Les bonnes pratiques de sécurité informatique à adopter en ligne

ÊTRE VIGILANT AVANT D'OUVRIR UN COURRIEL INCONNU
Une des méthodes les plus efficaces pour diffuser des virus est d'utiliser des fichiers joints aux courriers électroniques. Pour se protéger, ne jamais ouvrir les pièces jointes provenant de personnes inconnues. Rappel : nous communiquons avec vous uniquement via la messagerie client et nous ne vous envoyons pas de courrier électronique sur votre messagerie personnelle.

NE PAS CLIQUER TROP VITE SUR LES 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.

VÉRIFIER LA PRÉSENCE D'UN CADENAS SSL OU QUE LE SITE EST SÉCURISE
Dans la « barre d'adresse » de votre navigateur, vérifiez l'orthographe de l'adresse du site ainsi que la présence du cadenas ssl. Vous pouvez aisément contrôler que vous êtes sur un site sécurisé grâce à la mention « https » (et non http). Cette dernière apparaît dans la barre d'adresse de votre navigateur internet,

CHOISIR UN MOT DE PASSE DE QUALITE
Il est essentiel de savoir choisir un mot de passe de qualité, c'est-à-dire difficile à retrouver et à deviner par une tierce personne (par exemple, ne mettez pas votre date de naissance). Pour vous connecter à vos comptes, nous vous demandons de saisir votre code secret uniquement à l'aide d'un clavier virtuel.

SURVEILLER LA DIFFUSION DE VOS INFORMATIONS PERSONNELLES
Il est fortement recommandé de ne jamais laisser de données personnelles dans des forums, ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises.

DESACTIVER PAR DEFAUT LES COMPOSANTS ACTIVE X
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

AVOIR UN SYSTEME D'EXPLOITATION ET DES LOGICIELS A JOUR
Il est conseillé de vérifier régulièrement les versions de tous vos logiciels, et surtout de :

- votre système d'exploitation (ex. Windows, Mac OSX)
- votre navigateur internet
- votre anti-virus
- votre pare-feu (ou firewall)
- votre anti-espiogiciel (anti-spyware)