association reconnue d'utilité publique · eset · Microsoft

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

Licence Ouverte v2.0 (ETALAB)

Version 2.0

LA SÉCURITÉ **DES APPAREILS MOBILES**

Les téléphones mobiles intelligents (smartphones) et tablettes informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel. Leurs capacités ne cessent de croître et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs. Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder. Ils sont plus faciles à perdre ou à se faire voler. Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires. **Voici 10 bonnes pratiques à adopter pour la sécurité de vos appareils mobiles.**

1 METTEZ EN PLACE LES CODES D'ACCÈS

Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires (voir encadré) empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations. Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, par exemple). Activez également le verrouillage automatique de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.

CODE D'ACCÈS ET CODE PIN, **DEUX PROTECTIONS COMPLÉMENTAIRES**

Mot de passe, signe, combinaison de touches ou biométrie : **le code de verrouillage empêche de pouvoir se servir de l'appareil si on ne le connaît pas.**

Composé de 4 chiffres, **le code PIN bloque quant à lui l'accès à votre carte SIM** et empêche donc de pouvoir s'en servir dans un autre appareil si on ne le connaît pas.

2 CHIFFREZ LES DONNÉES DE L'APPAREIL

En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation. Si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

3 APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ

Qu'il s'agisse du système d'exploitation (Android, iOS) ou des applications qui sont sur votre appareil, installez sans tarder les mises à jour dès qu'elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

4 FAITES DES SAUVEGARDES

Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement car vous pourriez tout perdre en cas de casse, de perte ou de vol.

5 UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)… Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.ous en servez plus.

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

6 N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées. Méfiez-vous des sites « parallèles », qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

7 CONTRÔLEZ LES AUTORISATIONS DE VOS APPLICATIONS

Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer. Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos mots de passe, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

CHAMBRE DE COMMERCE ET D'INDUSTRIE · CLUSIF · e-Enfance

8 NE LAISSEZ PAS VOTRE APPAREIL SANS SURVEILLANCE

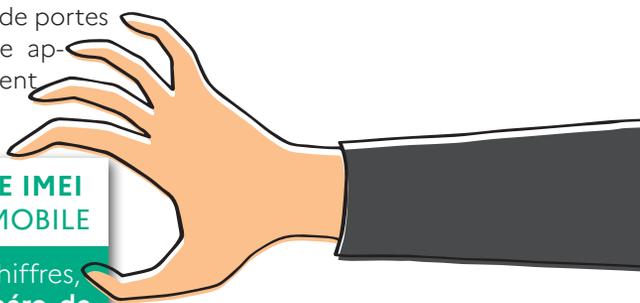
Une personne malintentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil. Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

9 ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutilement.

10 NE STOCKEZ PAS D'INFORMATIONS CONFIDENTIELLES SANS PROTECTIONS

Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.



CONSERVEZ LE CODE IMEI DE VOTRE APPAREIL MOBILE

Composé de 15 à 17 chiffres, le code IMEI est **le numéro de série de votre appareil mobile**. Il est généralement inscrit sur sa boîte d'emballage. En cas de perte ou de vol, ce code peut permettre de bloquer l'usage du téléphone sur tous les réseaux.

Notez-le soigneusement et si vous l'avez égaré **vous pouvez le récupérer en tapant *#06# sur votre clavier.**

POUR ALLER PLUS LOIN

- **Par la CNIL :** Comment sécuriser au maximum l'accès à votre smartphone ?
- **Par l'ANSSI :** Sécuriser son ordiphone

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

Licence Ouverte v2.0 (ETALAB)

Version 2.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES SAUVEGARDES

Dans nos usages personnels ou professionnels, nous utilisons de nombreux appareils numériques pour créer et stocker des informations. Ces appareils peuvent cependant s'endommager ou être endommagés, entraînant une perte, parfois irréversible, de vos données. Afin de prévenir un tel risque, il est fortement conseillé d'en faire des copies pour préserver vos données à long terme. **Voici 10 bonnes pratiques à adopter pour gérer efficacement vos sauvegardes.**

1 EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES DE VOS DONNÉES

En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports. Il peut s'agir de données auxquelles vous accordez une importance particulière ou considérées comme essentielles dans le cadre de vos activités personnelles ou professionnelles (photos, vidéos, documents personnels ou de travail, etc.). Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données.

2 IDENTIFIEZ LES APPAREILS ET SUPPORTS QUI CONTIENNENT DES DONNÉES

Dans notre vie quotidienne, nous utilisons un nombre croissant d'appareils et de supports qui enregistrent et stockent nos fichiers et nos données : ordinateurs, serveurs, tablettes, téléphones mobiles (smartphone), disques durs, clés USB, etc. Prenez le temps de les identifier.

3 DÉTERMINEZ QUELLES DONNÉES DOIVENT ÊTRE SAUVEGARDÉES

Il n'est pas toujours possible ni nécessaire de sauvegarder la totalité de ses données. Sélectionnez donc les données à protéger, notamment celles qui sont stockées sur vos appareils (dans le disque dur de votre ordinateur ou dans la mémoire de votre téléphone mobile). Pour savoir si des données doivent être sauvegardées ou non, posez-vous les questions suivantes : « quelles données ne peuvent pas être récupérées par ailleurs en cas de perte ? », « quelles données je consulte régulièrement ou celles qui me sont le plus souvent demandées ? ».

