La sécurité informatique, ça vous concerne !

1 Sécurité informatique

La sécurité informatique est un concept global qui dépasse largement le problème des logiciels malveillants. En effet, les questions relatives au vol, la cryptographie, l'anonymat, au contrôle parental entrent également en jeu lors de l'utilisation d'internet. Par conséquent, la meilleure arme pour lutter contre l'insécurité informatique reste l'éducation des utilisateurs.

L'objectif de ce document est donc de vous sensibiliser à certaines règles essentielles pour une utilisation en toute sécurité de vos outils informatiques.

2 Sauvegarde

Sauvegarder régulièrement vos données importantes fait partie des règles de base en informatique. Cette copie de sauvegarde doit s'effectuer sur un support physique indépendant de l'emplacement du fichier original afin d'éviter qu'en cas de défaillance du disque, l'original et sa copie soient définitivement perdus.

Au niveau privé, vos fichiers stockés sur votre disque dur doivent impérativement être sauvegardés sur une clé USB ou un autre support que vous pouvez placer en lieu sûr. En entreprise, il est recommandé de stocker ces fichiers sur le serveur qui est, en principe, sauvegardé quotidiennement.

3 Anti-virus

Les antivirus combattent les virus sur plusieurs fronts et fonctionnent pratiquement tous de la même manière : ils agissent comme un filtre entre le système d'exploitation de votre ordinateur et les fichiers qui y pénètrent.

La mise à jour de la base de données des signatures des virus est évidemment une opération cruciale, étant donné que les virus évoluent rapidement.

Mettre à jour votre antivirus c'est bien ! Mettre à jour votre système d'exploitation, c'est encore mieux ! Certains « Malwares » exploitent des failles de Microsoft, qui réagissent en sortant des patchs de sécurité, indispensables à la sécurité de votre système.

4 Bonnes pratiques

Les risques de sécurités sont nombreux et évoluent rapidement. Voici quelques conseils pour améliorer la sécurité de votre poste :

1. Ayez au minimum 2 mots de passe différents : 1 pour votre compte de messagerie, et 1 pour les comptes que vous ouvrez chez des tiers sur internet. Le mot de passe de votre compte de messagerie doit être modifié tous les 3 mois

   Optez pour des mots de passe qui ne se trouvent pas dans un dictionnaire et impossible à deviner.
2. Ne divulguez en aucun cas votre mot de passe à vos collègues ; il est personnel.
3. Vos fichiers de travail doivent se trouver sur le serveur de fichier, non sur votre poste (ou autre support de stockage).
4. Travaillez avec un compte utilisateur aux droits limités afin d'éviter l'installation de programme non désirés.
5. Verrouillez toujours votre session lorsque vous quittez votre place.
6. Soyez vigilant(e) quant aux mails que vous recevez : Vérifiez la pertinence de l'expéditeur, des pièces jointes, et des liens hypertextes (URL).
7. Attention aux informations qui circulent sur internet, elles ne sont pas toujours véridiques. Vous pouvez vérifier la consistance de l'information sur http://www.arobase.org/sos
8. Ne donnez jamais accès à votre système ou au réseau à des personnes inconnues.
9. Ne consultez pas de documents dont le contenu est prohibé par la loi ou amoral, cela pourrait avoir des répercussions importantes en cas d'enquête, ou pire...
10. Signalez immédiatement aux responsables toute anomalie informatique constatée.
11. Faites bien attention à ce que vous installez sur votre ordinateur, toutes les toolbars ne vous sont pas utiles !

En suivant ces quelques conseils vous ne serez pas complètement à l'abri d'attaques, mais vous pourrez néanmoins éviter certaines conséquences désastreuses.

Exemples de risques

Rogue - AntiSpy Pro

Un ordinateur est infecté par AntiSpy Pro lorsqu'un **utilisateur** installe un cheval de Troie qui se fait passer pour un codec vidéo requis pour regarder une vidéo. Une fois dans votre système, toutes les recherches sur Google ou Yahoo vous diront que vous êtes infecté et que vous devriez installer **AntiSpy Pro**.

Une fois installé, il va scanner votre ordinateur et montrer des fichiers légitimes comme étant infectés…

Ransomware - Bundesamt für Polizei virus

Bundesamt für Polizei virus est une infection ransomware qui peut infecter votre système d'exploitation de Windows, si celui-ci n'est pas protégé par logiciel automatique contre les logiciels malveillants. L'infection peut se glisser dans le PC à l'aide de **téléchargements** groupés ou à l'aide d'ingénierie sociale. Il y a cependant une plus grande chance qu'il ait été installé sur votre ordinateur par un cheval de Troie.

Une fois terminée, l'infiltration clandestine perturbe les fonctionnalités de votre ordinateur. Elle supprime votre accès au bureau, en vous bloquant sur un message complètement faux. Il ne faut absolument pas payer !

Ver – Stuxnet

Stuxnet est un malware qui exploite une faille du système d'exploitation Windows, sous la forme d'un vers et par l'intermédiaire d'une **clé USB**. Une fois implanté sur un système, il est capable de contrôler des oléoducs, centrales électriques ou autres installations industrielles.

Ce ver ne s'intéresse pas au PC de « monsieur tout-le-monde », mais à des systèmes de contrôle industriels, que l'on trouve sur des sites sensibles : usines, centrales nucléaires ou de gestion de l'eau.

Vie privée – Stockage à l'étranger

Un Romand s'est vu interdire d'entrée aux Etats-Unis après une mauvaise blague dans un e-mail. Il craint avoir été victime des «grandes oreilles» américaines.

«Une grave menace pour les droits des citoyens». Les conclusions d'un rapport du Parlement européen sont sans équivoque. L'objet de ce constat? Un amendement américain qui permet aux autorités de surveiller, outre les communications comme l'e-mail et le téléphone, toutes les données stockées aux Etats-Unis par des non Américains. Sont concernés tous les services de synchronisation en ligne comme iCloud, Google Drive ou Dropbox, et les services de messagerie.

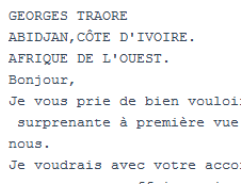
Virus – Tchernobyl

Le virus informatique Tchernobyl ou CIH est connu pour avoir été l'un des plus destructeurs.

Une fois la machine infectée, le virus attendait le 26 avril (date anniversaire de l'explosion de la centrale nucléaire de Tchernobyl, le 26 avril 1986). Puis, il détruisait l'ensemble des informations du système et parfois il rendait la machine quasiment inutilisable. Il a sévi de 1997 à 2002.

Scam 419 – Arnaque par mail

Le scam (« ruse » en anglais), est une pratique frauduleuse, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. La meilleure solution est comme toujours de supprimer le message. Inutile de mener vous-même une bataille contre ces brigands.


GEORGES TRAORE
ABIDJAN,CÔTE D'IVOIRE.
AFRIQUE DE L'OUEST.
Bonjour,
Je vous prie de bien vouloi
surprenante à première vue
nous.
Je voudrais avec votre acco

L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche étranger décédé il y a peu. Votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer des fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les montants.