FICHE PRATIQUE C

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

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 important d'adapter ses pratiques afin de protéger tant votre entreprise ou votre organisation, que votre espace de vie privée. Cette fiche pratique présente les **10 principales règles à adopter pour sécuriser au mieux ses usages numériques personnels et professionnels.**

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

1 Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez

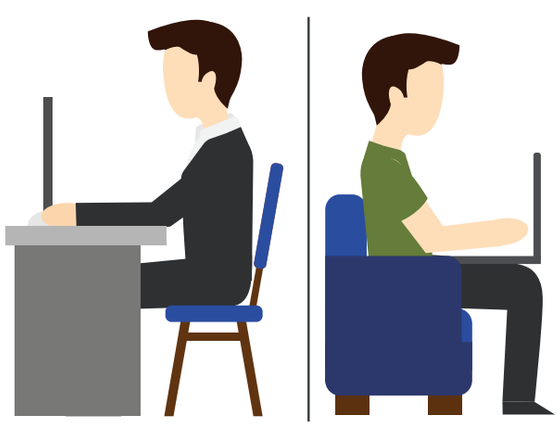
Si vous ne le faites pas et qu'un des services auquel vous accédez se fait pirater, le vol de votre mot de passe permettra à une personne malveillante d'accéder à tous vos autres services y compris les plus critiques (banque, messagerie, sites marchands, réseaux sociaux…). Et si vous utilisez ce même 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 personnelle et professionnelle

Déjà parce que c'est le meilleur moyen de rapidement ne plus s'y retrouver et de commettre des erreurs. Notamment des erreurs de destinataires qui pourraient avoir pour effet 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 entreprise 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.

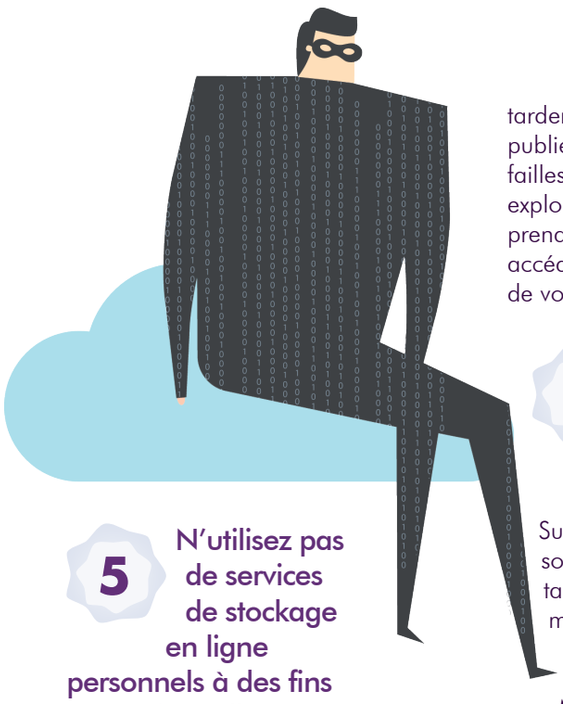
3 Ayez une utilisation responsable d'Internet au travail

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 poursuivis. 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. Alors n'utilisez pas votre connexion professionnelle pour des choses, qui n'ont pas, selon vous, 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 c'était vu ou retransmis par une personne malintentionnée.



5 N'utilisez pas de services de stockage en ligne personnels à des fins professionnelles

Ou du moins pas sans 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, car 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 et 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, 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 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 autre gadget connecté). 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 affecter 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 :

cpme · ESET · Fédération Française de l'Assurance · Microsoft · Entrepreneurs d'Assurances

En partenariat avec l'Agence nationale de la sécurité des systèmes d'information

ANSSI

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

Version 1.0