4 CHOISISSEZ UNE SOLUTION DE SAUVEGARDE ADAPTÉE À VOS BESOINS

Il existe des solutions gratuites ou payantes qui répondent à différents besoins. Identifiez-les et déterminez quelles sont les fonctionnalités attendues, l'espace de stockage requis et la facilité d'utilisation de la solution. Sachez qu'il est également possible de réaliser une sauvegarde manuelle de vos fichiers en les copiant sur un disque dur externe, une clé USB, etc. Enfin, la plupart des systèmes d'exploitation proposent des fonctionnalités de sauvegarde sur le support de votre choix ou sur un service en ligne. Si vous avez des besoins particuliers, renseignez-vous auprès de professionnels ou de sites Internet spécialisés.

5 PLANIFIEZ VOS SAUVEGARDES

Lorsqu'un fichier régulièrement mis à jour est perdu ou supprimé par erreur, sa restauration dans sa version la plus récente est nécessaire. La plupart des solutions de sauvegarde intègrent une fonctionnalité permettant de planifier la sauvegarde à échéance régulière. Vérifiez qu'elle est bien activée et que la fréquence de vos sauvegardes est adaptée à vos besoins. Si vous n'utilisez pas de solution dédiée, réalisez des sauvegardes manuelles régulièrement.

DIFFÉRENTS TYPES DE SAUVEGARDES

- **La sauvegarde complète** est une copie de la totalité de vos données.
- **La sauvegarde incrémentale ou incrémentielle** ne copie que les fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde.
- **La sauvegarde différentielle** est une copie complète des fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde complète.

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

ET LE CLOUD, DANS TOUT CELA ?

Des services en ligne, souvent appelés « Cloud », offrent des fonctionnalités de sauvegarde de données. Il existe des solutions gratuites ou payantes en fonction de la capacité de stockage souhaitée. Les fournisseurs d'accès Internet (FAI) et des entreprises spécialisées proposent ce type de service.

6 DÉCONNECTEZ VOTRE SUPPORT DE SAUVEGARDE APRÈS UTILISATION

Si vous êtes victime d'un virus comme un rançongiciel et que votre sauvegarde est connectée à votre ordinateur ou au réseau de votre entreprise, elle peut également être affectée par le programme malveillant qui pourrait la détruire. Déconnectez votre support de sauvegarde de votre ordinateur ou de votre réseau informatique ou mettez-le hors ligne lorsque vous ne l'utilisez plus.

7 PROTÉGEZ VOS SAUVEGARDES

Les risques de perte, de vol, de panne, de piratage ou de destruction peuvent également affecter vos sauvegardes. Protégez-les au même titre que vos données originales en effectuant, par exemple, plusieurs sauvegardes de vos données sur différents supports. Conservez également une sauvegarde dans un lieu différent de celui où sont stockées les données originales pour vous prémunir en cas de sinistre. Si vous estimez que vos données sont suffisamment sensibles pour les chiffrer ou en limiter l'accès, ou si un règlement vous y oblige, faites-en de même avec vos sauvegardes.

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

CDSE Club des Directeurs de Sécurité des Entreprises
LE GROUPE LA POSTE

8 TESTEZ VOS SAUVEGARDES

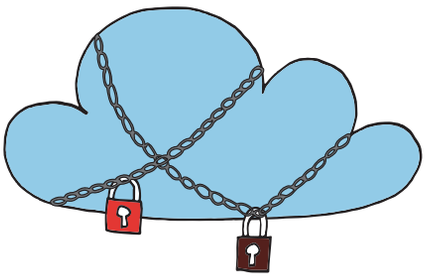
Parfois, le processus de sauvegarde ne s'effectue pas correctement. Aussi, assurez-vous régulièrement que votre sauvegarde fonctionne, par exemple, en la copiant dans le système original.

9 VÉRIFIEZ LE SUPPORT DE SAUVEGARDE

Tout comme les supports qui permettent de stocker les données originales, les supports sur lesquels sont réalisées les sauvegardes peuvent être endommagés. Vérifiez leur état, de manière à prévenir toute défaillance ou panne. Soyez également vigilant sur la durée de vie de votre support car certains conservent les données sur une durée plus ou moins longue. Par exemple, la durée de vie moyenne d'un DVD gravé est de 10 à 15 ans.

10 SAUVEGARDEZ LES LOGICIELS INDISPENSABLES À L'EXPLOITATION DE VOS DONNÉES Pro

La défaillance d'un appareil entraîne non seulement la perte des données produites par son utilisateur mais également du système d'exploitation de l'appareil comme MS Windows, iOS, Android, et des logiciels qui y sont installés. Si les données sauvegardées sont dépendantes d'un système d'exploitation, d'un logiciel ou d'une configuration particulière, sauvegardez vos données ainsi que celles nécessaires à leur exploitation. Les systèmes d'exploitation récents proposent des fonctionnalités de sauvegarde du système qui permettent de le restaurer. Reportez-vous à sa documentation pour plus d'information.



LÉGISLATION

Professionnels, associations, collectivités : tenez compte du cadre juridique applicable.

Quelle que que soit leur nature, vos sauvegardes sont soumises à de nombreux régimes juridiques au même titre que vos données originales. S'agissant de données personnelles, votre responsabilité civile ou pénale peut être engagée en cas de manquement avéré. De même, le Règlement Général sur la Protection des Données (**RGPD**) et la Loi Informatique et Libertés sont applicables.

Quelques textes :
- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés - Article 34
- **Article 226-17 du Code Pénal** (relatif au traitement et à la protection des données personnelles)
- **Article 1242 du Code Civil** (relatif à la responsabilité civile liée à un dommage causé à autrui)

Pro = destiné principalement aux professionnels

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

Licence Ouverte v2.0 (ETALAB)

Version 2.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES MISES À JOUR

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (*patch* en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger.
Voici 10 bonnes pratiques à adopter pour vos mises à jour.

