LES BONNES PRATIQUES EN SÉCURITÉ DE L'INFORMATION

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 !

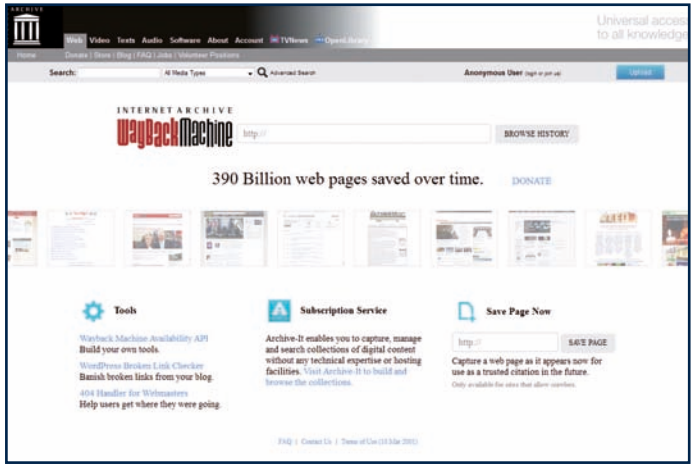
Le Web a une mémoire : toute contribution de votre part sur un site ou un forum par exemple, peut demeurer en ligne pendant des années tant que ce même site est en ligne. Il est également possible de retrouver des archives d'anciennes versions de sites.

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

Attention aux ransomwares !

Ces dernières années, une nouvelle technique d'attaque est utilisée par les pirates mettant ainsi la victime et ses données dans une situation critique. Le but est d'empêcher l'utilisateur d'accéder à ses appareils en demandant une rançon pour lever ce blocage, il s'agit des ransomware.

Qu'est-ce qu'un ransomware ?

Les ransomware ou rançongiciels sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des victimes et réclament le paiement d'une rançon.

Il existe trois types de ransomware en circulation :

1. Encrypting ransomware, qui intègre des algorithmes de chiffrement avancés. Il est conçu pour bloquer les fichiers système et exiger le paiement pour fournir à la victime la clé qui peut décrypter le contenu bloqué (CryptoLocker, Locky, CrytpoWall, ...).

2. Locker ransomware, qui bloque l'accès au système d'exploitation, ce qui rend impossible d'accéder au bureau et aux applications ou aux fichiers. Les fichiers ne sont pas cryptés dans ce cas, mais les attaquants demandent toujours une rançon pour déverrouiller l'ordinateur infecté (police-themed ransomware ou Winlocker ..)

3. Une autre version est le ransomware **Master Boot Record** (MBR). Quand le ransomware de MBR frappe, le boot process ne se termine pas et affiche à l'écran une demande de rançon (Satana et Petya).

PRINCIPALES CIBLES POUR LES CRÉATEURS ET LES DISTRIBUTEURS DE RANÇONS

Les utilisateurs particuliers, pourquoi ?

- Parce qu'ils n'ont pas de sauvegardes de données;
- Parce qu'ils ont peu ou pas d'éducation en matière de cybersécurité ;
- Parce qu'ils manquent de protection de base;
- En raison du nombre d'utilisateurs d'internet (plus de PC infectés = plus d'argent).
- Parce que le gain est important ;
- Parce que les attaquants savent qu'ils peuvent causer des perturbations importantes dans les affaires, ce qui augmentera leurs chances d'être payé;
- Parce qu'ils peuvent affecter non seulement les ordinateurs, mais aussi les serveurs et les systèmes de partage de fichiers sur le cloud.

Les institutions publiques, pourquoi ?

- Parce qu'elles gèrent d'énormes bases de données d'informations personnelles et confidentielles que les cybercriminels peuvent vendre;
- Parce que le personnel n'est pas formé pour détecter et éviter les cyberattaques.

Comment se propagent les Ransomware ?

Les Ransomware se propagent par tous les moyens disponibles. Les cybercriminels cherchent simplement la manière la plus simple d'infecter un système ou un réseau et d'utiliser une porte dérobée pour diffuser le contenu malveillant.

Néanmoins, les méthodes les plus courantes sont :

- Le courrier contenant des liens malveillants ou des pièces jointes
- Les exploits de sécurité dans les logiciels vulnérables;
- Le trafic Internet redirigé vers des sites Web malveillants;
- Sites Web légitimes qui ont un code malveillant injecté dans leurs pages Web;
- Les messages SMS (qui s'appliquent aux rançons qui ciblent les appareils mobiles);
- Botnets;
- Auto-propagation (diffusion d'un ordinateur infecté à un autre);

BIEN QUE LA PHASE D'INFECTION SOIT LÉGÈREMENT DIFFÉRENTE POUR CHAQUE VERSION DE RANSOMWARE, LES ÉTAPES CLÉS SONT LES SUIVANTES :

1. **Au départ, la victime reçoit un courrier électronique contenant un lien malveillant ou un fichier malveillant.**
2. **Si la victime clique sur le lien ou le télécharge et ouvre la pièce jointe, un gestionnaire de téléchargement sera placé sur le PC affecté.**
3. **Le gestionnaire de téléchargement utilise une liste de domaines ou de serveurs C & C contrôlés par des cybercriminels pour télécharger le programme du Ransomware sur le système.**
4. **Le serveur C & C contacté répond en renvoyant les données demandées, dans ce cas, le ransomware.**
5. **Le ransomware commence à chiffrer le contenu entier du disque dur, les fichiers personnels et les informations sensibles. Tout, y compris les données stockées dans des comptes cloud (Google Drive, Dropbox) synchronisés sur le PC. Il peut également crypter des données sur d'autres ordinateurs connectés au réseau local.**
6. **Un avertissement s'affiche à l'écran avec des instructions sur la façon de payer pour avoir la clé de décryptage.**

Conseils pour garder votre système à l'abri de Ransomware

1. Ne pas stocker les données importantes uniquement sur le PC.

2. Avoir deux sauvegardes des données: sur un disque dur externe et dans le cloud.

3. Le Dropbox / Google Drive / OneDrive / etc. ne doivent pas être activés par défaut.

4. Le système d'exploitation et les logiciels utilisés doivent être à jour.

5. Ne pas utiliser de compte « administrateur » pour un usage quotidien.

6. Désactiver les macros dans la suite Microsoft Office

7. Supprimer les plugins des navigateurs ou les activez au besoin.

8. Ajuster les paramètres de sécurité et de confidentialité des navigateurs.

9. Supprimer les plugins obsolètes et les add-ons des navigateurs.

10. Utiliser un bloqueur d'annonce pour éviter la menace d'annonces potentiellement malveillantes.

11. Ne jamais ouvrir de courriers indésirables ou d'emails provenant d'expéditeurs inconnus.

12. Ne jamais télécharger des pièces jointes de courriers indésirables ou de courriers suspects.

13. Ne jamais cliquer sur les liens dans les courriers indésirables ou les courriers suspects.

14. Utiliser un antivirus fiable.

15. Avoir une solution de filtrage du trafic qui peut fournir une protection proactive anti ransomware.

Comment récupérer vos données sans payer de rançon

Il y a des centaines de types de ransomware, mais les chercheurs en cyber sécurité travaillent sans cesse pour briser le chiffrement que certains utilisent. Malheureusement, la plupart se sont révélées irréductibles jusqu'à présent. Malgré cela, il existe de nombreux algorithmes de cryptographie qui ne sont pas bien codées et que les spécialistes ont réussi à craquer.

11

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.

12

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

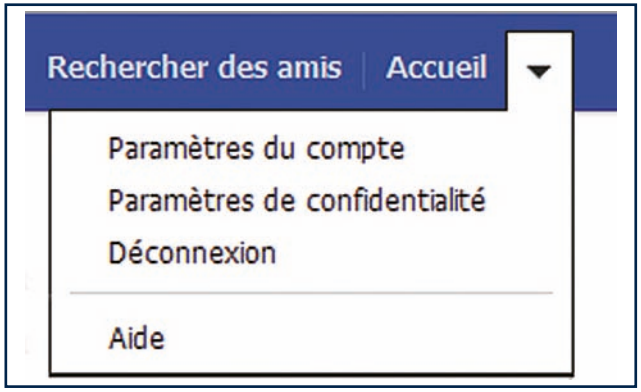
C'est ce qui vous permettra par la suite de choisir qui pourra voir quoi. Vous pouvez restreindre l'accès à votre profil à différents types de personnes (amis, amis des amis, ...). Il est aussi possible de séparer vos contacts en différentes listes (professionnelle, personnelle) et vous pouvez ainsi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

