Fiches Pratiques

Se servir de sa messagerie

Confidentialité :

Rien ne vous garantit que votre mail ne soit pas lu par un tiers. Votre messagerie contient énormément d'informations confidentielles et peut avoir énormément de valeur pour une personne mal intentionnée.

Conseil : ne communiquez jamais votre mot de passe et surtout déconnectez-vous chaque fois que vous avez fini de consulter vos e-mails, surtout si l'ordinateur n'est pas le vôtre.

Authenticité

Rien ne permet de garantir que l'expéditeur d'un email est bien celui qu'il prétend être. En effet, n'importe qui peut paramétrer son logiciel de messagerie pour qu'il affiche un expéditeur quelconque... Cette méthode est notamment employée dans le cadre du "pishing".

*Qu'est-ce que **le phishing***
Cette technique d'escroquerie consiste à vous subtiliser des données sensibles (mots de passe de connexion à un service, numéro de compte en banque ou de carte bancaire...) en vous piégeant avec un faux courrier électronique qui reprend le logo, la mise en page, l'adresse de votre banque, de votre fournisseur d'accès Internet, d'un service de messagerie ou d'un site marchand.
Le message prétexte un problème lié à votre compte et vous invite à cliquer sur un lien pour donner vos coordonnées et régler le souci. Vous basculez en réalité sur un faux site. Une fois entrées les informations demandées, le piège se referme sur vous.

Première chose essentielle à savoir, **aucune banque, aucun fournisseur d'accès Internet ni aucun marchand de biens ou services en ligne ne vous demandent jamais de donner votre mot de passe, un numéro de carte bancaire, un RIB ou quelques autres données sensibles** vous concernant. Un courrier électronique vous réclamant de telles informations, aussi alarmiste soit-il, est à coup sûr une tentative de phishing. Ne vous laissez surtout pas impressionner.

Autre indice révélateur, **ces messages sont souvent rédigés par des pirates étrangers qui maîtrisent mal notre** langue. Les fautes d'orthographe et les mauvaises tournures sont fréquentes. Ne répondez jamais à ce genre de courrier, même pour dire que vous avez démasqué leur tentative.

Fiabilité

Un e-mail peut ne pas parvenir à l'expéditeur – problème technique sur un serveur ou simple erreur dans l'adresse - . Si vous avez un message important à envoyer et que vous voulez vous assurer qu'il sera bien lu par le destinataire, utilisez les fonctions d'accusé de réception et d'accusé de lecture de votre logiciel de messagerie. L'accusé de réception vous permet de savoir si le message a bien été distribué, mais en aucun cas qu'il a été lu. L'accusé de lecture vous confirmera que le destinataire a ouvert son message.

Créez deux adresses mail différentes

Il est intéressant d'avoir une adresse qui vous permet de décliner votre identité pour des sites sérieux et d'avoir une adresse « poubelle » qui vous permet de vous inscrire sur des sites ou des jeux en ligne : ceux-ci amènent leur lot de spams et de courriers indésirables.

*Qu'est-ce qu'un **"Spam"** ?*
Le « spam » ou « pollupostage », désigne les communications électroniques massives, notamment de courrier électronique, non sollicitées par les destinataires, à des fins publicitaires ou malhonnêtes :
Par exemple, votre adresse de courrier électronique peut avoir été collectée sur un site internet grâce à un logiciel « aspirateur » de courriers électroniques.

Le plus souvent :
• ces messages n'ont pas d'adresse valide d'expédition ou de "reply to"
• l'adresse de désinscription est inexistante ou invalide.

Transmettre un message

Chaque fois que vous retransmettez un message, vous véhiculez des informations sur les personnes qui ont eu le message avant vous : nom, surnoms et même parfois l'adresse surtout leur adresse courriel.

Attention aux chaînes. Toutes les fois que vous recevez un message à transférer à 10 personnes et + « sinon la malchance s'abattra sur vous », il y a de fortes possibilités que ledit message cache un programme espion qui retrace les cookies. L'auteur du message original recevra une copie chaque fois que le message sera retransmis et sera capable d'extraire toutes les adresses des courriels.

Certains récupèrent ces adresses pour les revendre, ou vous envoient un courriel pour vous faire visiter leur site. A chaque fois que vous cliquez sur le site, ils touchent une certaine somme.

Attention aux pétitions : sur le même principe que pour les chaînes. Une pétition électronique sérieuse mentionne toujours un site web qui permettra d'avoir:

- Des informations sur l'auteur qui est à l'origine de la pétition,
- Les faits mentionnés dans la pétition
- La possibilité de signer la pétition sur le site
- La possibilité de connaître le résultat de l'action et un contact si on veut plus d'informations.

Conseils :

1. Avant de transmettre un message, il est impératif de faire disparaître les noms et adresses de la personne qui vous a envoyé le message.

2. Utilisez toujours le bouton « Transmettre », de la page sur laquelle vous lisez votre message, vous éviterez ainsi à votre correspondant d'avoir à passer en revue toutes les autres pages adressées précédemment.

3. Lorsque vous envoyez un mail à plusieurs personnes, prenez l'habitude d'employer la case CCI – Copie Carbonne Invisible - : de cette façon, seule la personne à qui vous écrivez aura son adresse apparente.

4. Attention aux fichiers joints dont l'extension se termine par exe ceux-ci peuvent être détruits par certain antivirus. Prenez la précaution de les compresser avant de les envoyer.

5. Avant de faire suivre un message d'alerte comme une recherche de personne ou la propagation d'un quelconque virus, visitez ce site **http://www.hoaxbuster.com**

   Celui-ci répertorie, analyse et informe sur la véracité du contenu de ces messages : vrai ou faux.