1 PENSEZ À METTRE À JOUR SANS TARDER L'ENSEMBLE DE VOS APPAREILS ET LOGICIELS

Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés… nous utilisons un grand nombre d'appareils et de logiciels. Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique. Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

2 TÉLÉCHARGEZ LES MISES À JOUR UNIQUEMENT DEPUIS LES SITES OFFICIELS

Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jour que vous allez installer ne sont pas infectées par un virus. À l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases précochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

3 IDENTIFIEZ L'ENSEMBLE DES APPAREILS ET LOGICIELS UTILISÉS

Il est conseillé d'identifier vos appareils, matériels et logiciels afin de les mettre à jour. Certains fournisseurs d'accès Internet (FAI) proposent une application d'inventaire qui permet de lister les appareils connectés à votre réseau informatique professionnel ou domestique. Si vous faites l'acquisition d'un nouvel appareil, remettez ses paramètres par défaut avant de l'utiliser en le réinitialisant et installez ensuite les différentes mises à jour proposées sur les sites du fabriquant ou des éditeurs des applications installées.

4 ACTIVEZ L'OPTION DE TÉLÉCHARGEMENT ET D'INSTALLATION AUTOMATIQUE DES MISES À JOUR

Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement. Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur. Assurez-vous également que la mise à jour fonctionne par une vérification manuelle, au besoin.

DIFFÉRENTS TYPES DE MISES À JOUR

- **Les mises à jour importantes ou critiques** corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement.
- **Les mises à jour de version** apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant.

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

QUELQUES EXEMPLES DE FAILLES DE SÉCURITÉ

• **Aux États-Unis,** des cybercriminels ont réussi à dérober des données confidentielles **d'un casino grâce au thermomètre connecté présent dans un aquarium** de l'établissement.
• **En France,** la **trottinette** électrique connaît un succès grandissant. **Une faille de sécurité sur certains modèles** a été découverte. Elle permettait d'exécuter certaines commandes sans avoir besoin du mot de passe comme **les déverrouiller, contrôler l'accélération ou le freinage.** Une mise à jour a été publiée pour corriger cette faille.

5 DÉFINISSEZ LES RÈGLES DE RÉALISATION DES MISES À JOUR

Pro

Pour assurer votre sécurité numérique, la définition de certaines règles peut faciliter l'opération de mise à jour, notamment en entreprise. Il s'agit par exemple de spécifier la façon de réaliser l'inventaire des appareils et logiciels utilisés, de savoir où et comment rechercher les mises à jour, comment et qui procède à la mise à jour ou encore à quel moment réaliser cette opération.

6 PLANIFIEZ LES MISES À JOUR LORS DE PÉRIODES D'INACTIVITÉ

Lorsqu'ils interrompent une activité personnelle ou professionnelle (visionnage d'une vidéo, rédaction d'un courriel…), les messages indiquant la disponibilité d'une mise à jour sont souvent ignorés car le processus de mise à jour peut être ressenti comme une contrainte. En effet, la mise à jour peut prendre du temps, allant de quelques secondes à plusieurs minutes ou heures, selon les cas. Aussi, profitez de périodes d'inactivité pour effectuer vos mises (déjeuner, réunion, de nuit…).

7 MÉFIEZ-VOUS DES FAUSSES MISES À JOUR SUR INTERNET

En naviguant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran : fausses publicités sur des sites Internet ou fenêtres (*pop-up* en anglais) malveillantes. Restez extrêmement vigilant car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

8 INFORMEZ-VOUS SUR LA PUBLICATION RÉGULIÈRE DES MISES À JOUR DE L'ÉDITEUR

Pro

L'utilisation d'un appareil ou d'un logiciel pas à jour augmente les risques d'attaques informatiques. Si les mises à jour ne sont plus proposées, ils sont plus vulnérables. Aussi, avant l'acquisition d'un nouveau matériel ou logiciel, vérifiez la publication régulière des mises à jour de l'éditeur ou du fabricant, ainsi que la date de fin de leur mise à disposition. Lorsqu'une solution arrive en fin de vie et que des mises à jour ne sont plus proposées, identifiez les délais et les ressources nécessaires pour migrer vers de nouveaux outils afin de rester protégé.

9 TESTEZ LES MISES À JOUR LORSQUE CELA EST POSSIBLE ET FAITES DES SAUVEGARDES

Pro

Il arrive que la mise à jour d'un équipement ou d'un logiciel entraîne des conséquences inattendues, comme de rendre incompatible la solution qui vient d'être mise à jour avec un autre équipement ou logiciel. Il convient donc de tester les mises à jour lorsque cela est possible. Par ailleurs, n'hésitez pas à réaliser une sauvegarde de vos données et de vos logiciels avant une opération de mise à jour pour pouvoir revenir en arrière si nécessaire.

10 PROTÉGEZ AUTREMENT LES APPAREILS QUI NE PEUVENT PAS ÊTRE MIS À JOUR

Pro

Dans certains cas, des appareils peuvent ne pas être mis à jour pour diverses raisons, comme leur ancienneté, la perte d'une garantie ou d'un agrément. Il est, par conséquent, nécessaire de protéger ce dispositif autrement, par exemple en ne le connectant pas à Internet, en le séparant du reste du réseau informatique ou encore, en désactivant les services vulnérables.

