SYNDESIN
ACCOMPAGNEMENT NUMERIQUE

Mes fiches mémos

INTRODUCTION

Hameçonnage, rançongiciel, arnaque au service client, virus, malware… Les dangers concernant la navigation sur Internet sont nombreux, et se dissimulent parfois sous les actes les plus communs que vous effectuez au quotidien sur le web. Pour éviter au maximum ce type de souci, et se protéger sur Internet au mieux, voici 10 réflexes à acquérir dans votre quotidien personnel comme professionnel.

ÉVITER DE SE RENDRE SUR DES SITES DOUTEUX OU ILLEGAUX

Le conseil peut sembler basique, mais il est finalement important : **si un site web vous semble douteux, ou qu'il propose des services illégaux, ne vous y rendez pas**.

Parmi les sites web qui peuvent vous exposer à des problèmes de sécurité, on compte notamment :

- Les sites de téléchargement pirates
- Les sites de vidéo en ligne (streaming) ou de vidéo à la demande (VOD) pirates
- Les sites pornographiques pirates

Il s'agit de véritables nids à virus, à éviter à tout prix.

De même, **évitez de télécharger et d'utiliser un logiciel piraté ou "cracké"**. Si cela peut être attirant, notamment parce que cela évite l'achat du logiciel, sachez que non seulement c'est illégal, mais qu'ils sont généralement infectés par des virus.

Plus spécifiquement pour les entreprises :

Expliquez à vos collaborateurs en quoi consiste une utilisation responsable d'Internet au travail. Sensibilisez-les, par exemple, au fait qu'ils pourront être poursuivis judiciairement s'ils commettent des actes répréhensibles (téléchargements illégaux, atteinte aux droits d'auteur, publication de propos outrageants au nom de l'entreprise ou à son propos…).

FAIRE SES MISES A JOUR DE SECURITE DES QUE POSSIBLE

Le saviez-vous ? Un système d'exploitation, un navigateur ou un logiciel qui n'est pas à jour de ses correctifs de sécurité est **un système très vulnérable aux attaques sur Internet**. Les pirates profitent facilement de ces brèches de sécurité. Aussi, dès qu'un système vous propose une mise à jour, faites-la au plus vite.

https://www.dailymotion.com/video/x7m3g9m

SE PROTEGER SUR INTERNET : CHOISIR DES MOTS DE PASSE SECURISES

Selon de nombreuses études**, le mot de passe 123456 reste l'un des plus utilisés au monde**. Or, le mot de passe est l'une des premières mesures de sécurité qui peut vous protéger de l'hameçonnage. Pour éviter cela, choisissez un mot de passe compliqué à trouver. Celui-ci doit :

- Contenir 12 caractères minimum
- Mélanger chiffres, lettres et caractères spéciaux
- Être anonyme (n'y intégrez pas votre date de naissance, le nom de votre chien ou autre)

La meilleure pratique est d'avoir **un mot de passe pour chaque compte ou logiciel utilisé**. La démarche vous semble complexe ? Pour gérer et stocker un grand nombre de mots de passe, procurez-**vous un logiciel de gestion de mots de passe**. L'outil Keepass, gratuit, a fait l'objet d'un agrément par une autorité nationale : vous pouvez vous y fier.

Enfin, renouvelez régulièrement vos mots de passe, car même en étant prudent, il se peut qu'ils aient été compromis et que vous l'ignoriez.

https://www.dailymotion.com/video/x7nwhwd

Plus spécifiquement pour les entreprises :

– Sensibilisez vos collaborateurs aux meilleures pratiques en termes de mots de passe. Distribuez-leur des fiches de bonnes pratiques, et obligez le renouvellement régulier de leurs divers mots de passe.
– Pensez également à **sensibiliser tous les prestataires et sous-traitants** qui utilisent des logiciels et comptes de votre entreprise : ils sont également des vecteurs d'attaque potentielle de votre entreprise.

BIEN CHOISIR SON PARE-FEU ET SON ANTI-VIRUS

Quel que soit votre système d'exploitation ou votre matériel informatique, vous ne pouvez pas faire l'impasse sur de bons logiciels anti-virus, qui vous protègent de différentes attaques par Internet.

Un bon anti-virus vous protège de tous les types de fichiers malveillants connus, à savoir :

- les virus, qui peuvent se cacher derrière des logiciels d'apparence bénigne
- les vers, qui sont souvent reçus par pièce-jointe dans les emails
- les chevaux de Troie (ou trojan) qui permettent d'accéder à vos données, voire de totalement contrôler votre ordinateur
- les spywares (ou logiciels espions), qui transmettent au pirate vos données personnelles

Munissez-vous également d'un pare-feu. Cette fonctionnalité permet non seulement de vous protéger contre les intrusions provenant d'un réseau tiers quand vous êtes sur Internet, mais également de bloquer les connexions non désirées depuis votre ordinateur. La plupart des systèmes d'exploitation (Mac et Windows) ont un pare-feu intégré, et nombre d'anti-virus proposent aussi cette fonctionnalité indispensable.

