SYNDESIN
ACCOMPAGNEMENT NUMERIQUE

Mes fiches mémos

ADOPTER UNE POLITIQUE DE MOT DE PASSE RIGOUREUSE

C'est l'un des gestes les plus simples à mettre en œuvre, et pourtant beaucoup le négligent : à chaque nouvelle inscription sur un site web, il vous faut adopter une gestion de mot de passe solide.

Pour cela, voici quelques bonnes pratiques à avoir en tête :

- Utilisez un mot de passe différent pour chaque accès : c'est la première chose à faire pour limiter les dégâts éventuels en cas de piratage.

- Utilisez un mot de passe suffisamment long et complexe : de 8 à 12 caractères contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux.

- Dans le cadre de votre navigation personnelle, changez vos mots de passe au moindre doute d'utilisation frauduleuse.

- Dans le cadre professionnel, n'attendez pas de soupçonner une fraude et modifiez vos mots de passe de façon régulière et systématique.

- Utilisez un mot que personne ne peut deviner : personne ne doit pouvoir le reconstituer, pas même vos proches. Evitez donc toute information très facile d'accès comme votre date de naissance ou le nom de votre chien.

- Ne communiquez jamais votre mot de passe à un tiers : Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe. Si l'on vous demande votre mot de passe après avoir cliqué dans un courriel, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

- Utilisez un gestionnaire de mots de passe : téléchargez un outil comme KeePass qui se chargera de mémoriser tous vos mots de passe et vous permettra de générer des mots de passes aléatoires suffisamment longs et complexes.

- Choisissez un mot de passe particulièrement robuste pour votre boîte de messagerie : l'adresse de messagerie est souvent demandée pour vous inscrire sur un site Internet. Sur cette adresse, vous pouvez recevoir les liens de réinitialisation des mots de passe des comptes en ligne sur lesquels vous êtes inscrits. Si un cybercriminel parvenait à pirater votre messagerie, il pourrait prendre le contrôle de tous vos comptes en ligne (réseaux sociaux, compte bancaire, sites administratifs, etc.).

https://www.dailymotion.com/video/x6lv2v2

SAUVEGARDER SES DONNEES REGULIEREMENT

Sauvegarder régulièrement vos données personnelles et professionnelles vous protège en cas de **panne**, de **perte**, de **vol**, de **destruction** de votre matériel ou de **piratage informatique**. Et pourtant, la majorité des internautes ne mettent en place une routine de sauvegarde régulière **qu'après** avoir subi une première perte de données… Pourquoi attendre d'en être victime alors que vous pouvez mettre en place cette routine dès aujourd'hui ?

Voici les différentes options qui s'offrent à vous pour sauvegarder vos données numériques :

Cas n°1 : Sauvegarder un volume de données faible

- Si vous souhaitez stocker un volume limité de données**, une clé USB voire un DVD enregistrable** devraient suffire.
- Vous pouvez aussi opter pour **un service de stockage en ligne (cloud).** Il existe des solutions gratuites ou payantes en fonction de la capacité de stockage souhaitée.

Cas 2 : Sauvegarder un volume de données conséquent

- Pour effectuer des sauvegardes de plus grande envergure**, le disque dur externe** est la meilleure option.
- Si vous manquez encore de place et que vous êtes à l'aise en informatique, vous pouvez également envisager le **stockage en réseau**. Créez votre propre serveur FTP ou bien achetez un Network Attached Storage (NAS) : vous pourrez alors partager des fichiers sur un serveur accueillant différents disques durs.

SECURITE NUMERIQUE : FAIRE SES MISES A JOUR REGULIEREMENT

Un appareil ou un logiciel qui n'est pas à jour **est vulnérable et davantage susceptible de faire l'objet d'attaques informatiques.**

Voici quelques conseils pour ne plus s'exposer à ce risque :

- Identifiez l'ensemble de vos appareils et logiciels utilisés.
- Lorsque l'on vous propose une mise à jour, **faites-la immédiatement**.
- Téléchargez les mises à jour uniquement depuis les sites officiels des éditeurs.
- Sur vos appareils, activez **l'option de téléchargement et d'installation automatique des mises à jour** si elle existe.
- Anticipez vos périodes d'inactivité en planifiant vos mises à jour.
- Méfiez-vous de fausses mises à jour que l'on vous propose sur Internet. Notre astuce : **vérifiez toujours l'URL du site sur lequel vous vous trouvez.**

SE PROTEGER DES VIRUS ET AUTRES LOGICIELS MALVEILLANTS

Sur Internet, les fichiers malveillants sont nombreux et variés.