BON À SAVOIR

En entreprise, s'il existe un service informatique, il est généralement chargé de la mise à jour des appareils et des logiciels. **Dans le cas contraire, ce sont les collaborateurs qui effectuent cette opération, sous l'autorité du chef d'entreprise.**

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :
CESIN · CLUSIF · Fédération Française de l'Assurance · paloalto NETWORKS · STORMSHIELD

Pro destiné principalement aux professionnels

Licence Ouverte v2.0 (ETALAB)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

ADOPTER LES BONNES PRATIQUES

LA SÉCURITÉ **DES USAGES PRO-PERSO**

La transformation numérique modifie en profondeur les usages et les comportements. Être connecté est devenu le quotidien. Le développement des technologies mobiles (PC portables, tablettes, smartphones) offre désormais la possibilité d'accéder, depuis presque n'importe où, à ses informations personnelles mais aussi à son système informatique professionnel : la frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse. Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant votre entreprise* ou votre organisation, que votre espace de vie privée. **Voici 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-perso.**

1 UTILISEZ DES MOTS DE PASSE DIFFÉRENTS POUR TOUS LES SERVICES PROFESSIONNELS ET PERSONNELS AUXQUELS VOUS ACCÉDEZ

Si vous ne le faites pas et qu'un des services auquel vous accédez se fait pirater, le vol de votre mot de passe permettra à une personne malveillante d'accéder à tous vos autres services y compris les plus critiques (banque, messagerie, sites marchands, réseaux sociaux…). Si vous utilisez ce même mot de passe pour accéder au système informatique de votre entreprise, c'est elle que vous mettez aussi en péril, car un cybercriminel pourrait utiliser vos identifiants de connexion pour voler ou détruire des informations.

2 NE MÉLANGEZ PAS VOTRE MESSAGERIE PROFESSIONNELLE ET PERSONNELLE

Ce serait, en effet, le meilleur moyen de ne plus s'y retrouver et de commettre des erreurs, notamment des erreurs de destinataires. Celles-ci pourraient avoir pour conséquences de voir des informations confidentielles de votre entreprise vous échapper vers des contacts personnels qui pourraient en faire un mauvais usage, ou à l'inverse de voir un message trop personnel circuler dans votre environnement professionnel alors que vous ne le souhaiteriez pas. Enfin, comme votre messagerie personnelle est généralement bien moins sécurisée que votre messagerie professionnelle, vous faire pirater votre compte pourrait mettre en danger votre entreprise si un cybercriminel accédait à des messages professionnels confidentiels que vous auriez gardés dans votre messagerie personnelle.

3 AYEZ UNE UTILISATION RESPONSABLE D'INTERNET AU TRAVAIL

Si l'utilisation d'une connexion Internet professionnelle à des fins personnelles est tolérée, il est important d'avoir à l'esprit que votre utilisation peut mettre en cause votre entreprise qui pourra se retourner contre vous si vous commettiez des actes répréhensibles comme du téléchargement illégal, de l'atteinte au droit d'auteur ou si vous publiez des propos qui pourraient être condamnables. De plus, vous devez avoir à l'esprit que votre entreprise est en droit de contrôler votre utilisation de la connexion qu'elle met à votre disposition. N'utilisez donc pas votre connexion professionnelle pour des choses qui n'ont, selon vous, pas à être connues de votre entreprise.

4 MAÎTRISEZ VOS PROPOS SUR LES RÉSEAUX SOCIAUX

Quand vous parlez de votre travail ou de la vie de votre entreprise (ambiance, nouveaux projets…) sur les réseaux sociaux, même si vos propos ne sont pas négatifs, vous ne contrôlez pas vos lecteurs : la rediffusion ou l'interprétation qu'ils peuvent faire de vos informations pourraient nuire à votre entreprise. À l'inverse, et pour les mêmes raisons, vous n'avez pas forcément envie que certains propos que vous pouvez tenir sur les réseaux sociaux et qui concernent votre vie privée puissent être connus de votre entreprise. Sur les réseaux sociaux, verrouillez votre profil pour que tout ne soit pas public et avant de poster, demandez-vous toujours si ce que vous communiquez ne pourra pas vous porter préjudice, ou à votre entreprise, si d'aventure vos propos ou messages étaient relayés par une personne malintentionnée.

*Le terme « entreprise » employé dans ce document regroupera toutes les organisations professionnelles qu'elles soient à caractère privé, public ou associatif.

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

5 N'UTILISEZ PAS DE SERVICES DE STOCKAGE EN LIGNE PERSONNEL À DES FINS PROFESSIONNELLES

Ou du moins pas sans l'autorisation de votre employeur et sans avoir pris les mesures de sécurité qui s'imposent. Ces services de stockage en ligne d'informations (Cloud en anglais) généralement gratuits pour les particuliers sont certes pratiques, mais d'un niveau de sécurité qui ne se prête pas forcément aux exigences des entreprises pour protéger leurs informations. Ils ne sont pas conçus pour cela. Pour les besoins des entreprises, il existe des solutions professionnelles et sécurisées. L'utilisation d'un service de stockage en ligne personnel pour des usages professionnels pourrait mettre en danger votre entreprise si votre compte d'accès à ce service était piraté alors qu'il contenait des informations confidentielles.

6 FAITES LES MISES À JOUR DE SÉCURITÉ DE VOS ÉQUIPEMENTS

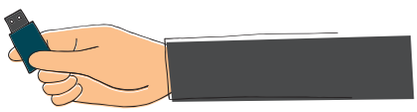
Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, il est important d'installer sans tarder les mises à jour dès qu'elles sont publiées. Elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations ou à celles de votre entreprise.

7 UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, utilisez une solution antivirus et tenez-la à jour. Même si aucune solution n'est totalement infaillible, de nombreux produits peuvent vous aider à vous protéger des différentes attaques que peuvent subir vos équipements comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)... Si un cybercriminel prenait le contrôle de vos équipements personnels, il pourrait accéder à toutes vos informations, mais aussi au réseau de votre entreprise si vous vous y connectez avec ce matériel.

