SOYONS SENSIBILISE SUR LA SECURITE INFORMATIQUE

L'internet est un formidable moyen de communication, d'échange et d'accès à la connaissance. Qu'il soit accessible d'un ordinateur, d'un smartphone ou d'une tablette, l'internet présente des risques que nous ne pouvons plus ignorer. Les menaces peuvent être accidentelles (erreur humaine, mauvaise configuration) ou intentionnelles (programmes informatiques malveillants cachés dans des pièces jointes à des messages électroniques ou dans des clés USB piégées, vol de mots de passe). Face à ces menaces, il est donc nécessaire de garantir la sécurité de nos informations.

A. **Les 10 habitudes pour sécuriser son Pc**

1) Mettre à jour régulièrement le système d'exploitation et les logiciels

Maintenir votre système d'exploitation à jour est la première des règles de sécurité. La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger leurs failles.

2) Installer des logiciels de sécurité

Les logiciels (Antivirus, firewall, anti-spam. etc.) permettent de vous protéger contre la plupart des attaques visant à corrompre votre ordinateur. Cependant, il ne faut pas oublier de les mettre à jour régulièrement. En général, une option de mise à jour automatique est disponible lors de la configuration de ces logiciels.

Un des premiers principes de défense est de conserver une copie de ses données (Sur des supports amovibles : CD/DVD, disque dur externe, sur le Cloud) afin de pouvoir réagir à une attaque ou un dysfonctionnement.
La sauvegarde de vos données est une condition de la continuité de votre activité.

4) Utiliser des mots de passe de qualité

Par définition, un mot de passe désigne une séquence de caractères utilisée par un usager pour valider son accès à des ressources personnelles. Plus la séquence est aléatoire, plus le mot de passe est sûr. Pour ce faire, une combinaison de majuscules, minuscules, chiffres et caractères spéciaux avec une taille du mot de passe dépassant les dix caractères est recommandée pour éviter qu'il soit cassé par des outils automatisés.

5) Ne pas ouvrir des pièces jointes provenant de sources suspectes ou inconnues

Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme par exemple une pièce jointe appelée «photos.pif), .com, .bat, .exe, .vbs et .lnk .

6) Eviter de cliquer rapidement sur des liens suspects

Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être

trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur, de nombreux problèmes seront ainsi évités.

7) Désactiver par défaut les composants ActiveX et JavaScript

Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes, mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. En dépit de la gêne que cela
peut occasionner, il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.

8) Eviter de divulguer des informations personnelles

Les informations personnelles diffusées sur internet (nom, prénom, numéro de tél… etc.) peuvent faciliter la tâche à un utilisateur malveillant préparant une attaque de type « social engineering ». Il faut éviter aussi de saisir des informations sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises.

9) Eviter d'installer des logiciels de partage (P2P)

Peer-to-Peer (P2P) est un moyen de téléchargement très populaire. Cependant, les auteurs de malwares ont investi ce réseau afin d'y déposer des fichiers piégés dans le but de propager leurs infections.

10) Ne pas surfer sur Internet tout en étant en mode Administrateur

Vous ne devez ni surfer sur le Web, ni consulter vos e-mails, ni accéder sous quelque forme que ce soit (messagerie instantanée, P2P etc. ...) à l'Internet lorsque vous êtes en mode Administrateur. Ceci peut être dangereux vu que les droits dits d'Administrateur donnent tous les privilèges à un attaquant si celui-ci a pu compromettre votre PC.

B. **Protéger sa vie privée sur Internet**

1) L'identité numérique

L'identité numérique d'un individu est composée de données techniques (adresse IP, cookies…), de données personnelles institutionnelles (nom prénom, adresse, n° de tel, certificats…) et informelles (commentaires, notes, billets, photos…). Toutes ces bribes d'information composent une identité numérique plus globale qui caractérise un individu, sa personnalité, son entourage et ses habitudes.

2) Sur internet : tout se garde, rien ne se perd

Le Web a une mémoire : toute contribution de votre part sur un site ou un forum par exemple, peut demeurer en ligne pendant des années tant que ce même site est en ligne. Il est également possible de retrouver des archives d'anciennes versions de sites.

3) protéger votre vie privée avec l'usage des smartphones

- Ne pas enregistrer dans le smartphone des informations confidentielles telles que des codes secrets (ex : accès à la banque en ligne), des codes d'accès (travail, ordinateur portable) afin de limiter les risques en cas de vol, piratage, ou usurpation d'identité ;
- Mettre en place un délai de verrouillage automatique du téléphone en veille. En effet, en plus du code PIN, ce dispositif permet de rendre inactif (verrouiller) le téléphone au bout

d'un certain temps, ce qui empêche la consultation des informations contenues dans le téléphone en cas de perte ou de vol ;

- Installer un antivirus quand cela est possible ;
- Ne pas télécharger d'applications de sources inconnues en privilégiant les plates-formes officielles ;
- Vérifier à quelles données contenues dans le smartphone l'application installée va avoir accès
- Lire les conditions d'utilisation d'un service avant de l'installer, et ne pas hésiter à consulter l'avis des autres utilisateurs ;
- Régler les paramètres au sein du téléphone ou dans les applications de géolocalisation afin de toujours contrôler quand et par qui l'appareil peut être géolocalisé ;
- Désactiver le GPS ou le WIFI après utilisation de l'application de géolocalisation.

C. **Sécurité lors de l'utilisation d'un Smartphone**

Tout comme les ordinateurs, les Smartphones sont des cibles privilégiées d'attaques. Par exemple le risque de phishing existe aussi sur Smartphone. En effet, il ne faut pas cliquer sur n'importe quel lien. L'internet mobile se développe très rapidement et nous allons retrouver sur les terminaux mobiles les mêmes risques que sur un ordinateur classique. Utilisés par des professionnels, ils contiennent également des données à priori confidentielles et ils sont une porte d'entrée dans le système d'information de l'entreprise.

Pratiques pour améliorer la sécurité de son smartphone :

Evaluer les faiblesses principales de votre Smartphone : représente la première ligne de défense, faire une recherche sur Internet pour en savoir davantage car chaque système d'exploitation a ses propres failles.

Les mises à jour : comme pour tout système d'exploitation, les fabricants de Smartphones proposent assez régulièrement des mises à jour faisant évoluer les fonctionnalités de leurs terminaux. Elles permettent par la même occasion de combler certaines vulnérabilités critiques.

Contrôler les systèmes de communication : il est fortement conseillé de désactiver les systèmes Bluetooth et Wifi quand ils ne sont pas utilisés. Ils peuvent être utilisés à des fins malveillantes comme porte d'entrée aux données du Smartphone.

Surveiller son trafic de données : l'un des indicateurs les plus pertinents de l'utilisation d'un mobile par un tiers mal intentionné est une augmentation du trafic de données qui doit éveiller tes soupçons. Une application comme Traffic Monitor Widget sur le système d'exploitation mobile Android s'acquitte parfaitement de cette tâche.

Activer le verrouillage automatique de son Smartphone : Réflexe de base, le verrouillage automatique, activer la fonction de verrouillage en cas d'inactivité en l'associant à un mot de passe va permettre de restreindre l'accès aux données de votre téléphone par des personnes malveillantes.

N'enregistrez pas de données confidentielles sur votre Smartphone : Conseil extrêmement simple à donner mais de plus en plus difficile à appliquer. En effet les Smartphones contiennent aujourd'hui presque par défaut des données sensibles. Votre localisation même approximative, vos emails, le

numéro de vos proches, votre adresse, et c'est de plus en plus compliqué de ne laisser filtrer aucune information dite « sensible » et donc qui pourrait vous nuire si elle est interceptée par un tiers, sur votre Smartphone.

Le blocage à distance : cette fonction de sécurité va permettre de bloquer son téléphone ou d'effacer les données à distance en cas de vol ou de perte. L'éditeur de logiciel de sécurité F-Secure propose une solution de verrouillage à distance des smartphones tournant sur Symbian et Windows Mobile.

Vérifiez quels droits vous donnez à quelle application : si vous avez un mobile Android par exemple, à chaque installation d'application apparaît à l'écran une petite liste des permissions à donner : Localisation, accès au réseau, accès au compte Google... la liste peut être longue et donne beaucoup de pouvoir à l'application en question. Vérifiez donc au moins si les permissions demandées sont logiques : un jeu a-t-il réellement besoin d'accéder et de modifier votre liste de contacts ? Si la réponse est non, donc prudence.

D. **Risques liés à l'utilisation des logiciels piratés**

Vous pouvez mettre votre PC à risque de dommages et de menaces de sécurité. Il existe plusieurs méthodes pour obtenir et utiliser des logiciels contrefaits. Ceux couramment utilisés sont : l'obtention et l'utilisation de « clés contrefaites de produit », l'obtention de programmes « Générateur de clé » et les utiliser pour créer des clés de produits, et l'obtention des « outils de craque » et de les utiliser pour contourner les mécanismes d'attribution et d'activation de licences.

Risques techniques d'utilisation des logiciels piratés :

- Les logiciels piratés peuvent provoquer une panne de votre système. Ils entraînent une perte de temps. Vous pouvez perdre des données ou des fichiers irremplaçables.
- Vous ne pouvez pas bénéficier des mises à jour du produit. Or, les mises à jour sont indispensables pour assurer la sécurité des logiciels : chaque année, les éditeurs publient des dizaines de « correctifs sécurité » ou des « patchs » améliorant le fonctionnement de leurs logiciels. Si, cependant, vous utilisez des logiciels contrefaits, vous ne pourrez pas incorporer ces correctifs et serez vulnérable face à d'éventuelles attaques.
- Les logiciels piratés sont souvent incomplets et manquent de documentation. De plus, certains logiciels téléchargeables sur Internet sont en fait des versions béta (de test) qui ne comportent pas toutes les fonctionnalités. Les pièces manquantes peuvent être parfois fatales : les versions béta étant destinées à l'essai, rien ne garantit qu'elles ne mettent pas en péril le bon fonctionnement de votre ordinateur.
- Les logiciels piratés peuvent ne pas fonctionner correctement ou être entièrement défectueux, ce qui entraîne une surconsommation des ressources de votre entreprise et une augmentation des coûts informatiques.
- En cas de problème, vous ne pouvez pas avoir recours au support technique de l'éditeur.
- Les logiciels contrefaits peuvent être malveillants, par exemple contenir des chevaux de Troie, des virus ou des spywares qui s'infiltrent sur votre ordinateur et font usage de vos informations personnelles sans votre autorisation, qu'il s'agisse de vos numéros de carte de crédit ou de comptes bancaires, de vos mots de passe ou de vos carnets d'adresses. Les informations volées peuvent être exploitées immédiatement par des usurpateurs d'identité.

Des conseils pour garder votre système à l'abri de Ransomware :

- Ne pas stocker les données importantes uniquement sur le PC.
- Avoir deux sauvegardes des données : sur un disque dur externe et dans le cloud.
- Le Dropbox / Google Drive / OneDrive / etc. ne doivent pas être activés par défaut.
- Le système d'exploitation et les logiciels utilisés doivent être à jour.
- Ne pas utiliser de compte « administrateur » pour un usage quotidien.
- Désactiver les macros dans la suite Microsoft Office
- Supprimer les plugins des navigateurs ou les activez au besoin.
- Ajuster les paramètres de sécurité et de confidentialité des navigateurs.
- Supprimer les plugins obsolètes et les add-ons des navigateurs.
- Utiliser un bloqueur d'annonce pour éviter la menace d'annonces potentiellement malveillantes.
- Ne jamais ouvrir de courriers indésirables ou d'emails provenant d'expéditeurs inconnus.
- Ne jamais télécharger des pièces jointes de courriers indésirables ou de courriers suspects.
- Ne jamais cliquer sur les liens dans les courriers indésirables ou les courriers suspects.
- Utiliser un antivirus fiable.
- Avoir une solution de filtrage du trafic qui peut fournir une protection proactive anti ransomware.

E. **Se protéger du Phishing**

Le phishing ou hameçonnage est une technique d'ingénierie sociale, qui consiste à exploiter non pas une faille informatique mais la « faille humaine ».

Des règles pour éviter le Phishing :

- Ne cliquez pas directement sur le lien contenu dans le mail, ouvrez plutôt votre navigateur et saisissez vous-même l'URL
  d'accès au service.
- Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique.
- Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas.