BELOUCIF ASSIA

Chapitre 3: LES BONNES PRATIQUES EN SÉCURITÉ DE L'INFORMATION

Les dix règles de base pour sécuriser votre PC

1. Mettre à jour régulièrement le système d'exploitation et les logiciels installés :

- 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 leus failles.

Les dix règles de base pour sécuriser votre PC

2. Se protéger contre les intrusions en installant des logiciels de sécurité :

- Ces 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.

Les dix règles de base pour sécuriser votre PC

3. Effectuer des sauvegardes régulières :

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

Les dix règles de base pour sécuriser votre PC

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.

Les dix règles de base pour sécuriser votre PC

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 .

Les dix règles de base pour sécuriser votre PC

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.

Les dix règles de base pour sécuriser votre PC

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.

Les dix règles de base pour sécuriser votre PC

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.

Les dix règles de base pour sécuriser votre PC

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

- Le Peer-to-Peer (P2P) est un moyen de téléchargement devenu 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.

Bien sécuriser son réseau sans-fil Wi-Fi domestique

- **Désactiver la diffusion du SSID :** Le SSID identifie le réseau. C'est un nom qui est utilisé pour différencier votre réseau sans-fil des autres. Si vous désactivez sa diffusion, celui-ci n'apparaitra pas dans la liste des connexions possibles de vos voisins.

Bien sécuriser son réseau sans-fil Wi-Fi domestique

- **Utiliser le chiffrement :** Il faut chiffrer les données qui circulent sur votre réseau. Comme vous ne pouvez pas savoir qui est à l'écoute, le chiffrement de vos données permet d'en assurer la confidentialité. Cela se fait à l'aide de ce que l'on appelle une clef. Si on ne connaît pas cette clef, il devient impossible de lire ou de transmettre des données valides.
- WPA2(Wi-Fi Protected Access 2) permet d'avoir un niveau de sécurité supérieur à celui de WPA(Wi-Fi Protected Access). Il est conseillé de l'utiliser quand c'est possible.

Bien sécuriser son réseau sans-fil Wi-Fi domestique

- **Utiliser le filtrage d'adresse MAC :** Chaque carte réseau possède un identifiant unique pour la reconnaître, c'est l'adresse MAC. Dans l'utilitaire de configuration de votre modem/routeur Wifi, il vous faut activer l'option de filtrage puis saisir les adresses MAC de chacune des machines qu'on autorise à se connecter à votre réseau.

Bien sécuriser son réseau sans-fil Wi-Fi domestique

- **Désactiver Le Serveur DHCP :** DHCP (Dynamic Host Configuration Protocole) est un mécanisme qui permet d'affecter automatiquement des paramètres nécessaires à la communication sur le réseau (adresse IP, masque de sous-réseau, passerelle, DNS). C'est très pratique d'utiliser le DHCP mais un pirate n'aura pas alors à deviner la configuration de votre sous-réseau. Donc, autant se mettre en configuration fixe : vous choisissez votre IP et vous la conservez.

Bien sécuriser son réseau sans-fil Wi-Fi domestique

- **Combiner les mécanismes de sécurité :** Chacun des mécanismes de sécurité cités peut être contourné d'une façon ou d'une autre. Pour avoir un bon niveau de sécurité utilisez une combinaison de ces mécanismes. Le minimum étant d'utiliser WPA2 et un filtrage par adresse MAC.

Faites attention à votre boîte de messagerie électronique

- Eviter de mentionner votre adresse e-mail dans les forums, les sites web… Des robots parcourent en effet toutes les pages présentes sur Internet afin de collecter des adresses e-mails.
- Ne jamais répondre à un message infecté ou à un Spam, sinon cela prouve que votre adresse est bien active, contentez- vous de supprimer le message. Si vous avez malgré tout ouvert le spam, ne visitez jamais les sites mentionnés dans le message.
- A la réception d'un canular le mieux est de mettre systématiquement l'expéditeur en indésirable. Fuyez alors ce type d'e-mail, en cas de doute, faites un tour sur le site « www.hoaxbuster.com » qui recense les canulars du Web.

Faites attention à votre boîte de messagerie électronique

- Méfiez-vous des messages que vous recevez, il se peut que vous receviez un message d'une de vos connaissances, dont la machine est infectée. Soyez sur vos gardes, particulièrement lorsqu'il y a une Pièce Jointe, s'il s'agit d'un message ‹''Transmis'' (Tr:) ou en ''Réponse'' (Re:) à un de vos précédents messages, que vous n'avez jamais envoyé.
- Les pièces jointes peuvent contenir des virus ne les téléchargez que lorsqu'elles proviennent d'expéditeurs que vous connaissez, même vos amis peuvent vous transmettre à leur insu des fichiers infectés. Veillez aussi à effectuer les mises à jour de votre Anti-virus.

Faites attention à votre boîte de messagerie électronique

- Quelques indications peuvent vous aider à déceler les courriers électroniques d'hameçonnage ou des liens frauduleux.
  - Les messages électroniques d'hameçonnage prennent diverses formes, voici la phrase qui est fréquemment utilisée dans les arnaques par courrier électronique d'hameçonnage : «Veuillez vérifiez votre compte », vous ne devez envoyer des mots de passe, des informations d'identification ou des noms d'utilisateur, ou d'autres informations personnelles par courrier électronique.
  - Si vous recevez un courrier électronique vous demandant d'actualiser vos informations ne répondez pas : c'est une arnaque par hameçonnage.

Protéger sa vie privée sur Internet

- **Qu’est ce qu’une donnée à caractère personnel ?**
- Il s’agit principalement des informations qui permettent d’identifier soit directement, soit indirectement par recoupement d’informations, une personne, telles que:
  - nom, prénom, • photo, • date de naissance, • statut matrimonial, • adresse postale, email, adresse IP d’ordinateur • n° de sécurité sociale, • n° de téléphone, • n° de carte bancaire, • plaque d’immatriculation du véhicule, • élément d’identification biométrique, • les données de géolocalisation • etc.

Protéger sa vie privée sur Internet

- **L'IDENTITE NUMERIQUE ?**
- « L'identité numérique d'un individu est composée de:
  - données techniques (adresse IP, cookies…)
  - données personnelles institutionnelles (nom prénom, adresse, n° de tel, certificats…)
  - données personnelles 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.
- Ces petits bouts d'identité fonctionnent comme des gènes : ils composent l'ADN numérique d'un individu ».

Protéger sa vie privée sur Internet

- **ATTENTION 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. Exemple : le site WayBackMachine (Internet Archive) conserve des versions antérieures de pages de sites et blogs depuis 1996.

  - Réfléchir avant de publier ou de poster des informations, avis ou photos : Avant de poster un message ou de diffuser une vidéo ou une photo, sachez que tout ce que vous diffuserez volontairement ayant un caractère privé pourra être visualisé par des milliers de personnes (inconnus) avec le risque que ces contenus soient détournés.

Protéger sa vie privée sur Internet

- Protéger vos mots de passe : choisissez des mots de passe compliqués et ne les communiquer à personne.
- Donner le minimum d'informations personnelles sur Internet.
- Vérifier vos traces sur Internet en utilisant un moteur de recherche pour découvrir quelles informations vous concernant circulent sur Internet.
- Prendre le temps de lire les Conditions Générales d'Utilisation avant de s'inscrire sur les réseaux sociaux.
- Sécuriser son compte sur les réseaux sociaux en paramétrant correctement son profil.
- Utiliser un pseudonyme connu seulement de vos proches.
- Prenez garde aux sites qui offrent prix et récompenses en échange de votre contact ou de toute autre information.
- Ne répondez jamais, et sous aucun prétexte, aux spammeurs.

Protéger sa vie privée sur Internet

- **Bonnes pratiques par rapport à l'usage des smartphones pour protéger votre vie privée :**
  - 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 ;
  - Activer si possible le chiffrement des sauvegardes du téléphone en utilisant les réglages de la plate-forme avec laquelle le téléphone se connecte. Cette manipulation garantira que personne ne sera en mesure d'utiliser les données figurant dans le smartphone ;
  - Installer un antivirus quand cela est possible ;

Protéger sa vie privée sur Internet

- **Bonnes pratiques par rapport à l'usage des smartphones pour protéger votre vie privée :**
  - 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.

BONNES PRATIQUES POUR AMÉLIORER LA SÉCURITÉ DE SON SMARTPHONE :

- 1. 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.
- 2. 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.
- 3. 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.

BONNES PRATIQUES POUR AMÉLIORER LA SÉCURITÉ DE SON SMARTPHONE :

- 4. Surveiller son trafic de données : Sans doute 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.
- 5. 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.

BONNES PRATIQUES POUR AMÉLIORER LA SÉCURITÉ DE SON SMARTPHONE :

- 6. Activer, si disponible, le chiffrement des données : C'est intéressant dans l'optique où si un logiciel pompe vos données, il ne pourra pas récupérer grand chose. Le chiffrement protège les informations personnelles, cette fonction existe nativement (ou par application tierce).
- Enregistrer les informations sensibles ou les notes (comme une liste de mots de passe ou des numéros de comptes) à l'aide d'une application de cryptage.
- Avant de faire réparer son appareil, réaliser une sauvegarde des données puis les effacer manuellement ou restaurer les paramètres par défaut.
- Activer la suppression automatique de tous les paramètres et de toutes les données lorsqu'une personne entre plusieurs fois un code ou un mot de passe erroné, en essayant de déverrouiller l'appareil.

BONNES PRATIQUES POUR AMÉLIORER LA SÉCURITÉ DE SON SMARTPHONE :

- 6. Activer, si disponible, le chiffrement des données : C'est intéressant dans l'optique où si un logiciel pompe vos données, il ne pourra pas récupérer grand chose. Le chiffrement protège les informations personnelles, cette fonction existe nativement (ou par application tierce).
- Enregistrer les informations sensibles ou les notes (comme une liste de mots de passe ou des numéros de comptes) à l'aide d'une application de cryptage.
- Avant de faire réparer son appareil, réaliser une sauvegarde des données puis les effacer manuellement ou restaurer les paramètres par défaut.
- Activer la suppression automatique de tous les paramètres et de toutes les données lorsqu'une personne entre plusieurs fois un code ou un mot de passe erroné, en essayant de déverrouiller l'appareil.

BONNES PRATIQUES POUR AMÉLIORER LA SÉCURITÉ DE SON SMARTPHONE :

- 8. 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.
- 9. 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.

BONNES PRATIQUES POUR AMÉLIORER LA SÉCURITÉ DE SON SMARTPHONE :

- 10. Evitez les noms d'applications douteux : les applications qui vous promettent trop ou encore les sources inconnues lors de l'installation d'applications sur votre Smartphone. C'est important car une fois l'application lancée, les droits donnés, il faut quelques minutes au logiciel espion pour envoyer toutes les données nécessaires à vous nuire. Les nouveaux terminaux mobiles de type iPhone ou Android par exemple sont, lors d'un usage normal, protégés via le système de signature et de plateforme « propriétaire » d'Apple et de Google respectivement.

Attention aux risques liés à l'utilisation des logiciels piratés.

- **Qu'est-ce que le piratage logiciel ?**
- Le piratage logiciel est l'utilisation, la copie ou la distribution non autorisée d'un logiciel soumis à des droits d'auteur. Il peut prendre différentes formes :

■ Copie illicite de logiciels achetés en toute légitimité (piratage par l'utilisateur final) ;

■ Accès illégal à un logiciel protégé (craquage) ;

■ Reproduction et/ou distribution de contrefaçons ou de logiciels non autorisés (généralement par Internet).

Attention aux risques liés à l'utilisation des logiciels piratés.

- **Qu'est-ce que le piratage logiciel ?**
- Le piratage logiciel est l'utilisation, la copie ou la distribution non autorisée d'un logiciel soumis à des droits d'auteur. Il peut prendre différentes formes :

■ Copie illicite de logiciels achetés en toute légitimité (piratage par l'utilisateur final) ;

■ Accès illégal à un logiciel protégé (craquage) ;

■ Reproduction et/ou distribution de contrefaçons ou de logiciels non autorisés (généralement par Internet).

Attention aux risques liés à l'utilisation des logiciels piratés.

- **Risques techniques d'utilisation des logiciels piratés :**
- 1. 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.
- 2. Lorsque vous utilisez la copie illicite d'un logiciel, 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.

Attention aux risques liés à l'utilisation des logiciels piratés.

- **Risques techniques d'utilisation des logiciels piratés :**
- 3. 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.
- 4. 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.

Attention aux risques liés à l'utilisation des logiciels piratés.

- **Risques techniques d'utilisation des logiciels piratés :**
- 5. En cas de problème, vous ne pouvez pas avoir recours au support technique de l'éditeur.
- 6. 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 usagee 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.

Attention aux risques liés à l'utilisation des logiciels piratés.

- **Comment se mettre à l'abri des logiciels piratés ?**
- Pour éviter d'être victime des pirates de logiciels, il est recommandé :

■ D'acheter les logiciels uniquement auprès de sociétés connues.

■ Lorsque vous faites des achats en ligne, assurez-vous que le site Web est légitime. Sur la page d'accueil du site de vente, cliquez sur l'icône de verrouillage qui apparaît sur le cadre de votre fenêtre de navigateur et affichez le certificat de sécurité.

■ Si un prix affiché semble trop attractif, méfiez-vous. Méfiez- vous également des prix extrêmement faibles et vérifiez l'authenticité du site.

L’ingénierie sociale

- Basée sur l’utilisation de la force de persuasion et l’exploitation de la naïveté des utilisateurs, cette technique permet de soutirer de l’information aux victimes sans avoir recours à l’outil informatique, mais à des moyens de communication plus “traditionnels” tels le téléphone, le courrier écrit, la messagerie instantanée et parfois même le contact direct.
- les pirates d’aujourd’hui exploitent l’abondance d’informations personnelles disponibles sur les sites de réseaux sociaux pour cibler leurs attaques sur les individus clés au sein des entreprises visées.
- L’ingénierie sociale est l’une des menaces les plus anciennes et les plus sérieuses pour les réseaux informatiques sécurisés. C’est un type d’attaque très performant dans la mesure où aucun logiciel ni matériel ne permet de s’en défendre efficacement.

L’ingénierie sociale

- **D’une manière générale les méthodes d’ingénierie sociale se déroulent selon le schéma suivant :**
- Une phase d’approche permettant de mettre l’utilisateur en confiance, en se faisant passer pour une personne de sa hiérarchie, de l’entreprise, de son entourage, d’un fournisseur, etc.
- Une mise en alerte, afin de le déstabiliser. Il peut s’agir par exemple d’un prétexte de sécurité ou d’une situation d’urgence ;
- Une diversion, c’est-à-dire une phrase ou une situation permettant de rassurer l’utilisateur et d’éviter qu’il se focalise sur l’alerte. Il peut s’agir par exemple d’un remerciement annonçant que tout est rentré dans l’ordre, d’une phrase anodine ou dans le cas d’un courrier électronique ou d’un site web, d’une redirection vers le site web légitime.

L’ingénierie sociale

- **Comment se protéger ?**
- La meilleure façon de se protéger est d’utiliser son bon sens pour ne pas divulguer à n’importe qui des informations pouvant nuire à la vie privée ou à la sécurité de l’entreprise. Il est ainsi conseillé, quel que soit le type de renseignement demandé :
- De se renseigner sur l’identité de son interlocuteur en lui demandant des informations précises (nom et prénom, société, numéro de téléphone) ;
- De vérifier éventuellement les renseignements fournis ;
- De s’interroger sur la criticité des informations demandées.