Virus, vers, cheval de Troie, ou **logiciels espions (spyware)** sont tout autant de techniques couramment utilisées par les pirates informatiques. Pour vous protéger de ces intrusions, il est indispensable de posséder ces deux outils :

- **Un antivirus**
- **Un pare-feu bien configuré** qui bloquera les connexions non désirées depuis votre ordinateur

Réalisez des analyses (ou scans) de votre ordinateur, votre téléphone mobile, votre tablette régulièrement pour identifier la présence de programmes malveillants. Lorsque votre antivirus demande à ce que ses bases virales soient mises à jour, faites-le immédiatement. De même, lorsqu'il vous signale un fichier suspect et vous propose de le supprimer ou de le mettre en quarantaine, réalisez l'opération au plus vite.

Par ailleurs, quelques bonnes pratiques sont de rigueur lorsque vous utilisez des appareils de stockage externe, comme des clés USB ou des disques durs externes :

- N'utilisez jamais un service ou un équipement inconnu ou abandonné.
- Attribuez un usage spécifique à chaque clé USB pour réduire les effets d'une éventuelle contamination.
- Chiffrez le contenu de vos appareils de stockage pour éviter le piratage.

ÉVITEZ LES RESEAUX WIFI PUBLICS OU INCONNUS

S'ils peuvent s'avérer très utiles**, les réseaux Wifi publics sont une aubaine pour les pirates informatiques**. Très faciles d'accès, ces réseaux peuvent être contrôlés par des cybercriminels pour **intercepter vos informations personnelles**.

Voici quelques conseils pour éviter de vous connecter à ces réseaux ou, le cas échéant, vous en servir de façon sécurisée :

- Pour éviter que vos appareils ne se connectent automatiquement à ces réseaux, **désactivez les connexions sans-fil** (Wifi, Bluetooth, NFC, …) lorsque vous ne vous en servez pas.
- Quand vous le pouvez**, privilégiez la connexion privée 3G ou 4G** associée à votre abonnement mobile. Et n'oubliez pas de sécuriser le partage de connexion de vos appareils à l'aide d'un mot de passe : cela évitera que n'importe qui puisse accéder directement à vos données partagées !
- Si vous n'avez d'autre choix que d'utiliser un Wifi public, veillez à ne jamais y réaliser d'opérations à caractère sensible (paiement par carte bancaire, déclaration d'impôts, renseignement d'informations confidentielles, etc.) et si possible utilisez un réseau privé virtuel (VPN).

SECURITE NUMERIQUE : BIEN SEPARER SES USAGES PROFESSIONNELS ET PERSONNELS

Avec la multiplication des accès à Internet, vos informations personnelles comme professionnelles deviennent accessibles de n'importe où. Il devient possible de :

- Consulter vos emails professionnels dans votre salon.
- Jeter un œil à vos réseaux sociaux pendant une pause-café au bureau.
- Relire un contrat important dans le train puis regarder une retransmission sportive.

Ainsi, avec Internet, **la frontière entre vie professionnelle et vie personnelle devient** de plus en plus poreuse. Pour sécuriser au mieux vos usages numériques dans ces différents environnements, commencez par utiliser **un mot de passe différent** pour chaque service professionnel et personnel auquel vous avez accès.

Distinguez également vos usages sur les **réseaux sociaux** :

- Évitez de partager des informations professionnelles sur vos réseaux sociaux personnels. Le partage et l'interprétation d'informations peuvent très vite nuire à votre entreprise.

- À l'inverse, vous ne souhaitez probablement pas que votre entreprise ait connaissance de tout ce que vous publiez dans votre cercle privé.

Il en va de même **pour les messageries électroniques et les services de stockage en ligne**. Ne mélangez pas vos messages et utilisez des services en lignes (cloud) distincts pour stocker vos données professionnelles et personnelles. Sans cela, vous risquez au mieux une erreur de destinataire, au pire, de mettre en danger votre entreprise et de vous trouver légalement responsable de la situation.

ÉVITER DE NAVIGUER SUR DES SITES DOUTEUX OU ILLICITES ET ETRE VIGILANT LORS DU TELECHARGEMENT D'UN FICHIER

De façon générale, évitez de vous rendre sur des sites douteux ou illicites. Certains sont susceptibles d'héberger des contrefaçons et **peuvent contenir des virus**. N'utilisez pas de plateformes non-officielles et ne téléchargez pas de fichiers provenant d'un site de téléchargement illégal : de nombreux fichiers sont infectés et peuvent contenir des virus et autres logiciels malveillants. Certains sites pornographiques sont également de véritables nids à virus, soyez vigilant.

Pour télécharger de nouvelles applications sur votre ordinateur, tablette ou smartphone, nous vous recommandons de **n'utiliser que les magasins officiels** ou encore le site de l'application elle-même.

CONTROLER LES PERMISSIONS DES COMPTES UTILISATEURS

Un même poste de travail, serveur ou logiciel peut être accessible par plusieurs utilisateurs, chacun disposant **d'un accès plus ou moins restreint selon son niveau de permission**.

Lorsqu'il vous revient d'ajouter des utilisateurs à un appareil ou service, et donc de choisir le niveau de permission à leur accorder, appliquez toujours **la règle du privilège minimum** : assurez-vous que chacun des utilisateurs ait uniquement les permissions dont il a besoin.

Ce principe simple limite les conséquences dommageables en cas d'attaque et augmente considérablement votre **sécurité numérique**.

Comment faire ?

- Par défaut, tous les utilisateurs d'un poste de travail ou d'un serveur doivent avoir un niveau d'accès au système d'exploitation et aux informations limité.
- Ensuite, personnalisez au maximum les attributions et possibilités de chacun en fonction de ses besoins.

Enfin, surveillez bien chaque compte et l'utilisation qui en est faite.

CONTROLER LES PERMISSIONS DES COMPTES UTILISATEURS

L'hameçonnage (ou phishing en anglais) désigne une technique frauduleuse qui consiste à usurper l'identité d'un organisme connu (banque, opérateurs, etc) ou d'un proche pour récupérer des informations confidentielles.

Voici quelques recommandations simples pour l'éviter :

- Ne communiquez pas d'informations personnelles ou professionnelles par messagerie ou par téléphone.
- En cas de réception d'un message contenant un lien, positionnez le curseur de la souris (**sans cliquer**) sur ce lien pour afficher l'adresse vers laquelle il pointe réellement.
- **Vérifiez bien l'adresse du site Internet** avant de renseigner des données. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux.
- Si le site le permet, activez **la double authentification** pour sécuriser vos accès.
- Utilisez des mots de passe de différents et complexes pour chaque site et application.
- Saisissez directement dans votre navigateur l'adresse du site concerné.

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 informations bancaires, faites opposition à vos cartes et déposez plainte.

FAIRE ATTENTION AUX INFORMATIONS PERSONNELLES OU PROFESSIONNELLES QUE L'ON DIFFUSE SUR INTERNET

De façon générale, chacun doit se sentir responsable de ce qu'il diffuse sur l'internet. Ne communiquez jamais d'informations sensibles sur des sites qui vous semblent insuffisamment protégés **et jamais lorsque la mention "Non sécurisé" apparaît à gauche de l'adresse du site Internet**.

De la même manière, faites attention à bien identifier les personnes avec qui vous parlez sur Internet. Si vous avez un doute sur une identité, à cause d'une façon d'écrire inhabituelle par exemple**, contactez cette personne via un autre moyen** avant de répondre à toute question. Enfin soyez toujours vigilant : même vos amis ou contacts peuvent vous envoyer ou partager des contenus malveillants, de façon non intentionnelle.