RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

ADOPTER LES BONNES PRATIQUES

LES 10 MESURES ESSENTIELLES POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE

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

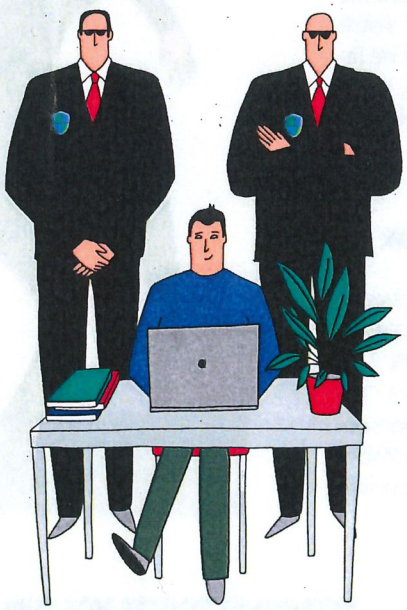
Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement 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 1.0

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.

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

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

COMPRENDRE LES RISQUES

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

mémo

L'HAMEÇONNAGE

CYBERCRIMINEL

VOL DE DONNÉES

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

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

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

VICTIME

COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir ci-dessous)

LIENS UTILES

Signal-spam.fr

Phishing-initiative.fr

Info Escroqueries
0 805 805 817 (gratuit)

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

COMPRENDRE LES RISQUES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

SES MISSIONS

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

QUI EST CONCERNÉ ?

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

Version 3.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

mémo

LES VIRUS INFORMATIQUES

VOL DE DONNÉES

Vous constatez un ralentissement ou un blocage anormal de votre appareil, des messages ou des fenêtres d'erreur s'affichent sans raison apparente ? Vous avez une alerte de votre antivirus ? Vous êtes peut-être victime d'un virus informatique !

BUT
Prendre le contrôle d'un système informatique pour en faire un usage frauduleux, comme espionner l'utilisateur, dérober des données personnelles et/ou confidentielles, attaquer d'autres appareils, chiffrer les fichiers et demander une rançon, etc.

TECHNIQUE
Infection d'un équipement suite à l'ouverture d'une pièce jointe piégée, d'un clic sur un lien frauduleux, de la navigation sur un site malveillant, de l'installation d'une application piratée, le branchement d'un support (clé USB...) contaminé, etc.

COMMENT RÉAGIR ?

- Débranchez la machine d'Internet ou du réseau local
- Identifiez et corrigez l'origine de l'infection
- Récupérez les preuves disponibles
- Déposez plainte
- Supprimez l'infection avec votre antivirus et en cas d'échec réinstallez votre système
- Changez tous vos mots de passe
- Au besoin, faites-vous assister par des professionnels

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

COMPRENDRE LES RISQUES