8 N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Que ce soit pour vos usages personnels ou professionnels si cela relève de votre responsabilité, et même s'ils ne sont pas infaillibles, seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées par un virus qui permettrait à un cybercriminel de prendre le contrôle de votre équipement. Méfiez-vous des sites « parallèles » qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, ne l'installez pas et choisissez-en une autre.



9 MÉFIEZ-VOUS DES SUPPORTS USB

Vous trouvez ou on vous offre une clé USB (ou tout autre support à connecter). Partez du principe qu'elle est piégée et que même les plus grands spécialistes pourraient avoir du mal à s'en apercevoir. Ne la branchez jamais sur vos moyens informatiques personnels et encore moins sur vos moyens informatiques professionnels au risque de les compromettre en ouvrant un accès à un cybercriminel. Utilisez une clé USB pour vos usages personnels et une autre pour vos usages professionnels afin d'éviter que la compromission de l'une ne puisse infecter l'autre.

10 ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU INCONNUS

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et ainsi récupérer au passage vos comptes d'accès et vos mots de passe personnels ou professionnels, vos messages, vos documents ou même vos données de carte bancaire... afin d'en faire un usage délictueux. Depuis un réseau Wi-Fi public ou inconnu, n'échangez jamais d'informations confidentielles.

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :
covea · cpme CONFÉDÉRATION DES PME · eset · Fédération Française de l'Assurance · Microsoft

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

Licence Ouverte v2.0 (ETALAB)

Version 2.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

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 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.

- 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.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

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.

COMPRENDRE LES RISQUES

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 (notre fiche dédiée aux mots de passe sur www.cybermalveillance.gouv.fr).

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

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)** pourra aussi être retenue (article 323-1 du code pénal) soit du fait d'une modification frauduleuse de données soit d'une entrave au bon fonctionnement d'un STAD.

  La loi du 24 juillet 2015 relative au renseignement a doublé les peines d'amende encourues de 75 000 euros à 150 000 euros.

  Par ailleurs, depuis 2013, la détention ou la cession d'un rançongiciel, sans motif légitime, est passible des mêmes peines.

  Dans le cadre des atteintes aux STAD, la **circonstance aggravante de bande organisée** est très souvent retenue. En effet, la commission de ces infractions requiert en principe la mise en œuvre de différentes compétences et donc l'intervention de plusieurs personnes pour la conception, injection du virus, expédition du mail infecté, collecte de la rançon.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

COMPRENDRE LES RISQUES

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

L'arnaque au faux support technique (***Tech support scam*** en anglais) consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

BUT RECHERCHÉ

Soutirer de l'argent à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

SI VOUS ÊTES VICTIME

NE RÉPONDEZ PAS AUX SOLLICITATIONS et n'appelez jamais le numéro indiqué.

CONSERVEZ TOUTES LES PREUVES. Photographiez votre écran au besoin.

S'il semble « bloqué », **REDÉMARREZ VOTRE APPAREIL**. Cela peut suffire à régler le problème.

Si votre navigateur reste incontrôlable, **PURGEZ LE CACHE, SUPPRIMEZ LES COOKIES, RÉINITIALISEZ LES PARAMÈTRES PAR DÉFAUT** et si cela ne suffit pas, supprimez et recréez votre profil.

DÉSINSTALLEZ TOUTE NOUVELLE APPLICATION SUSPECTE présente sur votre appareil.

FAITES UNE ANALYSE ANTIVIRALE COMPLÈTE de votre appareil.

Si un faux technicien a pris le contrôle de votre machine, **DÉSINSTALLEZ LE PROGRAMME DE GESTION À DISTANCE ET CHANGEZ TOUS VOS MOTS DE PASSE**. En cas de doute ou si vous n'arrivez pas à reprendre le contrôle de votre appareil, vous pouvez faire appel à un professionnel référencé sur www.cybermalveillance.gouv.fr.

Si vous avez fourni vos coordonnées de carte bancaire, **FAITES OPPOSITION SANS DÉLAI**. Si un paiement est débité sur votre compte, **EXIGEZ LE REMBOURSEMENT** en indiquant que vous déposez plainte.

SIGNALEZ LES FAITS sur la plateforme Internet-signalement.gouv.fr du ministère de l'Intérieur.

En fonction du préjudice subi, **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.

MESURES PRÉVENTIVES

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

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

Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.

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

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

N'ouvrez pas les courriels, 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 la structure du message est inhabituelle ou vide.

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

Aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.

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

FAUX SUPPORT TECHNIQUE

LES **INFRACTIONS**

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

- L'incrimination principale qui peut être retenue est 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* ». L'escroquerie est passible de cinq ans d'emprisonnement et de 375 000 euros d'amende.

- Si la victime est menacée de suppression de ses fichiers ou en est victime, de tels procédés relèvent de l'extorsion de fonds. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou la destruction de 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.