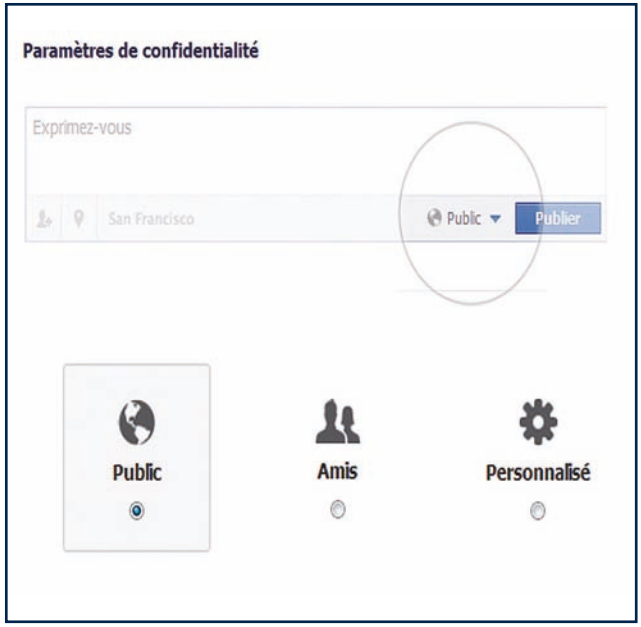
4. Prise de Contact

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



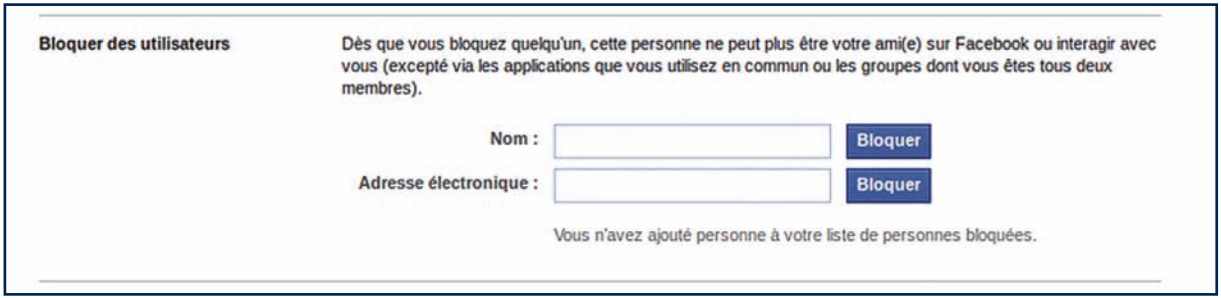
5. Contrôlez la confidentialité de ce que vous publiez

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.



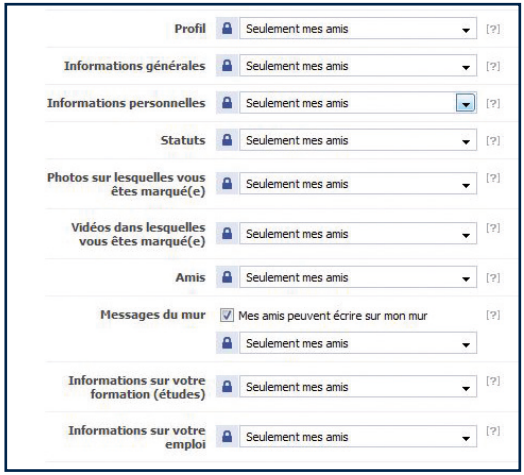
6. Bloquer des utilisateurs

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.



13

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 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.

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.

▪ 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.

14

Les Bonnes pratiques pour un serveur web sécurisé

LES BONNES PRATIQUES POUR UN SERVEUR WEB SÉCURISÉ

Diverses attaques de piratage de grande envergure ont démontré que la sécurité web reste le problème le plus critique pour toute entreprise qui exerce ses activités en ligne. Les serveurs Web et en raison des données sensibles qu'ils hébergent habituellement sont l'un des visages publics les plus ciblés d'une organisation. Sécuriser un serveur web est aussi important que la sécurisation du site ou d'une application Web elle-même et du réseau qui l'entoure. Si vous avez une application Web sécurisée et un serveur Web non sécurisé, ou vice versa, votre entreprise court un risque énorme. La sécurité de votre entreprise est son point fort comme étant son maillon le plus faible. Voici une liste des tâches que l'on doit suivre lors de la sécurisation d'un serveur Web.

1. Suppression des services inutiles

L'installation du système d'exploitation par défaut et sa configuration, ne sont pas sécurisés. Dans une installation par défaut, de nombreux services réseau qui seront inutiles dans une configuration serveur Web sont installés. Plus il y a des services fonctionnant sur un système d'exploitation, plus y aura des ports ouverts, laissant ainsi des portes ouvertes pour les utilisateurs malveillants. Désactiver les services inutiles libérera des ressources matérielles et rendra votre serveur plus performant.

2. Accès à distance

Les administrateurs des serveurs Web doivent se connecter localement. Si l'accès à distance est nécessaire, il faut s'assurer que la connexion est réalisée correctement, à l'aide de protocoles de tunneling et de chiffrement (TLS ,SSH). L'accès à distance doit également être limité seulement à des comptes et un nombre d'adresses IP spécifiques. Il est également très important de ne pas utiliser des ordinateurs publics ou des réseaux publics pour accéder aux serveurs d'entreprise à distance.

3. Séparer les environnements développement, test, et production

Comme il est plus facile et plus rapide pour un développeur de développer une nouvelle version d'une application Web sur un serveur de production, il est assez fréquent que le développement et le test d'applications web se font directement sur le serveur de production. Et comme ces applications web sont dans leurs premiers stades de développement, ils ont tendance à avoir un certain nombre de vulnérabilités, ce qui peut facilement être découvert et exploité par un utilisateur malveillant, en utilisant des outils disponibles gratuitement sur Internet. Idéalement, le développement et le test des applications Web doivent toujours être effectués sur des serveurs isolés d'internet, et ne devraient jamais utiliser ou se connecter à des bases de données réelles.

4. Contenu Web et scripts côté serveur

Les fichiers de site Web et les scripts doivent toujours être sur une partition autre que celle du système d'exploitation, des logs et tout autre fichier système. Puisque les expériences montrent que les pirates, ayant obtenu un accès au répertoire racine du serveur web, ont été en mesure d'exploiter d'autres vulnérabilités, et ont réussi à aller plus loin et d'élever leurs privilèges. Ils peuvent ainsi exécuter n'importe quelle commande du système d'exploitation, ce qui entraîne un contrôle complet du serveur web.

5. Permissions et privilèges

Les permissions sur les fichiers et les services réseau jouent un rôle essentiel dans la sécurité du serveur web. Attribuer le minimum de privilèges nécessaires pour le fonctionnement d'un service réseau spécifique. Il est également très important d'attribuer le minimum de privilèges aux utilisateurs pour accéder au site Web, et à toutes les données cotés serveur.

6. Correctifs de sécurité à jour

Un logiciel entièrement mis à jour ne signifie pas nécessairement que votre sevrveur est totalement sécurisé, il est toujours très important de mettre à jour votre système d'exploitation et tout autre logiciel fonctionnant sur votre machine avec les derniers correctifs de sécurité. Jusqu'à aujourd'hui, des incidents de piratage continuent à se produire à cause des serveurs et logiciels non mis à jour.

7. Les comptes d'utilisateurs

Lors de l'installation d'un système d'exploitation, des comptes utilisateurs inutilisés sont créés, ceux-ci doivent être vérifiés en leur affectant les autorisations nécessaires. Le compte administrateur doit être renommé et ne doit pas être utilisé. Chaque administrateur accédant au serveur Web doit disposer de son propre compte utilisateur, avec les privilèges adéquats nécessaires. Une bonne pratique en matière de sécurité est de ne pas partager les comptes utilisateurs.

8. Désactiver les modules inutilisés

Lors de l'installation d'un serveur web, un certain nombre de modules prédéfinis est activé, et ne sont jamais utilisés pour un serveur Web. Désactiver ces modules pour prévenir les attaques qui les ciblent. Par exemple le serveur Web de Microsoft (IIS) est configuré par défaut pour servir un grand nombre de types d'applications, (ASP, ASP.NET,...). La liste des extensions ne doit contenir que celles qui seront utilisées par le site ou l'application Web.

9. Utiliser les outils de sécurité fournis avec le serveur Web

Les éditeurs de serveurs web publient des outils pour aider les administrateurs à sécuriser l'installation des serveurs Web, on peut citer du coté de Microsoft l'outil URL scan. Aussi pour Apache un module appelé mod_security est fourni pour ce but. Bien que la configuration de ces outils est un processus fastidieux et peut prendre du temps, surtout avec des applications Web personnalisées, ils ajoutent un peu plus de sécurité et de tranquillité à l'esprit.

10. Surveiller et auditer votre serveur

Tous les logs de services réseau, d'accès au site Web, de serveur de base de données (Microsoft SQL Server, MySQL, Oracle,..) , et ceux du système d'exploitation doivent être surveillés et contrôlés fréquemment. Les fichiers logs ont tendance à donner toutes les informations sur une tentative d'attaque, et même d'une attaque réussie, mais la plupart du temps celles-ci sont ignorées.

11. Rester informé

Aujourd'hui, des informations et des conseils sur le système d'exploitation et les logiciels utilisés peuvent être trouvés gratuitement sur Internet. Il est très important de rester informé à propos des nouvelles attaques et les nouveaux outils, en lisant des revues liées à la sécurité (hakin9, MISC,..), la souscription aux newsletters (Deny All, CIV,..) forums ou tout autre type de communauté.

12. Utiliser des scanners

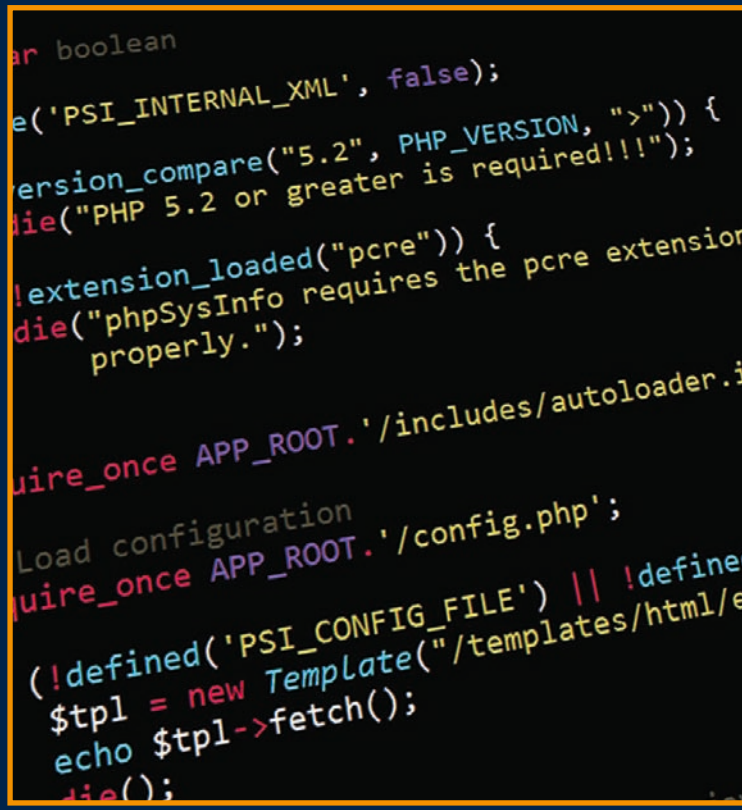
Les scanners sont des outils pratiques qui aident à automatiser et faciliter le processus de sécurisation d'un serveur et application web. Livrés souvent avec un scanner de port, scanner de sécurité réseau, vérificateur d'injection SQL, XSS, vérificateurs de problèmes de configuration, et d'autres outils très utiles pour se prémunir d'avantage.


ga.async = true;
ga.src = ("https:" == document.location.protocol
var s = document.getElementsByTagName("script")[0];
s.parentNode.insertBefore(ga, s);
})();
</script>
<?php
if (is_singular() && get_option("thread_comments")) {
wp_enqueue_script("comment-reply");
}
?>
<?php wp_head(); ?>
</head>
<body <?php body_class(); ?>>

<h1>
<?php if (is_front_page() && $paged < 2) : ?>
<img src="<?php bloginfo("template_url"); ?>/images/logo.png"
<?php else : ?>
<a href="/" title="Root"><img src="<?php bloginfo("template_url");
<?php endif;?>

15

Protéger son site web des attaques Sql Injection



PROTÉGER SON SITE WEB DES ATTAQUES SQL INJECTION

Les attaques de type injection sont considérées comme l'une des attaques les plus critiques. Dans les documents OWASP TOP10 des années 2007, 2010 et 2013, ce type d'attaque occupe toujours les toutes premières positions.

Une injection SQL fait en général référence à une attaque qui cible les applications web qui interagissent dynamiquement avec une source de donnée, dans le cas usuel, une base de données.Cette attaque est réalisée en injectant du code SQL dans une entrée utilisateur dans le but de former une nouvelle requête SQL et qui est non prévue par le programmeur. Cela permet à un attaquant de récupérer des données sensibles à partir de la base de données (récupérer des mots de passe par exemple).

Une telle attaque cible une faille dans une application web. Ce type de faille peut exister si les entrées utilisateur (formulaires, URL ou tout entête HTTP) ne sont pas filtrées correctement et sont utilisées comme paramètres pour récupérer des informations à partir de la base de données.

Exemple de faille : page d'authentification

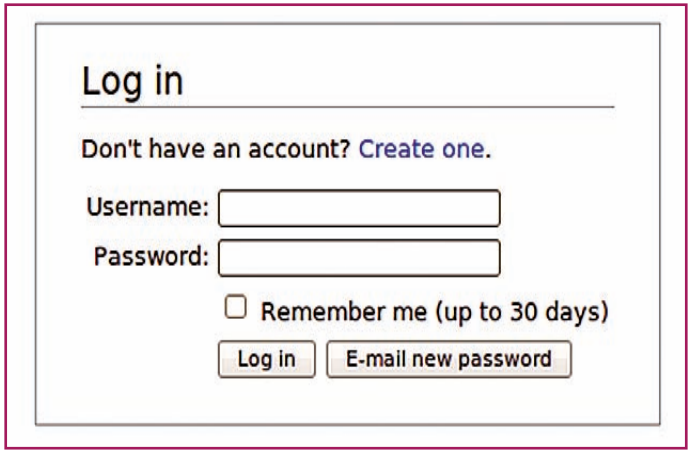
```php
<?php

...

mysql_connect(...);
mysql_select_db(...);

...

//récupération des paramètres
$utilisateur=$_POST['user'] ;
$password   =$_POST['password'] ;

//construction de la requête SQL
$requete='SELECT * FROM user WHERE user='. $utilisateur . 'AND password='. $password ;

//exécution de la requête
$result = mysql_query($requete);
...

?>
```

Nous illustrons un exemple de faille par une page d'authentification. Cette page contient deux champs : le champ utilisateur et le champ mot de passe. Ces deux données sont passées à un code PHP qui va vérifier leur légitimité par rapport à une base de données :

texte :
< ?php
…
mysql_connect(…);
mysql_sqlectdb(..) ;
…
//récupération des paramètres

```
$utilisateur=$_POST[‘user’] ;
$password=$_POST[‘password’] ;
//construction de la requête SQL
$requete=’SELECT * FROM user WHERE user=’. $utilisateur . ‘AND password=’. $password ;
//exécution de la requête
mysql_query($requete) ;
…
?>
```

Ici, la requête SQL est construite à partir des données envoyées par le formulaire. Aucune modification ou traitement sur ces données n’est effectué.



Exemple d’exploitation : contournement du mécanisme d’authentification

Le code précédent contient une vulnérabilité de type SQL injection. Les paramètres du formulaire sont envoyés tels quels. L’attaquant peut injecter du code SQL dans l’un des champs du formulaire. Il peut par exemple insérer:

Utilisateur : admin
Mot de passe : ‘ or 1=1 --
La requête devient après construction :
SELECT * FROM user WHERE user=’admin’ AND password=’’ or 1=1 --

La condition sur le mot de passe est toujours évaluée à vraie. L’attaquant peut donc se connecter avec l’identifiant admin sans vraiment connaître le mot de passe.

Classification des injections SQL :

Outre l'exemple précédent, plusieurs variantes des attaques
par injection SQL existent, elles peuvent être classées comme suit :

Tautologies : le principe ici est d'injecter un code pour que les instructions conditionnelles soient toujours évaluées à vraie (exemple du contournement du mécanisme d'authentification).

Requête avec union : le but est d'exploiter un paramètre de la requête pour extraire des données d'une table (autre que celle normalement utilisée dans la requête).

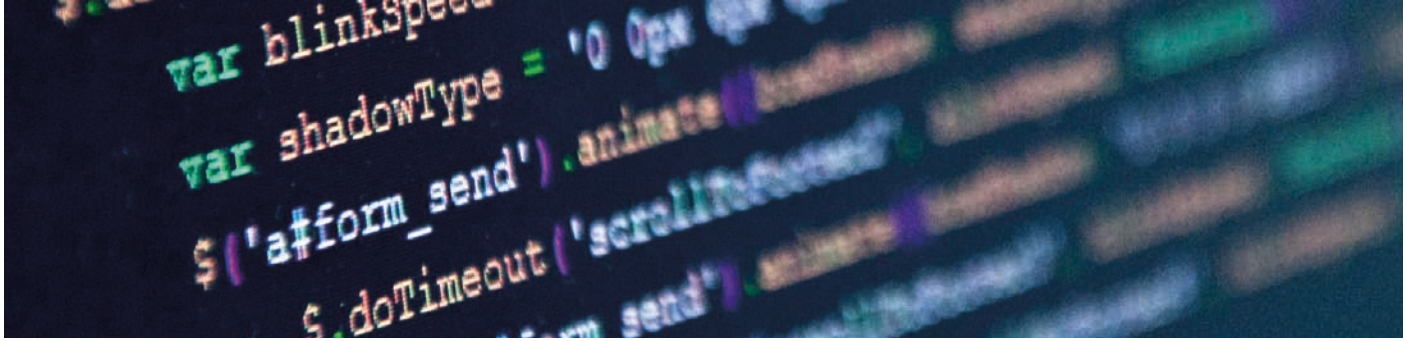
Requête Piggy-Backed : l'attaquant essaie avec ce type d'attaque d'injecter une nouvelle requête sans modifier la requête originale.

Requête incorrecte : elle consiste à causer intentionnellement une erreur dans la requête afin de récolter des informations importantes sur le système, l'application web ou la base de données.

Procédures stockées : le principe est d'exécuter les procédures stockées fournies par le SGBD. Dans les SGBD modernes, ces procédures permettent même l'interaction avec le système d'exploitation.

Inférence : consiste à modifier la requête pour simuler un mécanisme de réponse vrai ou faux. Comme le site ne retourne aucun message, l'attaquant doit observer le changement des pages du site web afin d'en déduire la réponse.

Encodage alternatif : est utilisé conjointement avec les autres techniques. Son but principal étant d'éviter la détection par les mécanismes de défense existants.



Techniques de protection :

Plusieurs techniques existent pour mitiger le risque des attaques par injection SQL.
Leur utilisation est grandement recommandée voir même obligatoire. Il est très important de prendre l'habitude de les utiliser notamment pour les développeurs.

Les procédures stockées : en utilisant cette technique, les données entrées par l'utilisateur sont transmises comme paramètres, sans risque d'injection.

Les expressions régulières : utiliser ces dernières permet de s'assurer que les données entrées par l'utilisateur sont bien de la forme souhaitée.

Principe moindre privilège : utiliser le principe du moindre privilège afin de limiter les droits des utilisateurs de l'application web ainsi que ceux de la base de données et ainsi limiter les risques ou les dégâts en cas d'intrusion.

Les requêtes paramétrées : en utilisant une requête paramétrée, c'est le SGBD qui se charge d'échapper les caractères selon le type des paramètres.

Les fonctions d'échappement : utiliser les fonctions d'échappement (exemple des fonctions mysql_real_escape_string et addslashes dans PHP) afin de filtrer les caractères spéciaux.


JOOMLA

16

Conseils pour utiliser Joomla ! en toute sécurité

CONSEILS POUR UTILISER JOOMLA ! EN TOUTE SÉCURITÉ

Un bon contrôle de sécurité est le meilleur moyen de renforcer efficacement la sécurité d'un site web. Joomla !, est un CMS Open Source, qui compte une communauté algérienne assez importante et de nombreux sites .DZ sont réalisés avec ce dernier. Cette rubrique contient une liste de conseils, qui vous permettront de faire un tour d'horizon sur ce qu'il est possible de faire afin d'optimiser la sécurité de son site Joomla! à lire donc et à appliquer bien sur pour une meilleure protection.

1. Téléchargez Joomla! du site officiel

Ne téléchargez jamais Joomla! à partir de sites non officiels, utilisez plutôt les fichiers d'installation téléchargés des sites JoomHYPERLINK **« http://www.joomla.fr/» «http://www.joomla.fr/» a.fr et Joomla.org.**

2. Installez la dernière version

Démarrez sur une base saine en installant la dernière version stable de **« http://www.joomla.org/download.html » Joomla « http://www.joomla.org/download.html »** ! à télécharger comme mentionné précédemment depuis le site officiel.

Pourquoi ? En n'utilisant pas la dernière version stable de Joomla! Votre site est une cible potentielle pour les pirates exploitant des failles de sécurité connues de la version antérieure.

3. Mettez Joomla! régulièrement à jour

La mise à jour régulière du CMS Joomla! est indispensable pour la sécurité du site. L'équipe Joomla! fournit régulièrement des mises à jour qui comprennent des correctifs de sécurité, mises à jour des composants, modules et plug-ins. Il est donc fortement recommandé d'installer la dernière version mais la tenir à jour. Aussi, il est conseillé de mettre à jour les extensions tierces également. De plus, depuis sa version 2.5, la mise à jour du CMS et ses extensions

compatibles se fait en un simple clic. Avant de faire une mise à jour, pensez à faire une sauvegarde.

4. Sauvegarde, Sauvegarde, Sauvegarde (Effectuez des backups réguliers)

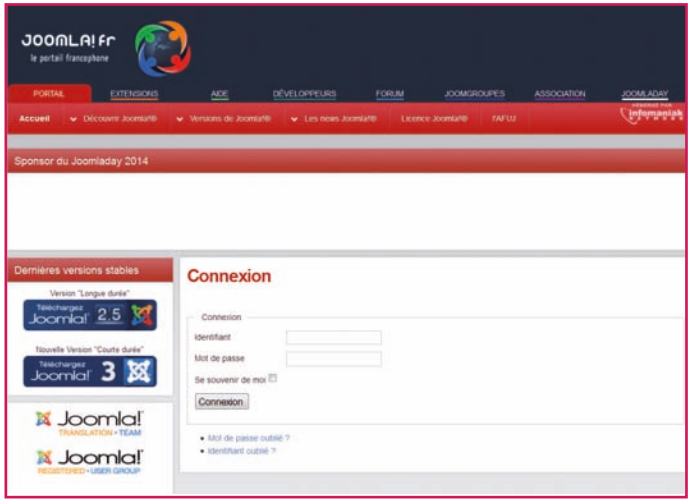
« Mieux vaut prévenir que guérir ! », il est important d'effectuer des backups réguliers : du site et de la base de données. Pensez également à tester les backups que vous planifiez, et stockez-les en lieu sûr. Même si votre site est attaqué, si vous faites des sauvegardes régulières de votre site vous pourrez, dans la grande majorité des cas, le restaurer.

D'une manière générale, vous devez sauvegarder régulièrement votre site. Vous devez le sauvegarder avant et après avoir installé, désinstallé ou mis à jour une extension ou avant et après avoir fait la mise à jour de Joomla! lui-même. Vous devez faire une sauvegarde après avoir créé du contenu. Vous devez faire une sauvegarde avant et après avoir apporté des modifications et surtout, vous devez faire une sauvegarde avant de faire toute intervention dont vous n'êtes pas certain du résultat.

5. Personnalisez le Login et Le Mot de passe

Pendant l'installation de Joomla!, l'identifiant admin est attribué par défaut à l'administrateur du site. La totalité des attaquants et les robots cracker attendent à ce que le nom d'utilisateur de l'administrateur est admin, avec cela la conséquence est qu'un pirate possède déjà une des deux clés pour accéder à votre back office. Il est recommandé de le modifier par un autre identifiant pour vous garantir plus de sécurité.

Pour le mot de passe, il faut choisir des mots de passe solides. Evitez tous les mots simples, votre nom, votre prénom, votre date de naissance, utiliser plutôt des chiffres, caractères spéciaux et lettres en majuscule/minuscule....



6. Protégez le répertoire /administrator

D'origine, Joomla! utilise le répertoire « /administrator » situé à sa racine comme dossier d'administration. Dès lors, il n'est plus un secret pour personne que la page de connexion au back office se situe à l'adresse suivante : http://www.monsite.dz/administrator. Plusieurs solutions s'offrent à vous pour protéger cette page un peu plus convenablement :

- Une protection par IP via .htacess
- Une protection par mot de passe via .htpasswd
- De nombreux plugins et autres solutions tierces pour Joomla! permettent notamment
- de renommer ce dossier, ou d'y ajouter une clé spécifique…

7. Modifiez le préfixe des tables

L'une des recommandations officielles Joomla!, est la modification du préfixe par défaut des tables de votre base de données, pendant l'installation du CMS, il vous propose « jos_ » comme préfixe par défaut, n'hésitez pas à le modifier et utiliser un préfixe de votre choix. En conservant le préfixe « jos_ » connu de tous, vous facilitez l'accès aux pirates désireux d'exploiter les données de votre base.

8. Utilisez des extensions utiles pour la sécurité

Installer un Plugin pour renforcer la sécurité de votre site Joomla! à différents niveaux. Exemple: sentinelle, AdminTools et jSecure Authentication, Akeeba, JMonitoring …

9. Installer des extensions de confiance

Joomla! permet d'étendre ses fonctionnalités à travers des extensions développées par des développeurs tiers dont une partie ne se soucie pas beaucoup de la sécurité, prenez l'habitude de télécharger les extensions à partir du site officiel.
Vous ne devez installer sur votre site que les extensions utiles à son fonctionnement. Beaucoup de débutants installent des extensions pour les tester. Avant d'installer une extension sur votre site, assurez-vous qu'elle sera utile, qu'elle réponde à vos besoins, et installez-la sur un site de tests au préalable afin de l'essayer. Si vous avez sur votre site des extensions inutiles, désinstallez-les.
Savez-vous que chaque extension installée sur un CMS (Joomla! et autres) peut nuire à la sécurité de votre site ? Car chacune d'elle demande de la maintenance donc elle augmente le risque de faille, ainsi chaque extension non à jour est une porte d'entrée pour les attaquants. Vous pouvez également consulter la « Vulnerable Extensions List » qui référence toutes les extensions Joomla! vulnérables.

10. Respectez les permissions des fichiers et répertoires

Vous avez parfois besoin de modifier les fichiers et dossiers de votre site Joomla!, avant de toucher à ces droits, soyez certain de ce que vous faites et/ou demandez conseil à votre hébergeur. Limitez les permissions sur les fichiers et les répertoires, appliquez le principe des « Moindres privilèges ». Pour une question simple de sécurité, ces droits ne doivent JAMAIS être en 777 car un fichier avec permission 777 est lisible, modifiable et exécutable par tous (sauf sur recommandation spéciale de votre hébergeur). Généralement, ils doivent être en 755/705 pour les dossiers et 604/644 pour les fichiers.

11. Supprimez les fichiers et dossiers non utilisés

Après chaque installation de Joomla!, supprimer le dossier d'installation et ne vous contentez pas de le renommer, supprimez également tous les fichiers non utilisés de votre template.

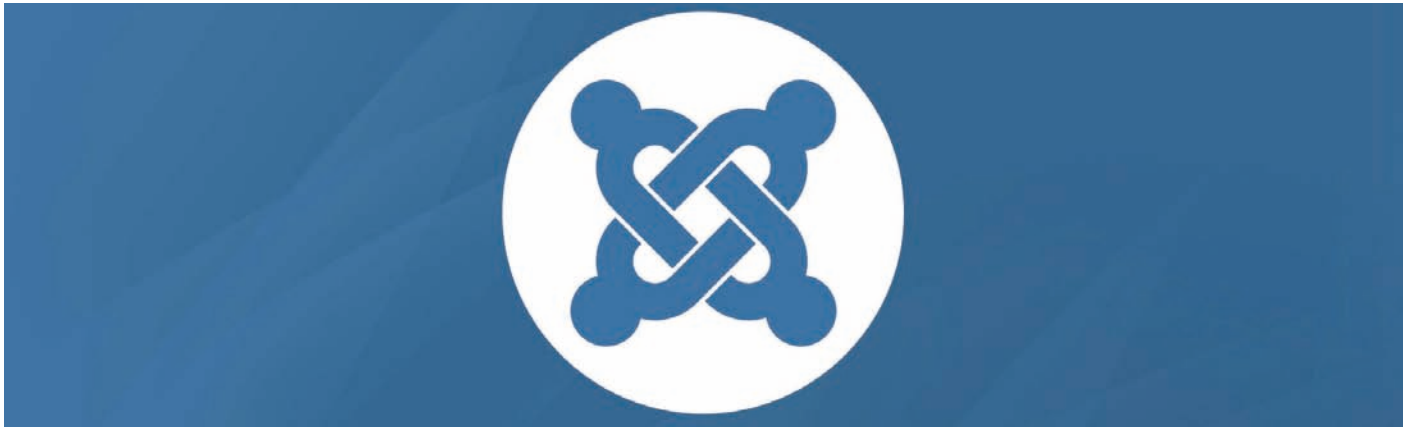
12. Utilisez le fichier Htaccess (Bloquez l'accès à tous les fichiers sauf index.php et index2.php)
Si vous n'avez pas un fichier htaccess, dans votre dossier Joomla!, vous devez renommer le fichier htaccess.txt fourni avec votre package d'installation Joomla! en .Htaccess.

13. Choisissez autant que possible le SSH (ou SFTP) au lieu du FTP.

14. Ne copiez-collez pas de texte provenant d'ailleurs dans vos articles sans nettoyer le code

15. Limitez autant que possible l'utilisation des iFrames (qui sont des portes ouvrant une page externe dans votre site)

16. Assurez-vous que vous exécutez votre site internet sur PHP 5.2 ou une version plus récente
Même si vous respectez à la lettre toutes ces règles, vous devez garder en tête que le risque 0 n'existe pas. Il y a toujours une chance, aussi infime qu'elle soit que vous vous fassiez hacker. Dans ce cas, vous aurez fait la majorité du travail surtout si vous respectez la règle des sauvegardes régulières. Ces

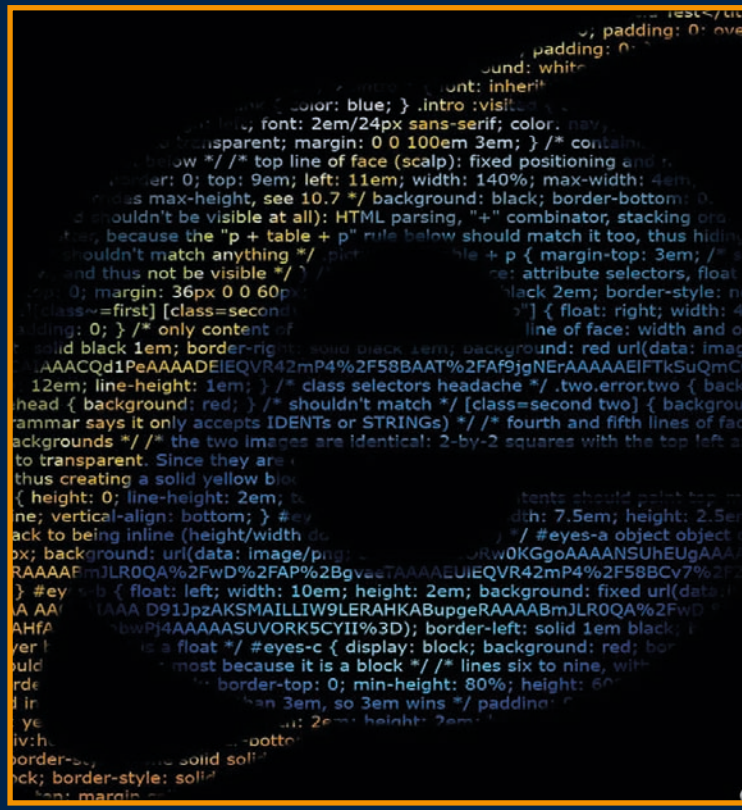


conseils représentent une ébauche concernant la sécurité d'un site propulsé sous Joomla! Pour apprendre plus il faut consulter la documentation **« http://docs.joomla.org/Category:Security_Checklist » « http://docs. joomla.org / Category:Security_Checklist » « http://docs.joomla.org/Category:Security_Checklist » « http://docs.joomla.org / Category : Security_Checklist » ! « http://docs.joomla.org/Category:Security_Checklist » sur « http://docs.joomla.org/Category : Security_Checklist » la sécurité.**


Windows® Internet
Explorer 10

17

Bonnes pratiques pour le déploiement sécurisé du navigateur Internet Explorer



BONNES PRATIQUES POUR LE DÉPLOIEMENT SÉCURISÉ DU NAVIGATEUR INTERNET EXPLORER

Aujourd'hui, les navigateurs Web sont installés sur presque tous les ordinateurs, ceci les a rendus une cible privilégiée pour les attaquants. Ces derniers exploitent les vulnérabilités inhérentes au navigateur pour prendre le contrôle de votre ordinateur. La compromission d'un navigateur est attractive pour un attaquant car elle lui permet souvent de contourner les mesures de sécurité liées à l'architecture réseau et aux différentes passerelles de filtrage. Les vulnérabilités d'un navigateur peuvent avoir des origines différentes : le navigateur lui-même, les modules complémentaires (add-ons), les plug-ins ou extensions ou les actions de l'utilisateur.

Microsoft Internet Explorer

Microsoft Internet Explorer est un navigateur Web édité par Microsoft. C'est un navigateur qui dispose de puissants mécanismes de sécurité. Néanmoins, comme tout navigateur Web, il représente une cible privilégiée des attaquants du fait de leur utilisation massive sur Internet mais aussi en raison des vulnérabilités qui sont propres aux différents modules complémentaires intégrés aux navigateurs dont les processus de mise à jour sont généralement indépendants de ces derniers.

Mécanismes de sécurité pris en charge par Microsoft Internet Explorer

Depuis sa version 10, Internet explorer intègre de nouvelles fonctionnalités de filtrage et des mécanismes de protection avancés qui sont activés par défaut et qui lui donnent un niveau de sécurité accru. Les principaux mécanismes de sécurité pris en charge par les différentes versions de Microsoft Internet Explorer sont :

- Protected Mode (Mode Protégé), utilise des mécanismes de sécurité comme :

A. l'UAC (User Account Control) : à chaque fois qu'un programme veut faire un changement majeur à votre ordinateur, l'UAC informe l'utilisateur et demande la permission.

B. l'UIPI (User Interface Privilege Isolation) : est une technique de sécurité qui permet une protection contre les exploits d'injection de code.

- LCIE (Loosely-Coupled IE), qui consiste à séparer d'une part les processus de pilotage du navigateur (interface graphique, fenêtres, etc.) et d'autre part, les processus d'affichage de contenu (contenu HTML, contrôles ActiveX, exten

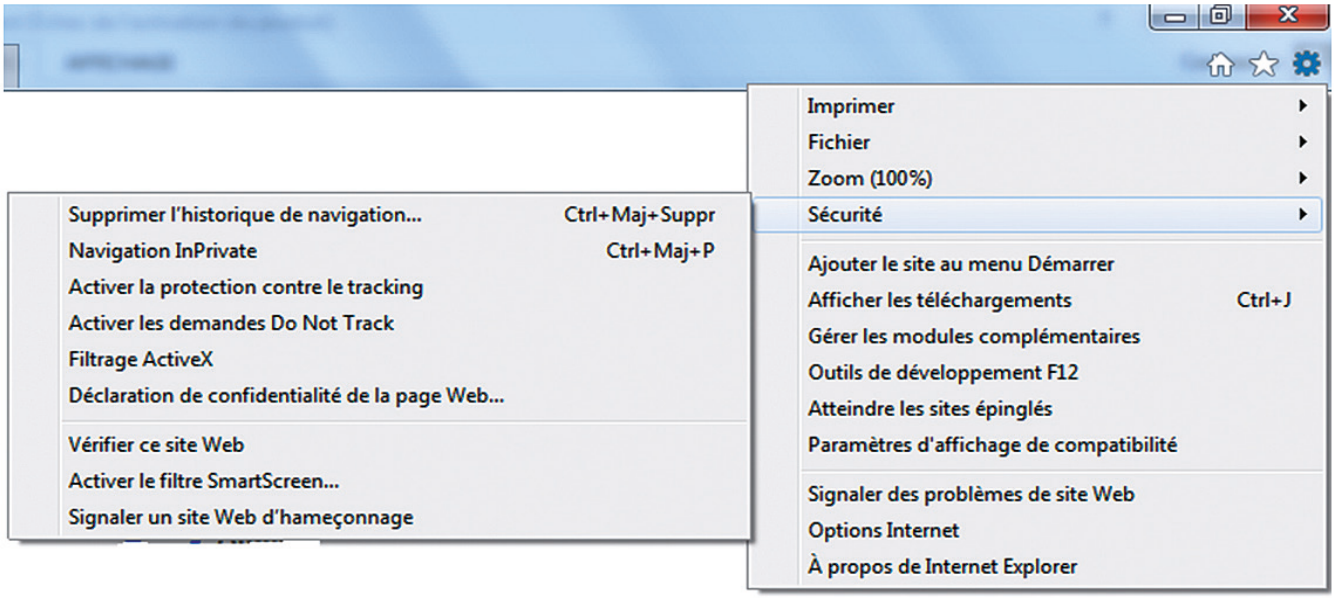
sions de barre d'outil, etc.). Cela permet de réduire la surface d'attaque des processus et de limiter ainsi les conséquences d'une exploitation de vulnérabilité.

• Filtre Smartscreen, mécanisme de protection contre le hameçonnage et les logiciels malveillants.

• Filtrage XSS 3 (anti-scripts de site à site), système de filtrage qui vise à repérer et bloquer le contenu malveillant injecté dans des pages Web par le biais de vulnérabilités.

• Filtrage ActiveX, système de filtrage qui permet de n'autoriser l'exécution de contrôles ActiveX que sur les sites de confiance.

• EPM (Enhanced Protected Mode), empêche les pages Web d'accéder en lecture/écriture au système d'exploitation.



LES RÈGLES À SUIVRE POUR UNE UTILISATION SÉCURISÉE DE MICROSOFT INTERNET EXPLORER

R1 Établir des listes de sites pour chaque niveau de confiance (zone intranet et zone des sites approuvés) auxquelles seront appliquées des configurations de sécurité spécifiques aux besoins de chaque zone.

R2 L'affectation des sites aux différentes zones de sécurité doit être faite par GPO (group policy object). Ces listes d'affectation doivent être verrouillées et non modifiables par les utilisateurs.

R3 Il est fortement conseillé de laisser le minimum possible de règles de sécurité dans un état non configurées.

R4 activation d'EPM pour que le niveau de sécurité atteint soit suffisant. Il en va de même pour le filtrage ActiveX et les autres fonctions visant à renforcer la sécurité d'exécution des modules complémentaires.

R5 Réduire la surface d'attaque du navigateur. Tout interdire puis renseigner exhaustivement par GPO une liste blanche de logiciel autorisés.

R6 Il est recommandé de désactiver l'utilisation SSL (ancien protocole) et de n'autoriser que les protocoles TLS qui offre une meilleure sécurité.

R7 Il est conseillé de désactiver le gestionnaire de mots de passe sur un réseau amené à traiter des données sensibles ou confidentielles.

R8 Il est recommandé d'activer toutes les « fonctionnalités de sécurité » facultatives.

R9 Activer les fonctionnalités de protection de la confidentialité (anti pistage, navigation privée, etc.) de l'onglet sécurité dès lors que le navigateur n'est pas dédié à une navigation en Intranet.

R10 Il est recommandé d'interdire les fonctions de géolocalisation en configurant le navigateur Internet Explorer pour empêcher qu'il divulgue votre position géographique aux sites que vous visitez.

R11 Si la confidentialité des recherches est jugée primordiale, il convient de désactiver les fonctionnalités de recherche instantanée ou de suggestion de recherche.

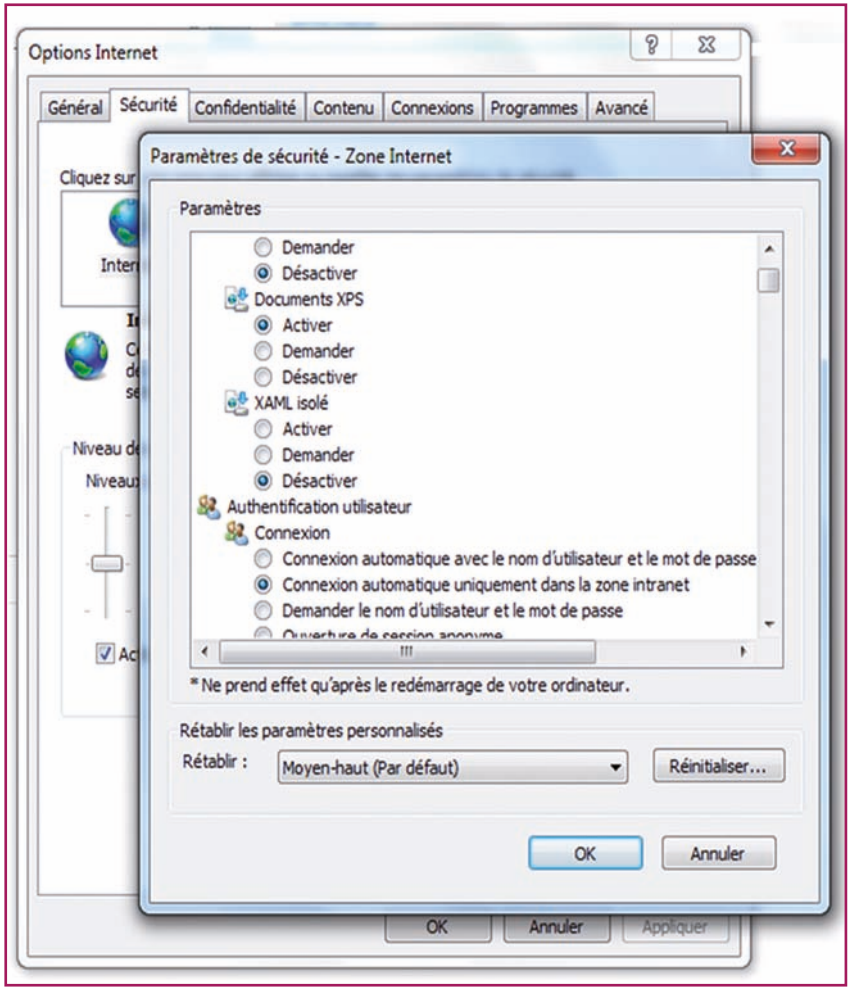
R12 Pour des questions de respect de la vie privée, il est conseillé d'imposer un moteur de recherche s'appuyant sur une connexion chiffrée (HTTPS).

R13 Il est recommandé d'activer les fonctionnalités de filtrage de contenu telles que l'anti-hameçonnage ou le bloqueur de fenêtres publicitaires (« pops-ups ») sur la zone Internet.

R14 Lors du démarrage du navigateur, il est préférable de ne pas restaurer la session précédente de l'utilisateur mais d'afficher une page connue et de confiance.

R15 Il est recommandé d'appliquer le modèle « niveau de sécurité haut » pour les sites que vous avez classé dans la « zone de sites sensibles » au niveau du navigateur.

R16 Si le navigateur est dédié à la navigation en intranet, il est plus pertinent d'appliquer directement le modèle de « niveau de sécurité haut » à la « zone Internet ».




Google

18

Bonnes pratiques pour le déploiement sécurisé du navigateur Google Chrome

BONNES PRATIQUES POUR LE DÉPLOIEMENT SÉCURISÉ DU NAVIGATEUR GOOGLE CHROME

Aujourd'hui, Google Chrome est devenu l'un des navigateurs les plus utilisés par les internautes. Ce navigateur possède plusieurs fonctionnalités telles qu'un système de « bac à sable », des possibilités de déploiement et de configuration centralisés, et son système de mise à jour automatique réactif. Nous présentons dans ce qui suit quelques recommandations pour un déploiement sécurisé de ce navigateur web.

1. Protéger ses mots de passe enregistrés

Si vous laissez Chrome enregistrer vos mots de passe, toute personne qui utilise votre PC peut facilement y accéder à travers le panneau réglages. Il est donc recommandé de ne permettre qu'aux personnes de confiance d'utiliser votre compte utilisateur. Vous pouvez créer un nouveau compte standard (non administratif) pour les autres utilisateurs ou les laissez utiliser le compte Invité. Vous pouvez aussi utiliser des extensions comme ChromePW, Browser Lock, ou un profil chrom sécurisé par mot de passe. Une autre option consiste à stocker vos données sensibles en utilisant un gestionnaire de mot de passe tiers.

2. Sécuriser vos données synchronisées

Si vous avez activé la synchronisation, Chrome conserve vos renseignements (préférences, mots de passe, etc) en utilisant vos identifiants de compte Google. La synchronisation devient cependant une vulnérabilité si votre compte Google venait à être piraté. Vous pouvez ajouter un niveau de protection en définissant un mot de passe de synchronisation, qui sera toujours requis pour accéder à vos données. Pensez aussi à renforcer la sécurité de votre compte Google en utilisant la validation en deux étapes par exemple.

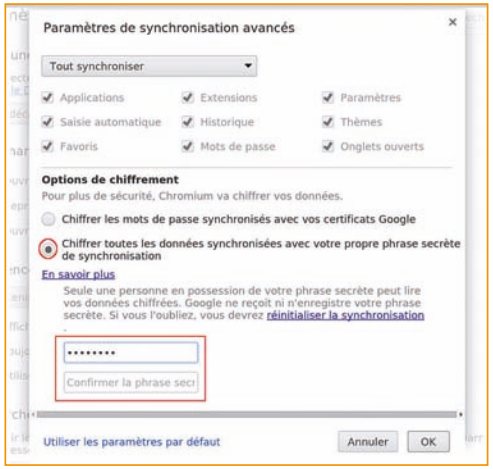


Figure 1 : Mot de passe de synchronisation

3. Safe browsing

Safe browsing est une fonctionnalité de sécurité qui vise à protéger l'internaute contre les sites de phishing et les téléchargements malveillants. Il fonctionne en envoyant les adresses de sites Web visités (sous forme de hash) à Google. Dans le cas d'une page dangereuse, l'utilisateur sera averti par message. La navigation sécurisée peut être entièrement désactivée si le compromis entre la vie privée (envoi de données de navigation à google) et la sécurité (liens et pages dangereuses) n'est pas acceptable.

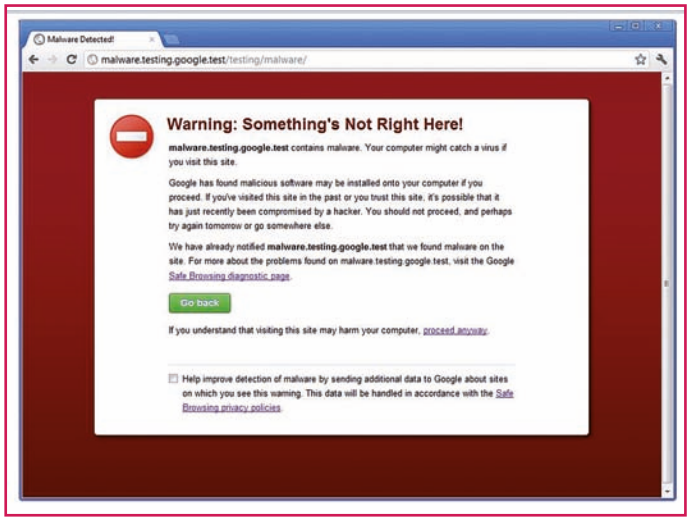


Figure 2 : Fonctionnalité Safe browsing

4. Sécurité des plugins/extensions

L'utilisateur peut installer des plugins et des extensions de la boutique en ligne Chrome.
Les plugins Chrome peuvent être développés en utilisant une des deux interfaces de programmation :

- NPAPI qui permet l'exécution des plugins avec le niveau de privilège de l'utilisateur. Une vulnérabilité affectant un plugin permet alors de compromettre la session ou le système.

- PPAPI: dont l'objectif est de rendre les plugins portables et sécurisés, et permet leur exécution en mode « bac à sable » en séparant les processus du navigateur et du moteur de rendu. L'exploitation de vulnérabilités du plugin reste alors confinée au processus.

Il est recommandé de n'autoriser que les plugins développés via PPAPI à l'inverse de NPAPI qui resté, malheureusement, l'outil le plus utilisé pour le développement de plugins. De même, il est recommandé de n'autoriser aucune extension sauf celles qui se justifient par un réel besoin métier comme par exemple les extensions de développement Web.

5. Installer des extensions pour plus de sécurité

Diverses extensions permettent d'ajouter encore plus de fonctions de sécurité. Par exemple, Adblock permet de supprimer les publicités qui peuvent conduire à des logiciels malveillants ou à des sites de Phishing.

Figure 2 : Ajout des extensions dans Google Chrome

6. Chrome, active directory et politique de sécurité

Dans ses dernières versions, Active Directory de Microsoft permet de définir des règles de sécurité dans les GPO (Group Policy Object), permettant ainsi une configuration centralisée du navigateur.

En entreprise, il est recommandé d'utiliser cette fonctionnalité pour inclure des règles de configuration importantes pour la sécurité de la navigation.

7. Installer un logiciel antivirus à jour

Il est indispensable d'installer des programmes de sécurité tel qu'un antivirus et de faire en sorte qu'il soit régulièrement mis à jour afin de se protéger contre les nouvelles menaces. Certains de ces programmes permettent d'empêcher le téléchargement des logiciels dangereux sur votre ordinateur pendant la navigation sur Internet. De plus, ils permettent d'identifier les sites Web suspects au niveau des résultats de recherche vous informant du risque que présentent ces sites avant d'y accéder.

Google chrome

19

Les bonnes pratiques pour le déploiement sécurisé du navigateur Firefox

LES BONNES PRATIQUES POUR LE DÉPLOIEMENT SÉCURISÉ DU NAVIGATEUR FIREFOX

Firefox est le navigateur web libre et gratuit édité par la fondation Mozilla et dont la première version stable date de 2004. Il a connu un succès croissant depuis sa sortie, il est aujourd'hui soutenu par une importante communauté de développeurs du monde libre.

Firefox dispose d'un mécanisme de mise à jour automatique et peut être configuré de manière centralisée. Il se prête bien à une utilisation professionnelle.

Avec Firefox, vous disposez de nombreux outils et réglages pour vous aider à vous protéger efficacement contre les sites frauduleux et les escrocs du net.

Ces bonnes pratiques visent à sensibiliser le lecteur aux enjeux de sécurité d'un navigateur Web et le guider dans la mise en œuvre d'une stratégie de sécurisation spécifique à Firefox.

1. Garder vos logiciels et votre système d'exploitation à jour

Les mises à jour logicielles contiennent des correctifs de vulnérabilité afin de protéger votre ordinateur et vos informations personnelles.

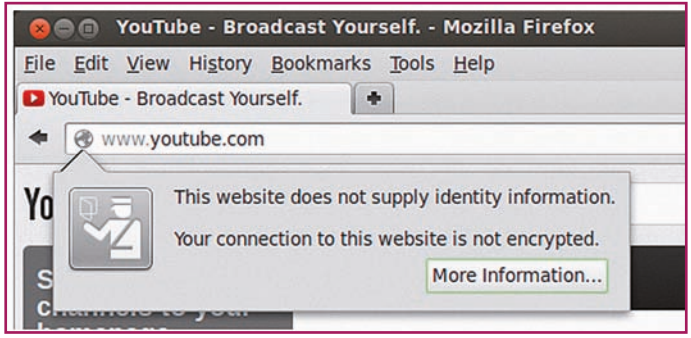
- Mettre à jour Firefox
- Cliquez sur le bouton (en haut à droite)
- Cliquez sur aide et sélectionnez le menu À propos de Firefox.
- Consultez Mettre à jour Firefox vers la dernière version pour plus de détails.[1]
- Mettre à jour vos plugins : Allez sur la page de vérification des plugins de Mozilla[2] et suivez les liens pour mettre à jour les plugins obsolètes.

1. https://support.mozila.org/kr/kb/mettre-jour-firefox-derniere-version
2. https://www.mozila.org/plugincheck

2. Définir des permissions

Dans la fenêtre d'informations sur la page que vous êtes en train de visiter, vous avez la possibilité de définir pour le site courant le comportement à adopter pour le chargement ou non des images, l'ouverture ou non des fenêtres pop-up, l'autorisation ou non des cookies, l'installation ou non de thèmes ou d'extensions pour le navigateur.

- Cliquez sur **le bouton d'identité du site** (l'icône du site web à gauche de son adresse), puis sur le bouton **Plus d'informations**… dans l'invite.
  Par exemple, lors de la visite d'un site (www.youtube.com) définir le comportement à suivre vis-à-vis des images **(Bloquer, Autoriser, Toujours demander).**
- Dans Permissions, Décochez la case **Permission par défaut** devant **Charger des images.**

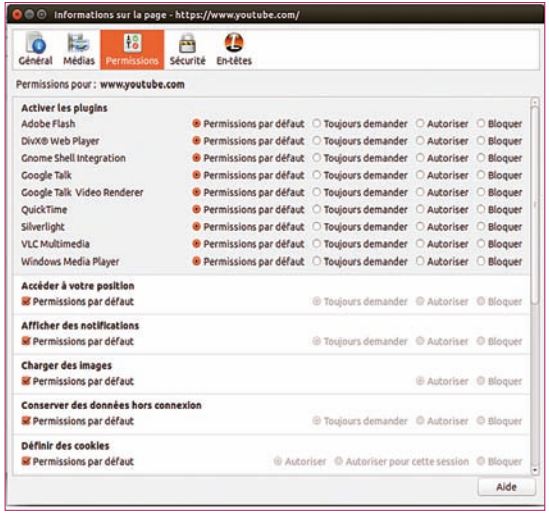


- Cliquer sur **Bloquer.**
- Ainsi les images seront bloquées pour ce site. **Fermez la fenêtre.**

3. Limiter le choix des plugins

Tout plugin ajouté à Firefox fait courir un risque de sécurité supplémentaire, d'où l'importance de les limiter au strict nécessaire.

Les plugins ou greffons, qui sont des composants compilés dédiés à offrir des fonctionnalités avancées du navigateur, et répondre à des besoins spécifiques. Une vulnérabilité affectant un plugin permet en revanche de compromettre la session ou le système.



4. Ne déployer que des extensions de confiance et nécessaires

Contrairement aux plugins qui sont des programmes compilés, les extensions s'exécutent dans le processus du navigateur et sans système de permission permettant de restreindre les libertés qui leur sont accordées. Ainsi, une extension malveillante peut accéder à des informations sensibles concernant la navigation de l'utilisateur puis les envoyer à un serveur illégitime sur Internet. Ou encore introduire de nouveaux comportements indésirables suite à une mise à jour. En parallèle, de nombreuses extensions présentent des vulnérabilités qui peuvent être exploitées (par le contenu des pages visitées ou encore, par courriels spécifiquement forgés et consultés par webmail).
Ces extensions vulnérables peuvent également servir à exploiter, par rebond, les vulnérabilités d'éventuels plugins activés et ainsi obtenir un accès complet au système.

5. Désactiver l'utilisation de SSL

Désactiver l'utilisation de SSL et n'autoriser que les protocoles TLS v1.1 et supérieurs (la v1.0 étant vulnérable). Il est également possible de restreindre les suites cryptographiques utilisable en désactivant celles reposant sur des algorithmes obsolètes comme RC4.

6. Garantir la confidentialité

- Désactiver les divers rapports disponibles de plantage, de performance, etc. pour limiter les données envoyées à Mozilla.
- Activer les fonctionnalités de protection de la confidentialité (anti pistage, navigation privée, suppression des données privées, etc.) lorsque le navigateur n'est pas dédié à une navigation Intranet.
- Interdire les fonctions de géolocalisation.
- Dès lors que la confidentialité des recherches est jugée primordiale, il conviendra d'imposer un moteur de recherche de confiance et de désactiver les fonctionnalités de recherche instantanée ou de suggestion de recherche.

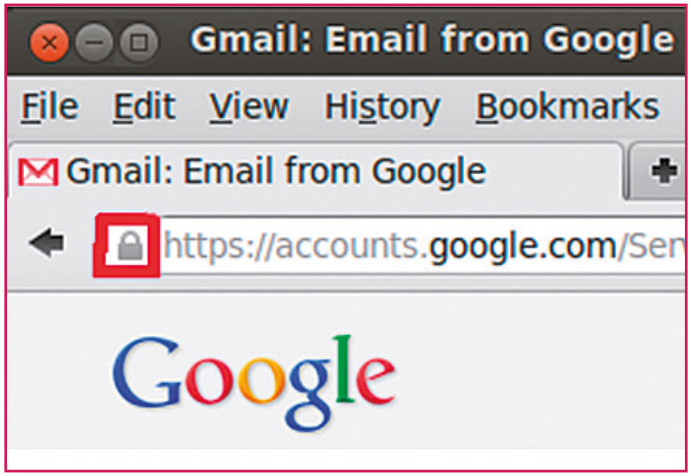
7. Page d'accueil

Il est préférable que le navigateur n'enregistre pas les sessions de navigation. Lors du démarrage du navigateur (après un arrêt normal ou brusque), il est en effet conseillé de ne pas restaurer la session précédente de l'utilisateur mais d'afficher une (des) page(s) connue(s) et de confiance.

8. Stratégie de double navigateur

Dédier un Il est recommandé d'utilise deux navigateurs. Le premier sera dédié à la navigation sur Internet avec une configuration durcie, sa surface d'attaque est réduite au

maximum. Le deuxième sera réservé à l'accès aux serveurs internes, configuré pour permettre uniquement l'accès et l'usage de l'ensemble des sites et applications légères de l'Intranet.



9. Vérifier vos paramètres de Firefox

Firefox a de nombreuses façons de vous aider à rester protégé sur le Web.

- Savoir si ma connexion vers un site web est sécurisée ?

Avec le bouton d'identité de site intégré à Firefox qui permet de donner des informations supplémentaires sur le site visité, savoir s'il est chiffré, si sa sécurité a été vérifiée et par qui, à qui appartient le site web. Cela peut vous aider à identifier les sites malveillants qui tenteraient d'obtenir des informations personnelles. Lors d'une visite à un site, vérifier toujours l'état du bouton d'identité du site qui peut prendre une de ces 5 formes.

- Désactiver les cookies tiers dans Firefox pour éviter de pister vos visites sur les sites web : Le réglage des cookies tiers est disponible dans le panneau « Vie privée » de la fenêtre « Préférences », cliquer sur **Ne rien indiquer aux sites concernant mes préférences de pistage** et aussi Positionnez **Accepter les cookies tiers à jamais.**
- Utiliser un mot de passe principal pour protéger les identifiants et mots de passe enregistrés :
- Cliquez sur le bouton menu et sélectionnez Préférences
- Cliquez sur le panneau **Sécurité.**
- Cochez Utiliser un mot de passe principal. La fenêtre « Modifier le mot de passe principal » apparaît.
- Saisissez votre mot de passe principal.

© CERIST 2017

CENTRE DE RECHERCHE SUR L'INFORMATION SCIENTIFIQUE ET TECHNIQUE
5, Rue des Trois Frères Aissou, Ben - Aknoun - BP 143. 16030 - Alger
Tél : +213 (23) 25 54 16 / Fax : +213 (23) 25 54 10
www.cerist.dz / سيريست.الجزائر