

Systemes d'Information : Règles prudentielles et bonnes pratiques

Stéphane Cholleton

Responsable du Pôle Conseil de Global Security : www.globalsecurity.fr

Cet aide-mémoire est un document générique réalisé à partir d'extraits des informations disponibles sur le site de l'ANSSI Agence Nationale pour la Sécurité des Système d'Information :
<http://www.securite-informatique.gouv.fr/index.html>

1 - Utiliser un mot de passe de qualité

Les mots de passe forts :

La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. Ainsi, **un mot de passe composé de caractères minuscules, majuscules, chiffres et caractères spéciaux sera de meilleure qualité qu'un mot de passe composé uniquement de minuscules.**

Choisir et retenir un mot de passe fort :

Un mot de passe long et ne comportant pas de mots du dictionnaire peut être difficile à retenir, et sera souvent inscrit sur un bout de papier à côté du poste, ce qui pourrait compromettre la sécurité de celui-ci dans un environnement partagé. Il faut donc trouver des **moyens mnémotechniques pour fabriquer et retenir facilement de tels mots de passe :**

phonétique : "J'ai acheté 3 CD pour cent euros cet après-midi" : ght3CD%E7am ;

méthode des premières lettres : "Un tiens vaut mieux que deux tu l'auras" : 1tvmQ2tl'A.

L'utilisation de caractères spéciaux, de chiffres et de majuscules peut être réalisée avec ces deux méthodes. De plus, il est possible de décliner plusieurs mots de passe à partir d'un mot de passe fort, en changeant, par exemple, l'un des caractères de celui-ci. Il est ainsi plus facile de retenir des mots de passe différents utilisés pour des accès divers. Cette méthode est toutefois à utiliser avec précaution, car si l'un des mots de passe est découvert, les autres peuvent être facilement devinés.

L'inscription de son mot de passe sur un bout de papier n'est pas toujours à proscrire, et cela dépend de l'environnement dans lequel on se trouve. Par exemple, cela est envisageable voire recommandé chez soi, où l'on est seul à avoir accès à l'ordinateur, mais pas dans un environnement partagé tel que le travail.

Recommandations :

Avoir des mots de passe de 10 caractères minimum, si possible de 16 caractères.

Utiliser des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux).



Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance...).

Le même mot de passe ne doit pas être utilisé pour des accès différents.

Changer de mot de passe régulièrement.

En règle générale, ne pas configurer les logiciels pour qu'ils retiennent les mots de passe.

Éviter de stocker ses mots de passe dans un fichier ou lieu proche de l'ordinateur si celui-ci est accessible par d'autres personnes.

Si possible, limiter le nombre de tentatives d'accès.

2 - Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc.

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 ces failles.

3 - Effectuer des sauvegardes régulières

Sauvegarder, c'est mettre en lieu sûr des informations pour les récupérer en cas de besoin.

Règles d'or :

Essayer et apprivoiser les logiciels de récupération (restauration) et de sauvegarde.

Mettre en lieu sûr les disques d'installation (système, logiciels, périphériques).

Sauver régulièrement les données (selon leur importance, la vitesse de modification, la quantité...).

Éloigner de l'ordinateur le support des sauvegardes de ses données.

Vérifier la lisibilité des sauvegardes, cela entraîne à l'utilisation du logiciel de récupération.

Sauvegarde Plus en détails :

Le meilleur moyen de ne pas perdre ses données est d'avoir toujours au moins une copie en lieu sûr, appelée sauvegarde. Il est primordial d'effectuer régulièrement des sauvegardes. La fréquence des sauvegardes dépend de la quantité de données que vous acceptez de perdre en cas de destruction de vos données.

En plus des données, vous pouvez sauvegarder votre système et vos logiciels, mais en général, ils sont fournis avec des moyens de réinstallation qui rendent cette sauvegarde moins importante que celle des données.

Pour effectuer une sauvegarde, vous pouvez utiliser soit un outil spécialisé soit faire de la simple copie de fichiers.

Il est recommandé, une fois la sauvegarde effectuée, d'entreposer les supports loin de l'ordinateur qui contient les données. Cette précaution évite que la destruction des données d'origine ne puisse s'accompagner de la destruction de leur copie de sauvegarde (ce qui pourrait arriver en cas d'incendie ou d'inondation).

Le support externe utilisé pour stocker la sauvegarde peut être un CD, un DVD enregistrables, un disque dur externe, une bande magnétique (DAT, DLT)... en fonction de l'équipement que vous possédez (interface USB, graveur, lecteur de bande) et de la quantité de données que vous avez à sauvegarder.