FAIRE DES SAUVEGARDES REGULIERES DE SES DONNEES

Même si vous vous dotez de bons logiciels anti-malware, il est plus prudent de considérer que vos données ne sont jamais totalement protégées ; c'est pourquoi elles doivent faire l'objet de **sauvegardes régulières, stockées sur des équipements déconnectés**.

Pour les entreprises, ce conseil est particulièrement essentiel, notamment concernant **les données vitales au bon fonctionnement de la société**. Cela permet d'éviter une baisse d'activité trop importante en cas d'attaque ou d'effacement de ces données cruciales.

https://www.dailymotion.com/video/x7chrba

SE PROTEGER SUR INTERNET : SE MUNIR D'UN BLOQUEUR DE PUBLICITES

Les plugins bloqueurs de publicités pour les navigateurs web permettent de limiter l'exposition aux publicités potentiellement malveillantes. Certains navigateurs offrent déjà des fonctionnalités de ce type, mais l'ajout d'un tel plugin vous assurera un second moyen de protection.

Certains sites, comme les sites de média en ligne, vous demanderont de désactiver votre bloqueur de publicités pour consulter le contenu du site web : faites preuve de vigilance et de discernement lorsque vous le faites.

REDOUBLER DE VIGILANCE FACE AUX MESSAGES D'INCONNUS

Le courriel est l'un des leviers les plus puissants pour les pirates sur Internet. **Gardez toujours un œil attentif à ce qui vous est envoyé par ce biais**.

N'ouvrez pas les pièces jointes ou ne cliquez pas sur les liens dans les messages provenant d'utilisateurs inconnus. Il en va de même pour les messages provenant d'utilisateurs connus, mais dont la structure du message est inhabituelle ou vide.

https://www.dailymotion.com/video/x5s2fp2

Le conseil en plus :

N'utilisez pas un compte avec des droits "administrateur" pour consulter vos messages ou naviguer sur Internet. En effet, si un virus veut s'installer sur votre machine, une confirmation vous sera au moins demandée. Dans le cas contraire, et si votre machine se fait pirater, le pirate sera administrateur de votre machine et pourra donc agir comme il l'entend dessus.

FAIRE ATTENTION A QUI ON TRANSMET SES DONNEES

Dans le cadre personnel comme le cadre professionnel, vous avez souvent l'occasion de remplir des formulaires pour accéder à des informations, des promotions, ou pour vous inscrire à des événements ou des sites web. Lorsque vous vous apprêtez à transmettre des données, même les plus basiques, comme votre email, **vérifiez à qui vous les transmettez** :

- Consultez la Politique de Confidentialité du site web (qui doit normalement être mentionnée dans le formulaire lui-même, depuis la mise en application du RGPD).

- Ne transmettez jamais vos données personnelles (adresse, numéro de téléphone, coordonnées bancaires ou de carte bancaire, ou encore données sensibles concernant votre santé par exemple) par email à des inconnus.

Plus spécifiquement pour les entreprises :

S'il vous faut protéger certaines données particulièrement sensibles de votre entreprise, n'hésitez pas à créer un guide interne de bonnes pratiques à destination de vos collaborateurs. Précisez dans ce guide que ces données ne doivent pas être diffusées en dehors de l'entreprise, notamment par email ou via les réseaux sociaux.

BIEN REFLECHIR AVANT DE PUBLIER SUR INTERNET

À l'ère des réseaux sociaux, il peut être tentant de publier des éléments de sa vie personnelle sur Internet. Cependant, il est important de prendre conscience de **l'impact que peuvent avoir ces publications sur votre vie personnelle**. Certains utilisateurs malveillants peuvent profiter de ce que vous publiez notamment pour :

- **Connaître vos habitudes quotidiennes** : on ne compte plus, par exemple, le nombre de cambriolages effectués grâce à une publication sur les réseaux sociaux qui indique que l'occupant était en vacances,

- **Utiliser ou détourner vos photos** : l'usurpation d'identité est commune sur Internet.

Quel que soit le paramètre de confidentialité que vous choisissez sur un réseau social, souvenez-vous que cela reste du partage d'information. Si seuls vos "amis" peuvent voir une publication, elle reste publiée sur le web, à la portée de potentiels utilisateurs malveillants. Réfléchissez donc bien avant de publier quoique ce soit sur Internet.

https://www.dailymotion.com/video/x665ji1

SE PROTEGER SUR INTERNET : NE PAS OUBLIER VOS TELEPHONES ET TABLETTES

On a tendance à séparer l'utilisation d'un téléphone portable ou d'une tablette de celle d'un ordinateur de bureau. Or, **ces appareils sont, eux aussi, connectés à Internet et contiennent des données personnelles**. Lorsque vous utilisez une application, elle va, souvent, utiliser une connexion internet pour chercher et transmettre des données.

Gardez donc à l'esprit que vos téléphones et tablettes, ainsi que vos objets connectés (type montre connectée ou assistant vocal) sont également concernés par tous ces conseils.

Avec ces 10 bonnes pratiques en tête, vous voilà paré à naviguer sur le web en prenant le maximum de précautions. Même si ces éléments deviennent des réflexes pour vous, n'oubliez pas que vous n'êtes jamais à l'abri d'un problème : la vigilance est finalement l'élément-clé pour bien se protéger sur Internet.