Les bonnes pratiques en sécurité de l'information

DZ-CERT
Algerian Computer Emergency Response Team

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

SOMMAIRE

PRÉAMBULE

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 sont souvent liées à l'exposition de nos données sur ce réseau. Ces 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.

L'objectif de la sécurité de l'information est triple. Le premier objectif : la confidentialité, est d'empêcher que nos données personnelles ne puissent être consultées par des personnes non autorisées. Le deuxième objectif, l'intégrité, est d'empêcher que nos données ne puissent être modifiées sans que nous ne puissions nous en rendre compte. Le troisième et dernier objectif, la disponibilité, consiste à s'assurer que nous puissions accéder à nos données quand nous en avons besoin.

De la même façon que la sécurité routière passe par la maitrise du code de la route, la sécurité de l'information résulte autant de l'attitude de l'utilisateur que des technologies qu'il emploie. A cet effet, ce guide a pour vocation d'être un recueil de bonnes pratiques pour mieux se prémunir des risques inhérents à l'usage de ces nouvelles technologies. Ces règles ne prétendent pas avoir un caractère d'exhaustivité. Elles constituent cependant le socle minimum des règles à respecter pour protéger nos informations.

1

Parents, Enfants et les Dangers d'Internet

Parents, Enfants et les Dangers d'Internet

L'augmentation fulgurante de l'accès à Internet en Algérie par les enfants ces dernières années les expose à de multiples agressions de diverses natures. Il est donc nécessaire que les parents prennent conscience de l'importance de protéger leurs enfants contre les dangers de ce nouveau moyen de communication !
Ainsi, ils doivent les accompagner mais surtout les informer des menaces qu'ils peuvent encourir dans un monde virtuel qui n'est ni plus ni moins dangereux que le monde physique. Cette partie est donc destinée aux parents, qui trouveront des conseils pratiques permettant de mieux protéger leurs enfants des dangers d'Internet.

Connaître les dangers D'Internet

- Informations non référencées, douteuses et sans valeur
- Sites portant atteinte à la morale
- Messages non sollicités envahissant les e-mails
- Invasion de la vie privée

Conseils : Parents - Enfants

L'éducation à l'Internet fait désormais partie de l'éducation en général.

Pour cela, conseillez vos enfants de :

- Ne jamais divulguer sans l'autorisation des parents des renseignements personnels : (Nom. Adresse. Numéro de téléphone. Mot de passe. Etc.).
- Ne jamais répondre à un message dont l'émetteur est inconnu.
- Ne jamais mettre la « vraie » adresse éléctronique (réservée aux parents et aux amis) lors d'une inscription dans un site web.
- Ne jamais donner le nom pour personnaliser le contenu web. Il vaut mieux créer des pseudos en ligne qui ne révèlent aucune information personnelle.
- Ne jamais accepter un rendez-vous d'un(e) « ami(e) » rencontré(e) en ligne sans prévenir les parents.
- Ne jamais répandre des rumeurs, harceler ou menacer les autres.

Toute prévention doit d'abord passer par une sensibilisation des enfants et un dialogue parents-enfants.

Ainsi, nous vous suggérons de :

- Communiquer ouvertement et de façon positive avec ses enfants sur leurs activités sur Internet. Dialoguer avec eux et créer un partage familial autour des usages de l'Internet.
- Établir une liste de règles d'utilisation d'Internet, spécifiant quel genre de sites leur est autorisé ou interdit.
- Installer l'ordinateur dans un endroit passant de la maison afin de pouvoir superviser facilement leurs activités en ligne.
- Se tenir au courant des sites Web qu'ils fréquentent et s'assurer qu'on n'y trouve ni contenus offensants, ni photos et informations personnelles.
- S'informer des sites de chat qu'ils fréquentent et à qui ils parlent.

Afin de mieux contrôler leurs activités sur Internet, il vous est conseillé de :

- Les protéger de l'apparition de publicités offensantes à l'aide d'un logiciel de blocage.
- Se servir des filtres de messageries électroniques pour bloquer les messages non sollicités ou contenant certaines expressions ou mots inappropriés.
- Utilisez des moteurs de recherche pour enfants ou ceux offrant un contrôle parental.
- Considérez les filtres Internet comme un complément de sécurité qui ne remplacent en aucun cas la supervision parentale.

2

Les dix règles de base pour sécuriser votre PC

LES DIX RÈGLES DE BASE

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.

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.

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.

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.

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.

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) : 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.

3

Le Premier reflexe d'un bon utilisateur : Bien choisir son mot de passe

Bien choisir son mot de passe

Les incidents de sécurité ont souvent pour point de départ l'acquisition par des moyens « frauduleux » de mots de passe. C'est en effet la méthode classique la plus utilisée par les intrus pour prendre le contrôle d'un système. Choisir et sécuriser son mot de passe est principalement la mesure la plus importante à entreprendre. Pour cela :

- Le mot de passe doit être assez long : une chaîne de 8 caractères au minimum. Plus un mot de passe est long, plus il est difficile à deviner.

- Augmentez le degré de complexité de votre mot de passe en combinant des lettres majuscules et minuscules et en rajoutant des chiffres et des symboles spéciaux.

- N'utilisez jamais une information personnelle comme mot de passe, telle que votre nom, prénom, prénoms de proches, votre numéro de téléphone, matricule de votre voiture, etc.

- N'utilisez jamais un mot existant dans les dictionnaires.

- Le mot de passe doit être difficile à deviner mais facile à retenir.

PROTÉGER SON MOT DE PASSE :

- Un mot de passe est une information sensible, éviter de la noter, gardez le dans votre mémoire.

- Un mot de passe est strictement personnel : ne le confiez à personne et ne le partagez pas.

- Un mot de passe doit être changé régulièrement, évitez de reprendre les anciens mots de passe déjà utilisés.

4

Bien sécuriser son réseau sans-fil Wi-Fi domestique

Bien sécuriser son réseau sans-fil Wi-Fi domestique

Le Wi-Fi (Wireless Fidelity) est une technologie permettant de créer avec aisance des réseaux informatiques sans fil. Sa portée varie de quelques dizaines de mètres à plusieurs centaines de mètres, ce qui en fait une technologie de premier choix pour le réseau domestique avec connexion internet. Elle est de plus en plus utilisée par divers matériels informatiques :
ordinateur, Assistant personnel (PDA), Smartphone, console de jeux, portable, etc. La Sécurité de ce type de réseau, souvent négligée et toujours source de problème, vient du fait qu'il est facile de monter un réseau Wi-Fi mais qu'il est un peu plus difficile de le sécuriser.
Parmi les risques liés à cette technologie, on trouve : l'écoute ou le vol d'informations personnelles, l'intrusion au réseau local, l'utilisation de la connexion Internet à l'insu de son propriétaire.
Plusieurs mécanismes existent pour assurer un niveau de sécurité acceptable, on parle toujours de filtrage d'adresse MAC, WEP, WPA, etc.

Bonnes pratiques pour sécuriser son réseau Wifi:

- **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.

- **Utiliser le chiffrement :** Le WEP (Wired Equivalent Privacy) et WPA (Wi-Fi Protected Access) sont deux possibilités pour chiffrer (donc pour protéger) 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.
Le système WPA est plus efficace que le système WEP. Privilégiez donc WPA si votre Point d'accès/carte sans fil le supporte.

• **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.

• **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.

• **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 WEP et un filtrage par adresse MAC.

WPA2 est supporté dans les nouvelles cartes/points d'accès Wi-Fi. WPA2 permet d'avoir un niveau de sécurité supérieur à celui de WPA. Il est conseillé de l'utiliser quand c'est possible.


Stat
Attn
DDR
Stat
Attn
DDR
Stat
Attn
DDR
Stat
Attn
DDR
Stat
Attn
DDR

5

Faites attention à votre boîte de messagerie électronique

FAITES ATTENTION À VOTRE BOÎTE DE MESSAGERIE ÉLECTRONIQUE

Aujourd'hui la messagerie électronique est de plus en plus utilisée et est devenue une application internet indispensable, parce que la messagerie est un vecteur de communication, de productivité et de production. Sa sécurité et sa disponibilité sont des préoccupations légitimes des entreprises.