Attention, bien trop souvent, la sauvegarde n'est pas réalisée sur les données importantes et il est trop tard une fois qu'elles sont perdues pour faire quoi que soit. Faites donc vos sauvegardes régulièrement, par exemple en vous mettant un rappel dans votre calendrier ou en programmant une tâche automatisée. N'oubliez pas non plus que si vous avez chiffré des données, il faut sauvegarder les clés qui permettront de déchiffrer les données, sinon vos données seront illisibles en cas de perte de la clé.

Écrire sur un morceau de papier une information importante permettra certes de s'en souvenir mais il ne faut pas perdre le papier ! Ainsi sauvegarder c'est bien, mais l'important c'est de pouvoir récupérer les données (les restaurer). Il est donc nécessaire de s'entraîner à la restauration des données ou des systèmes afin de s'assurer que tout fonctionne, que le personnel est formé et opérationnel et aussi permettre de limiter le stress le jour où la restauration sera nécessaire.

4 - Désactiver par défaut les composants ActiveX et JavaScript

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

*Les ActiveX ou plus précisément les contrôles ActiveX sont une technologie propre à Internet Explorer. Ils permettent l'exécution de programmes sur votre machine par l'intermédiaire de votre navigateur. Un contrôle ActiveX malveillant que vous auriez accepté d'installer sur votre machine a potentiellement accès à tout ou partie de votre ordinateur. **Il est recommandé de les désactiver par défaut dans Internet Explorer et d'en limiter l'utilisation aux sites de confiance***

Les scripts JavaScript

Recommandation : Bien que cela soit de plus en plus délicat, il convient de désactiver autant que faire se peut les scripts JavaScript dans votre navigateur et ne les activer que sur des sites de confiance et lorsque cela est réellement nécessaire.

Pourquoi ? Le JavaScript est un langage très utilisé permettant l'intégration de programmes directement dans les pages des sites. Il est présent dans de nombreuses pages et sites internet. On peut le trouver également dans certaines interfaces d'administration d'imprimantes ou d'équipements en réseau. Il peut être le vecteur de certaines attaques visant à utiliser des fonctionnalités de votre navigateur à votre insu ou à récupérer des informations sur votre ordinateur.

5 - Bonnes pratiques de navigations

Les extensions de navigateur :

Recommandation : une bonne pratique consiste à **n'installer que des extensions dont vous avez besoin et dont l'origine est de confiance.**

Pourquoi ? Il existe des extensions disponibles pour les navigateurs permettant le support de nouvelles fonctionnalités ou de nouvelles technologies. Il conviendra à chaque ajout de



prendre en compte le fait que celui-ci peut être à l'origine d'une nouvelle vulnérabilité sur votre ordinateur. Il est donc nécessaire de ne les installer qu'au cas par cas.

Naviguer prudemment sur l'internet :

Une fois votre navigateur et votre machine correctement configurés et à jour, il convient encore de prendre quelques précautions d'usage lorsque vous naviguez sur des sites internet.

Vérifier les certificats :

Recommandation : **Ne donnez pas d'informations personnelles et confidentielles (vos coordonnées personnelles, vos coordonnées bancaires, etc)** sur un site marchand ou un site bancaire, sans avoir vérifié au préalable que le site est sécurisé par l'emploi d'un certificat électronique qui garantit que le site est authentique, et qui va servir à protéger la confidentialité des informations échangées. Pour cela, il y a deux informations affichées par le navigateur qui doivent être vérifiées :

L'adresse URL du site doit commencer par "https://" et le nom du site doit correspondre à l'attente de l'utilisateur ;

un petit cadenas fermé doit figurer à droite de l'adresse du site, ou en bas à droite de la barre d'état (selon la version et le type de votre navigateur) ; il symbolise une connexion sécurisée. En cliquant dessus, on peut afficher le certificat électronique du site, et visualiser le nom de l'organisme.

6 - Ne pas cliquer trop vite sur des liens

Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à **l'inciter à cliquer sur un lien placé dans un message**. Ce lien peut-être trompeur et malveillant. **Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur**. De nombreux problèmes seront ainsi évités.

7 - Ne jamais utiliser un compte administrateur pour naviguer

L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les **droits dits d'administrateur** et les **droits dits de simple utilisateur**. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'internet. **En limitant les droits d'un utilisateur on limite aussi les risques d'infection ou de compromission de l'ordinateur.**

8 - Contrôler la diffusion d'informations personnelles

L'internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir...

9 - Ne jamais relayer des canulars

Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.

10 - Soyez prudent : l'internet est une rue peuplée d'inconnus !

Il faut rester vigilant ! Si par exemple **un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou tout autre langue) il convient de ne pas l'ouvrir.** En cas de doute, il est toujours possible de confirmer le message en téléphonant. D'une façon générale, **il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.**

11 - Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants

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 ; .lnk**. A l'inverse quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus "inerte" possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations