1ère année – Cours N° 05

La sécurité sur Internet

1 – Les risques liés aux mauvaises rencontres

On trouve de tout sur Internet : le meilleur comme le pire. L'accès facile à tout ce qui s'y trouve doit nous conduire à être vigilant, notamment à l'égard des enfants. La première précaution consiste donc à activer le contrôle parental que propose gratuitement chaque opérateur.
Par ailleurs, le « chat » qui consiste à converser avec d'autres personnes sur internet doit être proscrit lorsqu'il conduit à échanger avec un inconnu.
D'une manière générale, on ne doit jamais donner son e-mail à quelqu'un que l'on ne connaît pas ou le laisser sur un site non-marchand occasionnel.

2 – Les risques liés au paiement par carte bancaire

Les fraudes à la carte bancaire deviennent de plus en plus fréquentes. Quelques précautions s'imposent dans le paiement par internet :
- ne jamais s'inscrire dans une démarche d'achats de type « en 1 click » (conservation des coordonnées bancaires chez le commerçant ad-vitam aeternam)
- préférer les paiements par carte virtuelle (type Virtualis) avec des coordonnées qui ne durent que le temps de l'achat
- le « must » consiste dans les systèmes nécessitant, avant le déclenchement du paiement effectif, la saisie sur la page internet d'un code passé préalablement par la banque sur le téléphone portable par SMS
- dans tous les cas de figure, le « passage au crible » du relevé bancaire des opérations par carte s'impose, surtout lorsqu'il s'agit de petites sommes.
- en cas de manœuvre frauduleuse dont nous pourrions être victimes, il faut le signaler immédiatement à sa banque (par téléphone, puis confirmation par mail ou courrier). Certaines banques réclament un récépissé de dépôt de plainte . La loi ne l'exige pas, mais cela ne coûte rien de faire néanmoins la démarche. Dans tous les cas de figure, la banque est responsable des conséquences de l'usage frauduleux de la carte et doit vous indemniser du montant dérobé.

3 – Les risques liés aux infections de sa machine

Les attaques par virus sur internet sont malheureusement devenues monnaie courante ! Les virus informatiques sont des petits programmes qui se logent dans l'ordinateur à notre insu au moment des connections internet ou lorsque l'on insère un média amovible infecté (clé USB, disque amovible, disquette, CD, ...)
Il existe désormais des « catégories » de virus qui se distinguent par la nature des dommages occasionnés :
- le **spyware** : un logiciel espion (aussi appelé mouchard ou espiogiciel) est un logiciel qui s'installe dans un ordinateur *dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé*, sans que l'utilisateur en ait connaissance.
- le **malware** : un logiciel malveillant (aussi appelé maliciel) est un logiciel développé *dans le but de nuire à un système informatique*, sans le consentement de l'utilisateur infecté. Les malwares englobent les virus, les vers, les chevaux de Troie.
- le **ransomware** : un logiciel malveillant (aussi appelé rançongiciel) *qui prend en otage des données personnelles*. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Un

ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent. Les modèles modernes de rançongiciels sont apparus en Russie initialement, mais on constate que le nombre d'attaques de ce type a grandement augmenté dans d'autres pays, entre autres l'Australie, l'Allemagne, les États-Unis.

Il existe bien entendu des parades pour se protéger de ces programmes malveillants. La première précaution consiste à se doter de logiciels protecteurs payants (MacAfee, Kaspersky, Norton, Avast, …) qui développent des stratégies efficaces de détection et de suppression en temps réél des menaces. On peut, si l'on choisit des formules gratuites, s'équiper d'un ensemble de trois logiciels qui ne se gênent pas mutuellement et qui garantissent une certaine efficacité :
L'un des cocktails satisfaisants en solutions gratuites peut se composer de :
{Avast gratuit + Malwarebytes gratuit + Spybot gratuit}
Chacun de ces logiciels peut être trouvé sans difficulté en téléchargement par le biais du moteur de recherche Google.
Attention en lançant l'installation de ces logiciels : plusieurs d'entre eux proposent subrepticement des cases pré-cochées permettant l'installation de versions payantes « à l'essai » ou d'autres logiciels non souhaités. Il convient donc d'être très attentif lors de la séquence d'installation de ces programmes, en décochant les cases qui doivent être décochées.

De nombreux virus se propagent par le biais de téléchargements illégaux (musique, photos, livres, logiciels, vidéos,…) . Une parade importante et simple consiste donc à ne pas utiliser de tels procédés et à préférer les téléchargements légaux (dont le coût reste souvent abordable).

Notons enfin le déclenchement à distance de sa webcam sans qu'on l'ait demandé. A portée de mains de connaisseurs des systèmes informatiques, cette manipulation peut conduire aux pires excès dans de nombreux domaines. La précaution minimale consiste en l'obturation temporaire de la webcam. D'une manière générale, évitons de laisser connectée notre machine lorsque nous ne nous en servons pas !

Enfin, pour se prémunir contre le risque de dommages importants de ses données informatiques, il est essentiel de sauvegarder régulièrement ses données principales sur un support non régulièrement connecté (clé USB, disque dur externe, DVD).

-=-=-=-=-=-