Les canulars ou « hoax » sont des messages qui circulent sur le Net. Ces messages sont souvent inquiétants ou font appel à la solidarité des internautes. Dans tous les cas, ils les exhortent à transférer le courrier à un maximum de contacts. La conséquence : toutes ces adresses peuvent être récupérées par des «spammeurs», les expéditeurs de courriers indésirables.

Les courriers identifiés comme indésirables par votre messagerie sont automatiquement rangés dans le dossier « spams» et effacés au bout d'un laps de temps que vous pouvez paramétrer. Le spam (ou spamming, pourriel), c'est l'action d'envoyer des courriers électroniques, des emails, dans un but publicitaire ou promotionnel, qu'ils soient commerciaux ou non, et en général en grand nombre, à des personnes qui ne l'ont pas sollicité.

Il arrive que certains envois «sûrs» soient classés à tort dans cette catégorie. Pour éviter que cela se reproduise ajoutez l'adresse concernée dans la liste des «expéditeurs autorisés». L'utilisation des adresses e-mail pour l'envoi des spams contenant en général des publicités devient un acte pénible pour l'utilisateur de la boite de messagerie.

Outre les canulars et les spams, les courriers électroniques d'hameçonnage sont conçus pour usurper votre identité. Ils demandent vos données personnelles ou vous dirigent vers des sites Internet ou des numéros de téléphone où il vous est demandé de fournir des données personnelles. Ils peuvent sembler venir de votre banque ou organisme financier, d'une entreprise telle que Microsoft, ou des sites de vos réseaux sociaux.

LES BONNES PRATIQUES POUR MIEUX PROTÉGER LA BOÎTE DE MESSAGERIE

Face à ce harcèlement de messages indésirables, vous devez d'une part, suivre certaines règles pour protéger votre boite de messagerie :

• 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.

• 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.

• 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.

6

Protéger sa vie privée sur Internet

PROTÉGER SA VIE PRIVÉE SUR INTERNET

Avec l'émergence des blogs et des réseaux sociaux, le nombre d'informations personnelles accessibles en ligne augmente sans cesse. Un nouveau concept est né par analogie à notre environnement naturel, il s'agit de l'intimité numérique et le droit de préserver sa vie privée et ses données personnelles. Dans cette rubrique, nous vous proposons un ensemble de bonnes pratiques pour protéger vos données personnelles 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.

L'IDENTITE NUMERIQUE ?

« 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. Ces petits bouts d'identité fonctionnent comme des gènes : ils composent l'ADN numérique d'un individu ».

ATTENTION SUR INTERNET : TOUT SE GARDE, RIEN NE SE PERD !

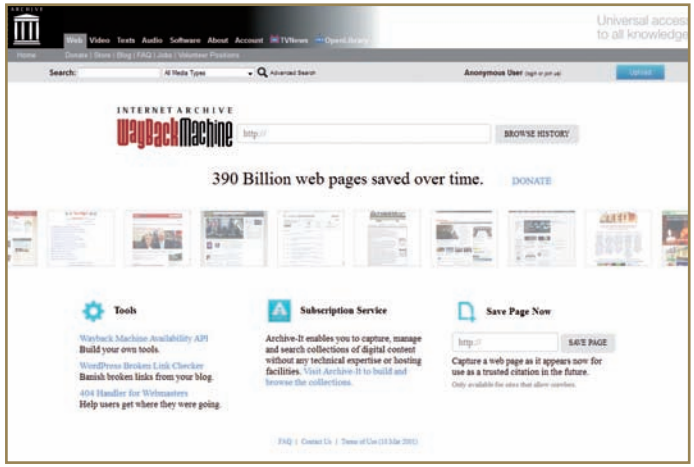
Le Web a une mémoire : toute contribution de votre part sur un site ou un forum par exemple, peut demeurer en ligne pendant des années tant que ce même site est en ligne. Il est également possible de retrouver des archives d'anciennes versions de sites.

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 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.

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 ;
- 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.

7

Téléphonie mobile : Sensibilisation et Sécurité lors de l'utilisation d'un Smartphone

SÉCURITÉ DES SMARTPHONES

La sécurité logicielle des Smartphones est devenue une préoccupation de plus en plus importante de l'informatique liée à la téléphonie mobile. Elle est particulièrement préoccupante car elle concerne la sécurité des informations personnelles disponibles au sein des Smartphones.

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.

La sécurité de ces terminaux mobiles suscite toujours beaucoup d'interrogations. Les Smartphones intègrent toutes les technologies de communication existantes, du Wifi à la 3G en passant par le Bluetooth. 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. Ils deviennent en outre de plus en plus populaires et attirent donc l'intérêt des pirates vers ces nouvelles plateformes mobiles. Il est à noter qu'Android est actuellement le système d'exploitation mobile le plus utilisé au monde. Le succès de celui-ci fait de la plateforme la cible favorite des pirates. Donc rester prudent et appliquer quelques bonnes pratiques va permettre de profiter pleinement de tous les bienfaits de cette technologie avancée. Le risque se présente quand un inconnu peut consulter nos sms, nos photos, notre agenda… Il en va de même pour les Smartphones à usage professionnel : il est peu probable que votre employeur voit d'un bon œil que n'importe qui puisse avoir accès aux documents, emails de la société, aux serveurs Exchange ou SharePoint, ou encore au réseau Wifi. Aussi, il apparait de plus en plus indispensable de protéger son téléphone contre tous les types de menaces.

A travers ces conseils, nous rappellerons à l'utilisateur quels sont les aspects importants en matière de sécurité et quels sont les moyens de protéger son appareil.

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.

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.

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.

7. 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.

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.

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.

Pour conclure, la meilleure protection reste donc la vigilance car par exemple il est plus raisonnable d'installer les applications approuvées, plutôt que celles qui ont une provenance douteuse, non pas qu'elles soient moins sécurisées, mais leur provenance n'ayant pas été approuvée officiellement, il est difficile d'avoir entièrement confiance.

De ce fait, les pirates exploitent les failles, notamment à l'aide des applications. En effet, il faut savoir que les applications non contrôlées par les plateformes officielles (Android Market, Apple Store, Blackberry App World…) ont plus de chances de contenir des malwares donc lisez les avis des personnes ayant téléchargé le logiciel (signalement de bugs ou de virus) et sachez que vous pouvez également installer un antivirus et Firewall sur le Smartphone si vous possédez des données très confidentielles.

8

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

Le piratage de logiciels est une affaire sérieuse, en plus d'enfreindre la loi et les droits de propriété intellectuelle des créateurs de logiciels, 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.

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).**

Les logiciels font partie des œuvres protégées par le code de la propriété intellectuelle. Dans ce qui suit, nous allons focaliser sur les risques techniques 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.

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.

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 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.

De même, un vendeur qui propose de violer la loi ne s'arrêtera probablement pas au piratage de logiciels. Toute donnée de carte de crédit ou information personnelle que vous communiquez peut être exploitée par des voleurs d'identité.

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.


http://www

9

L'ingénierie sociale

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. Plus intéressant encore, 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.

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.

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.

10

Méfiez-vous du Phishing

Méfiez-vous 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 ». Cette technique d'escroquerie consiste à vous subtiliser des données personnelles (mots de passe de connexion à un service, numéro de compte en banque ou de carte bancaire...) en vous piégeant avec un faux courrier électronique qui reprend le logo, la mise en page, l'adresse de votre banque, de votre fournisseur d'accès à Internet, d'un service de messagerie …etc. Le message prétexte un problème lié à votre compte et vous invite à cliquer sur un lien pour donner vos coordonnées. Vous basculez en réalité sur un faux site et ainsi l'attaquant récupère les informations saisies. Les conséquences sont diverses selon le type de renseignements que vous avez fournis. Cela va du pillage de votre compte en banque, en passant par des achats effectués avec votre numéro de carte bancaire. Autre arnaque très en vogue, l'usurpation de votre identité sur des sites de réseaux sociaux comme Facebook ou MySpace.

Quelques 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 (voire impossible) qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone !

- N'envoyez jamais vos mots de passe, identifiants de connexion ou toutes autres informations personnelles par courrier électronique. Méfiez-vous toujours des messages vous invitant à saisir des informations personnelles, même si la demande semble légitime. Si vous pensez avoir été victime de phishing en donnant vos identifiants de connexion et/ou vos mots de passe, changez vos données d'authentification au plus vite.

- 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 est affiché dans la barre d'état au bas de votre navigateur.

- Lorsque vous cliquez sur le lien d'un courriel, vérifiez, une fois le navigateur ouvert, que l'adresse du site est bien orthographiée. Les attaquants utilisent parfois la même charte graphique d'un site légitime et modifient un ou plusieurs caractères dans l'url afin de faire croire à la victime qu'elle est bien sur le site sollicité.

11

Sécuriser son compte facebook et protéger sa vie privée

Sécuriser son compte facebook et protéger sa vie privée

Facebook est un réseau social sur Internet permettant de publier des informations de tout type (photos, vidéos, documents, textes, etc) mais aussi à créer des groupes et des pages pour faire connaitre des institutions, des entreprises ou des causes variées.

Toutes ces informations publiées peuvent être consultées par n'importe quel internaute ayant un compte ou des fois sans qu'il soit nécessaire d'en avoir un, et aussi par facebook qui peut les utiliser dans différents domaines (publicité, politique, études psychologiques ou comportementale,…)

A la création d'un compte, il est nécessaire de suivre les règles de sécurité suivantes :

1. Régler les paramètres de sécurité

Aller à :
Accueil>Paramètres du Compte>Sécurité :

- Créer une question secrète qui confirmera votre identité.
- Activer la navigation sécurisée avec https.
- Activer la notification lors des connexions pour être averti lorsque votre compte est utilisé à partir d'un ordinateur ou d'un appareil que vous n'avez pas encore utilisé.

2. Créer des listes d'amis

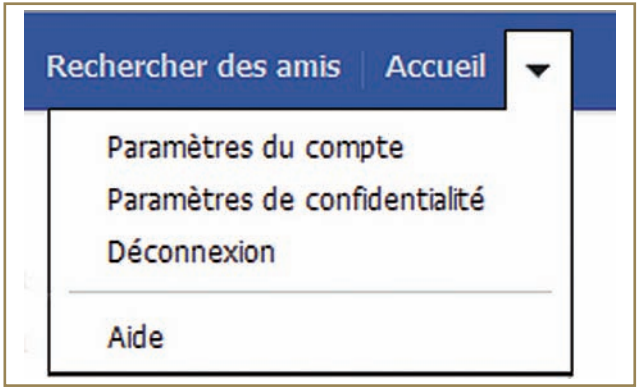
C'est ce qui vous permettra par la suite de choisir qui pourra voir quoi. Vous pouvez restreindre l'accès à votre profil à différents types de personnes (amis, amis des amis, ...). Il est aussi possible de séparer vos contacts en différentes listes (professionnelle, personnelle) et vous pouvez ainsi ajuster les paramètres selon vos relations avec ces personnes.

3. Régler les paramètres de Confidentialité

Les paramètres de Confidentialité permettent de rendre son compte inaccessible au grand public. Seules vos connaissances pourront accéder et voir vos informations personnelles et vos connaissances. Pour régler les paramètres de sécurité et choisir qui aura accès à quelles informations, allez a : Accueil>Paramètres de Confidentialité>Personnalisé.
Vous pourrez ensuite choisir, pour chaque élément de votre page, les personnes qui pourront y accéder. Vous pouvez également personnaliser toute information, et restreindre l'accès en fonction de ce que vous souhaitez divulguer.

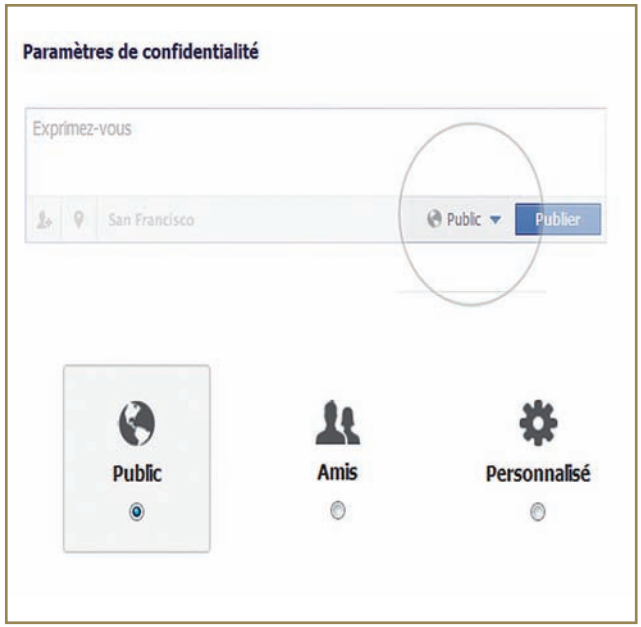
4. Prise de Contact

Contrôlez la façon dont vous entrez en contact avec les personnes que vous connaissez : Accueil>Paramètres de confidentialité>Prise de contact



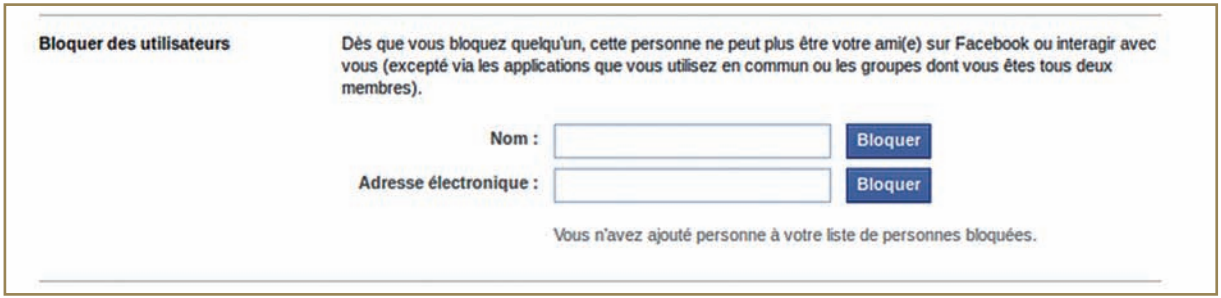
5. Contrôlez la confidentialité de ce que vous publiez

Vous pouvez gérer la confidentialité des mises à jour de votre statut, des photos et des informations en utilisant le sélecteur d'audience, lorsque vous publiez ou après. Rappelez-vous : les personnes avec qui vous partagez peuvent toujours partager vos informations avec d'autres, y compris les applications.



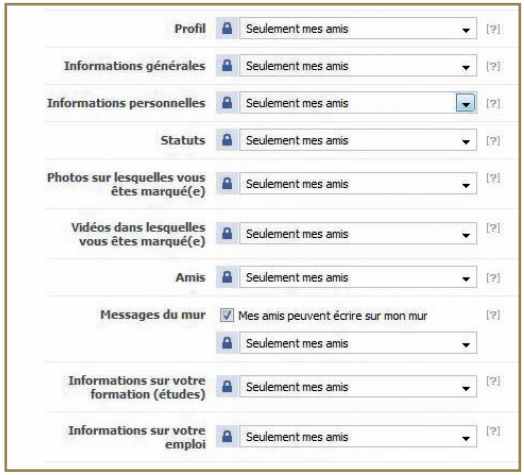
6. Bloquer des utilisateurs

Pour différentes raisons, vous pouvez souhaiter qu'une personne en particulier ne puisse pas accéder à votre profil. Dans ce cas, rendez-vous dans la rubrique Paramètres de confidentialité>Personnes et applications bloquées>Gérer le blocage, et inscrivez son nom.



7. Ne pas faire apparaître sa photo de profil sur les publicités du site

Facebook utilise les photos de profil de ses membres pour illustrer ses publicités. Pour éviter tout désagrément lié à cette utilisation, rendez-vous dans Paramètres du compte>Publicités Facebook.



12

Les bonnes pratiques en cas d'incident sur un système d'information

LES BONNES PRATIQUES EN CAS D'INCIDENT SUR UN SYSTÈME D'INFORMATION

Aujourd'hui, aucune personne ou organisation n'est à l'abri des incidents de sécurité. Bien que des mesures pour assurer la sécurité du système d'information sont mises en place, il peut arriver que cette sécurité soit compromise par des attaques informatiques. Un plan de réponse aux incidents de sécurité doit faire partie intégrante de la stratégie de sécurité globale de l'entreprise pour se préparer /réagir aux incidents.

▪ Préparation

L'étape de préparation est sans aucun doute la plus importante puisque c'est durant celle-ci que s'élabore l'équipe qui intervient lors des incidents ainsi que les procédures qui vont permettre de traiter rapidement et efficacement les incidents qui peuvent affecter le système d'information. Il est également important de disposer des sauvegardes à jours des données critiques.

▪ Identification

Tout d'abord, il faut procéder à l'examen du système pour mettre en évidence les comportements suspects et les signaler aux personnes appropriées (le responsable de la sécurité et de la hiérarchie). Certains signes indiquent que le système a peut-être été

Figure 1 : Processus de gestion d'incidents de sécurité

Ce document propose les étapes à suivre pour mieux gérer les incidents de sécurité. Un petit conseil avant de commencer : « PAS DE PANIQUE! » Concentrez-vous pour éviter de faire des erreurs d'inattention.

compromis. Ils peuvent être recherchés systématiquement par des outils de détection d'intrusion, mais peuvent également être remarqués ponctuellement par : l'analyse des fichiers de journalisation, les programmes en cours d'exécution et les tâches planifiées, les programmes configurés pour être exécutés automatiquement au démarrage du système, les détails de la configuration réseau, les paramètres DNS et ARP, les connexions et les sessions et ports ouverts, les comptes des utilisateurs et leurs privilèges et les fichiers inhabituels laissés par l'intrus.

▪ Confinement des dommages

Après avoir identifié l'incident sur le système, la première action à faire est de limiter l'extension de l'incident. Il s'agit d'isoler les

machines infectées et protéger les machines saines. Une combinaison appropriée des actions suivantes peut être adoptée selon la nature de l'incident :

- Déconnecter la machine compromise du réseau. En revanche, il faut maintenir la machine sous tension et ne pas la redémarrer pour ne pas perdre des informations nécessaires à l'analyse de l'incident.
- Modifier les règles de filtrage d'un pare-feu ou d'un routeur.
- Désactiver le service concerné par l'attaque.
- Désactiver les comptes utilisateurs suspects.
- Changer les mots de passes.

La deuxième action à faire consiste à préparer une copie de sauvegarde du système pour une investigation numérique. Cette analyse permettra de comprendre la nature de l'incident et les vulnérabilités exploitées. Enfin, décider si le système sera nettoyé ou réinstallé à partir d'une version saine.

▪ Éradication

D'une manière générale, il est recommandé de réinstaller entièrement le système afin de s'assurer qu'une machine ne possède plus de porte dérobée ou autre modification laissée par l'intrus. Restaurer les données et les applications affectées à partir des sauvegardes (étape 1). Ensuite, valider la sécurité du système avec un scanner de vulnérabilités et corriger les vulnérabilités identifiées avant de remettre le système en production.

▪ Retour à la normale

Mettre le système nouvellement reconstruit en production et maintenir une surveillance sur ce système afin de détecter d'éventuels futurs incidents.

▪ Tirer des leçons

Rédiger un rapport décrivant l'incident et ce qui a été fait pour le traitement de cet incident. Enfin, identifier les améliorations à apporter au système d'information.

© CERIST 2015

CENTRE DE RECHERCHE SUR L'INFORMATION SCIENTIFIQUE ET TECHNIQUE
5, Rue des Trois Frères Aissou, Ben - Aknoun - BP 143. 16030 - Alger
Tél : +213 (21) 91 62 05 - 08 / Fax : +213 (21) 91 21 26
www.cerist.dz