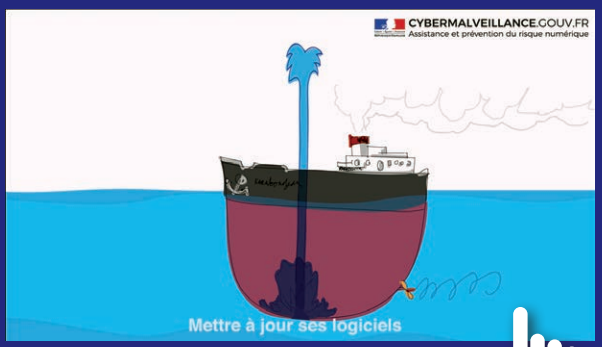
- L'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra également être retenue. Les articles 323-1 à 323-7 du code pénal disposent que : « *le fait d'accéder ou de se maintenir frauduleusement* » *dans un STAD,* « *la suppression ou la modification de données contenues dans le système* », ou l'« *altération du fonctionnement de ce système* » sont passibles de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

8 VIDÉOS À TÉLÉCHARGER

1 LES MISES À JOUR



2 LES SAUVEGARDES

3 LES RANÇONGICIELS

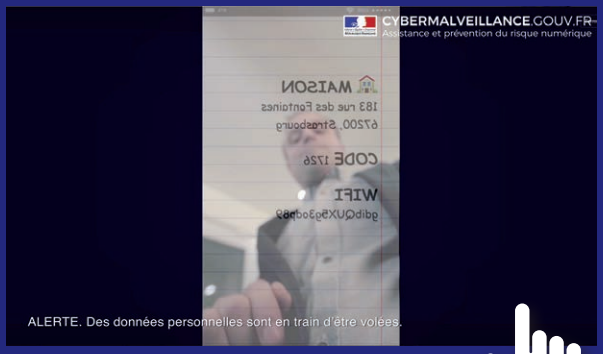
4 L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

RETROUVEZ CES VIDÉOS SUR :
www.cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

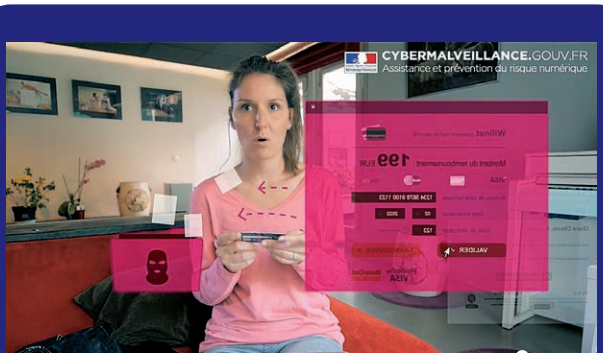
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

5 LA SÉCURITÉ DES APPAREILS MOBILES

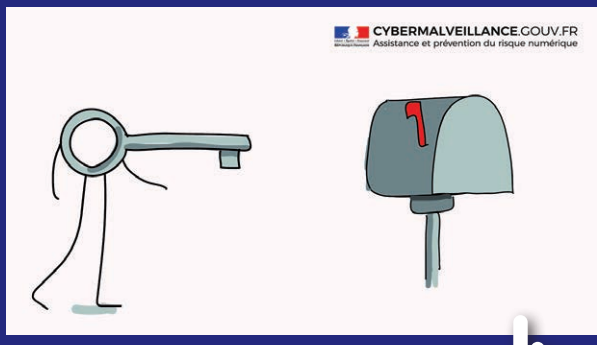


6 LA SÉCURITÉ DES USAGES PRO-PERSO

7 L'HAMEÇONNAGE



8 LES MOTS DE PASSE



RETROUVEZ CES VIDÉOS SUR :
www.cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

TESTEZ VOS CONNAISSANCES

GÉRER SES MOTS DE PASSE

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer la sécurité de vos mots de passe ?

- ☐ **A** Les noter sur un post-it pour s'en souvenir
- ☐ **B** Choisir un mot de passe suffisamment complexe
- ☐ **C** Les confier à un tiers en cas de besoin
- ☐ **D** Utiliser un mot de passe différent pour chaque accès

2/ Vrai ou Faux

J'ai un mot de passe très sécurisé. Je peux donc l'utiliser sur tous mes comptes et services.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

Un mot de passe sécurisé :

- ☐ **A** est facile (suite logique, le prénom de mes enfants, ma date de naissance, etc.)
- ☐ **B** comporte 12 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux
- ☐ **C** suit un moyen mnémotechnique

4/ Reliez les situations à leurs solutions

Je ne me souviens jamais de mes mots de passe	**A** ☐	☐ **1**	Je n'enregistre pas les mots de passe et me déconnecte après utilisation
Je soupçonne qu'un de mes comptes ait été piraté	**B** ☐	☐ **2**	Je fais confiance à Keepass, mon gestionnaire de mots de passe
Je travaille sur un ordinateur à la bibliothèque	**C** ☐	☐ **3**	Je change immédiatement de mot de passe

RÉPONSES

1/B et D – Vos mots de passe sont la porte d'entrée de vos appareils numériques et de l'accès à vos comptes, qui peuvent contenir des données sensibles. Protégez vos accès en utilisant un mot de passe complexe et unique pour chaque accès.
2/FAUX – Il vaut mieux utiliser un mot de passe différent et complexe pour chaque accès ou service. En effet, en cas de perte ou de vol d'un de vos mots de passe, vous limitez les risques d'accès frauduleux au seul compte lié à ce mot de passe.
3/A – Un mot de passe trop simple ou facile à deviner n'offre pas un niveau de sécurité suffisant, ce qui pourrait faciliter la tâche des cybercriminels.
4/A – 2 B – 3 C – 1

HAMEÇONNAGE

1/ Bonnes pratiques

Sur mon compte bancaire, je découvre un débit que je ne reconnais pas. Je crains d'être victime d'un «hameçonnage» lié à un message douteux auquel j'ai répondu il y a deux semaines. Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre ?

- ☐ **A** Je vérifie auprès de ma banque l'origine du débit et fais opposition à celui-ci
- ☐ **B** Je laisse passer quelques jours pour m'assurer qu'il s'agit vraiment d'un débit frauduleux
- ☐ **C** Je dépose plainte au commissariat de police ou à la gendarmerie la plus proche

2/ Vrai ou Faux

Il est inutile de déposer plainte pour un message d'hameçonnage auquel j'ai répondu.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

Comment se prémunir de l'hameçonnage ?

