Principales menaces informatiques

Afin de vous protéger de toute tentative de fraude, vous devez prendre un certain nombre de mesures pour sécuriser votre ordinateur.

La cybercriminalité, pratiquée par des pirates informatiques ou hackers, consiste à accéder aux ordinateurs d'autrui à des fins frauduleuses. À tout moment, vous pouvez être victime d'une attaque si votre ordinateur n'est pas protégé : que ce soit en recevant un e-mail trompeur réclamant votre « attention immédiate » ou en surfant tout simplement sur Internet.

Les pirates informatiques peuvent rechercher des informations d'identification personnelles stockées sur votre ordinateur, telles que vos numéros de carte bancaire ou les informations de connexion de vos comptes personnels, qu'ils utilisent pour vous soustraire de l'argent ou pour accéder à vos services en ligne dans un but criminel. Ils peuvent également s'approprier les ressources de votre ordinateur, notamment votre connexion Internet, pour augmenter leur bande passante afin d'infecter d'autres ordinateurs.

De nombreux dangers menacent la sécurité de votre ordinateur. Vous trouverez ci-après une liste des différents types de menaces existants ainsi que certaines mesures à prendre pour limiter leur impact.

Failles de sécurité

Les failles de sécurité sont constituées par les défauts d'un logiciel, qui fragilisent la sécurité globale de votre ordinateur ou de votre réseau. Les menaces de ce type tirent parti de ces failles, qui peuvent alors endommager l'ordinateur ou ses données.

Que faire ?

•Tenir à jour les correctifs de sécurité et logiciels. (Mise à jour des patchs de sécurité)
•Installer une solution de sécurité. (antivirus, pare-feu ..)
•Configurer les paramètres de sécurité pour votre système d'exploitation, votre navigateur Internet et votre logiciel de sécurité.

Logiciels espions

Un logiciel espion peut être téléchargé à partir de sites Web, d'e-mails, de messages instantanés et de connexions directes de partage de fichiers. Par ailleurs, un utilisateur peut, sans le savoir, recevoir un logiciel espion en acceptant un contrat de licence utilisateur final d'un programme informatique.

Que faire ?

•Utiliser un programme de sécurité Internet connu pour vous protéger contre les logiciels espions et les autres risques de sécurité.
•Configurer le pare-feu de ce programme de sécurité pour bloquer les demandes de communications sortantes qui n'ont pas été sollicitées.
•Ne pas accepter, ni ouvrir de messages d'erreur suspects dans votre navigateur.
•Refuser les offres de logiciels gratuits, les logiciels espions pouvant être intégrés à de telles offres.
•Toujours lire attentivement le contrat de licence utilisateur final lors de l'installation et annuler l'installation si d'autres « programmes » sont installés avec le programme souhaité.
•Tenir à jour les correctifs de sécurité et logiciels.

Courrier indésirable

Le courrier indésirable est la version électronique des publicités papier que vous recevez dans votre boîte aux lettres. Cela consiste à envoyer des messages non sollicités, la plupart du temps de la

publicité, à un grand nombre de destinataires. Le courrier indésirable pose un sérieux problème de sécurité, car il peut être utilisé pour envoyer un e-mail susceptible de contenir des chevaux de Troie, des virus, des vers, des logiciels espions et des attaques ciblées qui visent à obtenir des informations d'identification personnelles et confidentielles.

Que faire ?

•Installer un logiciel de blocage/filtrage du courrier indésirable.
•Ne répondre à aucun courrier suspect et supprimer systématiquement ce type de courrier.
•Désactiver le volet de prévisualisation de vos e-mails et lire les messages en texte brut.
•Rejeter tous les messages instantanés provenant de personnes qui ne figurent pas dans votre liste de contacts.
•Ne pas cliquer sur les liens URL figurant dans un message instantané, sauf s'ils proviennent d'une source connue et qu'ils sont attendus.
•Tenir à jour les correctifs de sécurité et logiciels.

Programmes malveillants

Les programmes malveillants font partie des programmes hostiles, comprenant les virus, les vers et les chevaux de Troie. Les programmes malveillants dits destructeurs utilisent les outils de communication les plus courants pour se propager, notamment sous la forme de vers envoyés dans des messages électroniques ou instantanés, de chevaux de Troie propagés via des sites Web et de fichiers infectés par des virus téléchargés à partir de connexions P2P. Les programmes malveillants tentent également d'exploiter les failles existantes des systèmes en s'introduisant de façon aisée et transparente.

Que faire ?

•Ouvrir uniquement les pièces aux messages électroniques ou instantanés provenant de sources fiables, et que vous attendiez.
•Faire analyser les pièces jointes aux messages électroniques par un programme de sécurité Internet connu avant de les ouvrir.
•Supprimer tous les messages non sollicités sans les ouvrir.
•Ne pas cliquer sur des liens Web envoyés par des personnes que vous ne connaissez pas.
•Si une personne figurant dans votre liste des contacts vous envoie des messages, fichiers ou liens vers des sites Web étranges, fermer votre session de messagerie instantanée.
•Analyser tous les fichiers avec un programme de sécurité Internet connu avant de les transférer sur votre système.
•Transférer uniquement les fichiers provenant de sources connues.
•Utiliser un programme de sécurité Internet connu pour bloquer toutes les communications sortantes non sollicitées.
•Tenir à jour les correctifs de sécurité.

Hameçonnage (ou Phishing)

Le hameçonnage est essentiellement une escroquerie en ligne, et les hameçonneurs ne sont rien d'autre que des escrocs usurpateurs d'identité, particulièrement doués en informatique. Ils utilisent le courrier indésirable, les sites Web malveillants et les messages électroniques et instantanés pour inciter les utilisateurs à divulguer leurs informations confidentielles telles que les coordonnées de carte bancaire ou de crédit, ou encore les informations permettant d'accéder à leurs comptes personnels.

Il existe quatre méthodes permettant d'identifier les tentatives d'hameçonnage :
1. Les hameçonneurs, se faisant passer pour des sociétés légitimes, peuvent envoyer un e-mail pour demander des informations personnelles et amener les destinataires à répondre via des sites Web

malveillants. Ils peuvent également convaincre les destinataires qu'il est urgent d'agir et les conduire à télécharger des programmes malveillants sur leurs ordinateurs.

2. Les hameçonneurs jouent sur l'émotion, en envoyant des demandes urgentes ou en évoquant des menaces, pour inciter les destinataires à répondre.

3. Les sites de hameçonnage peuvent avoir un aspect quasi identique aux sites originaux, car les criminels ont tendance à utiliser les images sous copyright des sites légitimes.

4. Toute demande d'informations confidentielles effectuée par messagerie électronique ou instantanée n'est pas recevable.

Que faire ?

Si vous pensez avoir reçu un courrier d'hameçonnage, avoir été incité à cliquer sur un lien ou à télécharger un programme et que vous craigniez d'avoir installé un programme malveillant sur votre ordinateur, voici quelques éléments à vérifier :

•Votre programme antivirus fonctionne-t-il ?
•Les définitions de virus sont-elles à jour (datées de moins d'une semaine) ?
•Avez-vous récemment effectué une analyse antivirus complète de la mémoire/du disque ?
•Utilisez-vous un logiciel anti-espion, comme Adaware et/ou SpybotSD ?
•Après avoir exécuté vos programmes antivirus et avoir obtenu des résultats positifs ou avoir supprimé des programmes, assurez-vous que vos comptes en ligne sont sécurisés (modifiez les mots de passe de vos comptes).

Source : http://interne.monster.ca/computer-threats/inside2.aspx