- ☐ **A** Si j'ai un doute concernant un message électronique ou un appel, je contacte directement l'organisme concerné pour en confirmer l'authenticité
- ☐ **B** Je vérifie qu'il y ait bien un logo officiel dans le message reçu
- ☐ **C** Avant de cliquer sur un lien douteux, je positionne le curseur de ma souris sur le lien sans cliquer pour vérifier l'adresse vers laquelle il pointe
- ☐ **D** Je ne communique jamais d'informations sensibles par téléphone ou messagerie électronique

4/ Reliez les situations à leurs solutions

Mon adresse de messagerie a été usurpée	**A** ☐	☐ **1**	Je fais opposition auprès de ma banque et je dépose plainte
J'ai malencontreusement communiqué mon numéro de carte bancaire	**B** ☐	☐ **2**	Je la signale à Phishing Intiative
J'identifie une adresse de site d'hameçonnage	**C** ☐	☐ **3**	Je change immédiatement de mot de passe

RÉPONSES

1/A et C
2/FAUX – Si vous avez malencontreusement communiqué des informations sensibles, comme votre numéro de carte bancaire, déposez plainte au commissariat de police ou à la gendarmerie la plus proche. Les cybercriminels pourraient, en effet, en faire un usage frauduleux. Pour être conseillé en cas d'hameçonnage, contactez le service Info Escroqueries au 0805 805 817 (appel gratuit).
3/B – Le fait qu'il y ait dans un message le logo officiel d'un organisme ne signifie pas nécessairement que le message ait été envoyé par l'organisme concerné.
4/A – 3 B – 1 C – 2

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

SÉCURITÉ DES APPAREILS MOBILES

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer au mieux la sécurité numérique de vos appareils mobiles ?

- ☐ **A** Je ne fais jamais fonctionner le Wifi et le Bluetooth en même temps
- ☐ **B** Je mets régulièrement mes appareils à jour
- ☐ **C** Je les verrouille avec un code d'accès difficile à deviner, en plus du code PIN
- ☐ **D** J'équipe mes appareils d'une coque et d'une protection d'écran

2/ Vrai ou Faux

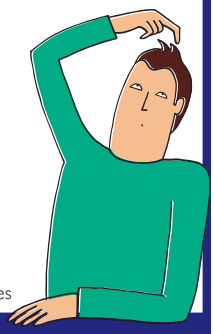
Je n'ai pas besoin de faire des sauvegardes de mon téléphone.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

J'ai besoin d'une application mobile. Je la télécharge :

- ☐ **A** sur le site officiel du fournisseur
- ☐ **B** sur les magasins officiels d'applications comme Google Play ou App Store, par exemple
- ☐ **C** sur n'importe quel autre site



4/ Reliez les situations à leurs solutions

Je travaille régulièrement à l'extérieur **A** ☐
J'ai perdu ou je me suis fait voler mon téléphone **B** ☐
Je télécharge un jeu sur mon téléphone **C** ☐

- ☐ **1** Je bloque ma ligne en appelant mon opérateur et mon téléphone en communiquant mon code IMEI et je dépose plainte
- ☐ **2** J'évite de me connecter à un réseau Wi-Fi public
- ☐ **3** Je n'autorise pas l'accès à mes photos, mes contacts et mes messages

RÉPONSES

1/B et C
2/FAUX – Votre appareil mobile contient de nombreuses données, comme votre répertoire de contacts, vos messages, vos photos et vidéos. En cas de perte, de panne ou de vol de votre appareil, vous pourriez ne plus retrouver vos données.
3/C – Seuls les sites ou les magasins officiels vérifient que les applications que vous installez ne sont pas piégées.
4/A – 2 B – 1 C – 3

SÉCURITÉ DES USAGES PRO / PERSO

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour sécuriser au mieux mes usages numériques pro/perso ?

- ☐ **A** J'utilise des mots de passe différents pour tous les services professionnels ou personnels auxquels j'accède
- ☐ **B** Peu importe l'usage, je n'utilise que mes dossiers professionnels
- ☐ **C** Au travail, je mélange fichiers personnels et professionnels
- ☐ **D** Je ne mélange pas mes messages pro et perso dans ma messagerie personnelle

2/ Vrai ou Faux

J'ai le droit de m'exprimer sur mon travail ou mon entreprise sur les réseaux sociaux lorsque j'utilise mon ordinateur personnel.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

Pour protéger mes usages numériques pro/perso :

- ☐ **A** J'utilise un stockage de données professionnelles distinct du stockage de données personnelles
- ☐ **B** J'utilise ma connexion professionnelle uniquement pour mes besoins professionnels
- ☐ **C** J'utilise mon matériel professionnel pour des besoins personnels
- ☐ **D** J'effectue les mises à jour de mes systèmes très régulièrement

4/ Reliez les situations à leurs solutions

Je suis à la maison et je consulte mes messages professionnels **A** ☐
Je stocke des documents professionnels sur un service en ligne personnel **B** ☐
Je réalise parfois des téléchargements illégaux depuis mon ordinateur professionnel **C** ☐

- ☐ **1** Je demande l'autorisation à mon employeur et prends des mesures de sécurité supplémentaires
- ☐ **2** Je ne le fais qu'à partir de mon ordinateur professionnel
- ☐ **3** Mon entreprise pourrait contrôler mon utilisation de la connexion Internet professionnelle et se retourner contre moi

RÉPONSES

1/A et D
2/VRAI – Uniquement si vos propos ne portent pas préjudice à l'entreprise. Dans le cas contraire, vous risqueriez des poursuites judiciaires.
3/C – Bien que l'utilisation d'une connexion Internet professionnelle à des fins personnelles soit tolérée, gardez à l'esprit que votre utilisation peut mettre en cause votre entreprise. Elle pourrait se retourner contre vous si vous commettiez des actes répréhensibles. Par ailleurs, votre entreprise est en droit de contrôler votre utilisation de la connexion qu'elle met à votre disposition.
4/A – 2 B – 1 C – 3

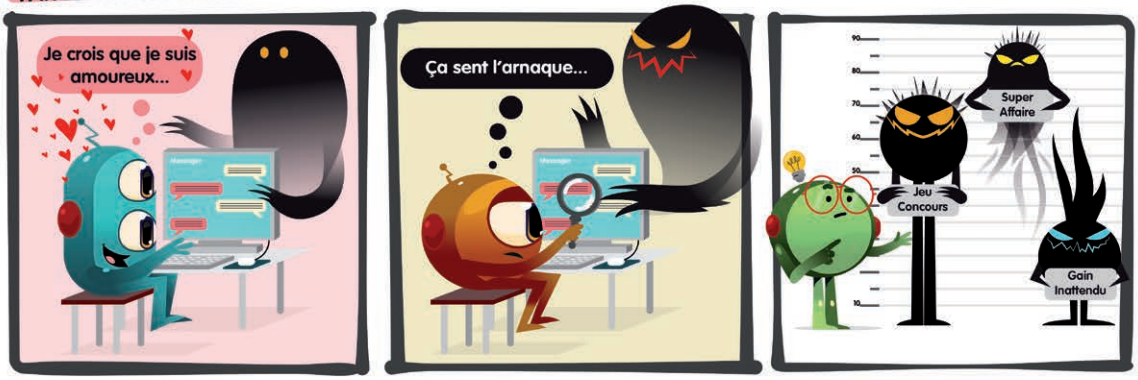
DOCUMENT RÉALISÉ AVEC NOS MEMBRES : cpme CONFÉDÉRATION DES PME — France Victimes — UFC Que Choisir

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES RÉSEAUX SOCIAUX **EN BD**

FAITES ATTENTION À QUI VOUS PARLEZ

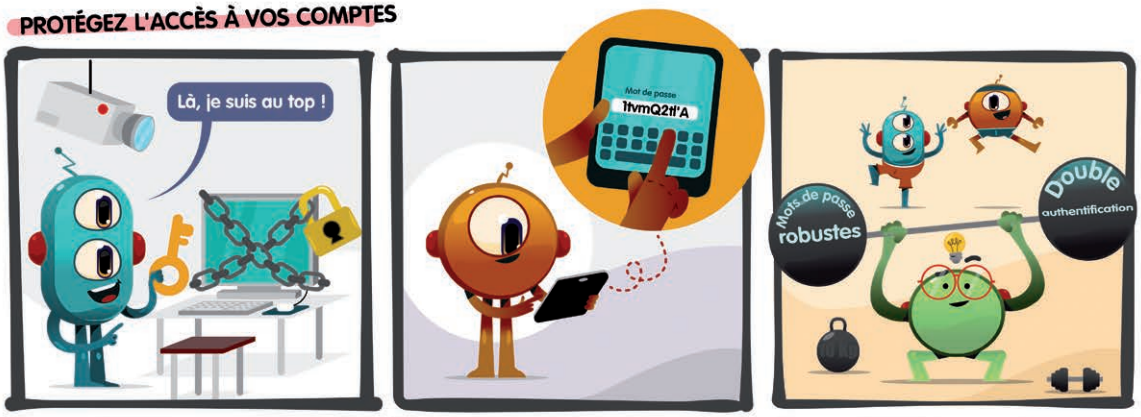


Connaissez-vous l'identité réelle de vos interlocuteurs ?

À leur insu, même vos contacts peuvent vous partager des contenus malveillants.

Méfiez-vous de certaines offres alléchantes, qui peuvent cacher des arnaques

PROTÉGEZ L'ACCÈS À VOS COMPTES



Pas besoin d'être dans l'excès pour protéger l'accès à vos comptes...

Un conseil : utilisez des mots de passe uniques, différents et robustes.

Lorsque votre service le permet, activez également la double authentification.

MAÎTRISEZ VOS PUBLICATIONS

Avant de publier vos messages, pensez à l'utilisation qui pourrait en être faite.

Ne diffusez pas d'informations personnelles ou sensibles, même à un cercle restreint.

Comme Super Discret, faites attention à ce que vous postez sur les réseaux !

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

À PROPOS DE CYBERMALVEILLANCE.GOUV.FR

Lancé en octobre 2017, Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes de cybermalveillance. Ce dispositif a été incubé par l'Agence nationale de sécurité des systèmes d'information (ANSSI) en copilotage avec le ministère de l'Intérieur et avec le soutien des ministères de l'Économie et des Finances, de la Justice et du secrétariat d'État chargé du Numérique. Il est désormais piloté par le Groupement d'Intérêt Public (GIP) ACYMA.

SES PUBLICS SONT:

- les **particuliers**
- les **entreprises** (hors opérateurs critiques – OIV)
- les **collectivités** (hors opérateurs critiques – OIV)

SES MISSIONS SONT:

- l'**assistance aux victimes** d'actes de cybermalveillance
- l'**information** et la **sensibilisation** au niveau national sur la sécurité numérique
- l'**observation du risque numérique** pour pouvoir l'anticiper

SES MEMBRES SONT:

PREMIER MINISTRE

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

SECRÉTARIAT D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES

GIP ACYMA
6 rue Bouchardon, 75010 Paris
www.cybermalveillance.gouv.fr

Suivez-nous sur :