Faire attention au contenu des mails

Il y a deux types de mails auxquels il faut faire attention :

- les mails de tentative d'arnaque
- les mails avec pièces jointes

Commençons par parler des mails de type arnaque :

Vous êtes à la caisse d'épargne et vous recevez un mail qui semble tout ce qu'il y a de plus officiel vous demandant de rentrer pour des raisons de maintenance toutes vos coordonnées bancaires sur le site après avoir cliqué dans le lien donné dans le message ? C'est très certainement un faux, et vous risquez si vous le faite de voir s'envoler ailleurs tout votre argent.

C'est ce qu'on appelle le phishing, ou hameçonnage en français. Cette technique est utilisée par les fraudeurs afin de vous soutirer des informations personnelles (identifiants, mots de passe, numéro de carte de crédit, date de naissance, …) dans le but de se faire passer pour vous. Cela consiste à se faire passer pour un organisme de confiance (sa propre banque, Paypal, …) afin de vous soutirer ces informations. Le phishing existe sous deux formes : par mail et sur des sites Internet. Et bien souvent, c'est un mail qui vous fait aller sur un site Internet frauduleux.

Petite leçon à connaitre : votre banque ou toute autre organisation ne vous demandera jamais vos identifiants par email !

Si vous avez un doute, n'hésitez pas à aller sur le site officiel de la banque / de l'organisation / de l'entreprise concernée (en passant par Google, pas en cliquant sur les liens dans le mail bien entendu). Allez ensuite voir si ce site dispose d'une rubrique avec des actualités afin de voir s'il n'y a pas une vague de tentative d'arnaque par mail. Si le site ne dispose pas d'actualités, n'hésitez pas à les contacter (toujours en passant par le site officiel, un numéro donné dans un mail de ce type peut aussi être frauduleux) afin d'obtenir plus de renseignements, ou pour demander si le mail reçu est légitime.

Il existe un autre moyen de vérifier l'authenticité du message :

Souvent, les liens inclus dans ces messages sont faux, et il est facile de le voir. Regardons avec un exemple :

Déjà, ce mail a quelques problème avec les lettres accentuées (il n'y en a aucune comme vous pourrez le remarquer). De plus, la traduction depuis l'anglais est imparfaite (voir cadre orange de l'image ci-dessus). Enfin, si vous passez la souris au dessus des liens qui sont dans ces mails, vous verrez dans votre logiciel de messagerie (ou sur le site sur lequel vous êtes pour lire vos e-mails) que l'adresse du site est très louche (voir cadre bleu). Par exemple dans ce mail, la première partie de l'adresse qui est l'adresse réelle du site, c'est « womum.co.nz », ce qui n'a aucun rapport avec Paypal.

Parmi les mails auxquels il faut faire attention, il y a ceux contenant des pièces jointes.

Première règle de base, n'ouvrez pas une pièce jointe d'un mail dont vous ne connaissez pas l'expéditeur !

Et même si vous connaissez l'expéditeur, il faut aussi se méfier : il existe de nombreux virus qui regardent le carnet d'adresse des gens pour s'envoyer automatiquement en pièce jointe chez les personnes du carnet d'adresse. Du coup, vous pourriez très bien recevoir un mail d'une personne que vous connaissez très bien, mais qui contient un virus.

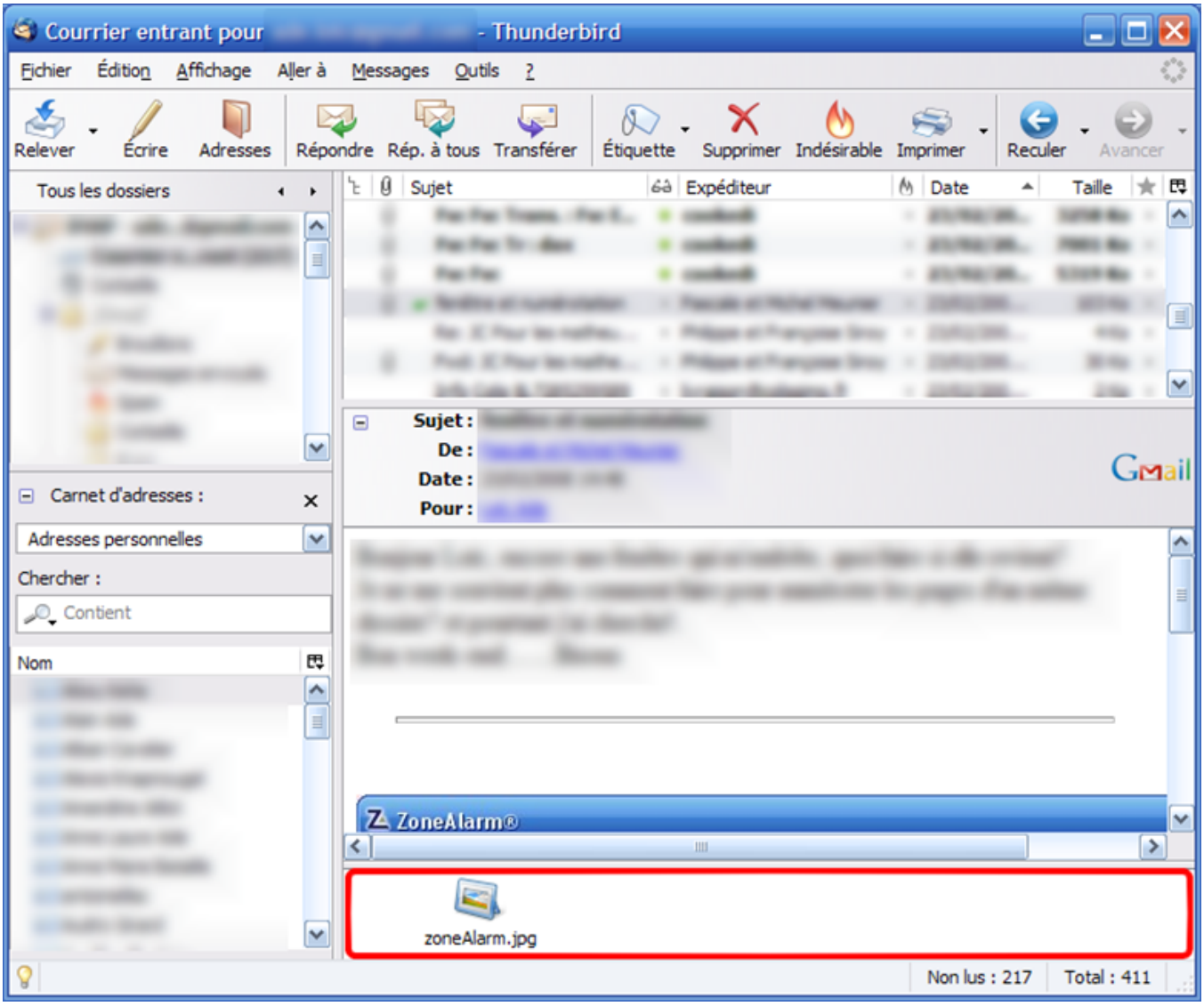
Il y a plusieurs signes permettant de détecter ça :

- le mail est écrit en anglais alors que la personne ne comprend pas un mot de cette langue (valable pour

n'importe quelle autre langue que l'anglais)
- le mail est écrit en français parfait alors que la personne écrit toujours ses mails en SMS
- l'inverse, donc que le mail soit écrit en SMS alors que la personne emploie toujours un français parfait.
- vous avez reçu plusieurs fois le même mail louche

Autre moyen de faire attention avec les pièces jointes :

Si l'icône ne correspond pas au nom du fichier indiqué. Par exemple, l'icône de la seule pièce jointe du mail ci-dessous correspond bien à l'icône d'une image. De plus, l'extension jpg du nom du fichier (zonealarm.jpg) correspond bien à une image.



La plupart des logiciels de messagerie affichent le nom complet d'un fichier dans la liste des pièces jointes, ainsi que de nombreux services de messagerie (Windows Live Hotmail, Yahoo mail, GMail, …).

De cette façon, vous pouvez voir si les pièces jointes sont suspectes.

Voici une liste des extensions de pièces jointes suspectes :

- .exe

- .com
- .pif
- .cmd
- .bat
- .vbs
- .msi

Il y a quelques exceptions : les fichiers compressés, qui peuvent contenir d'autres fichiers. Dans ce cas là, il faut regarder l'extension de chaque fichier à l'intérieur de ce fichier compressé. Les fichiers compressés les plus répandus ont pour extension :

- .zip
- .rar
- .7z

Il existe d'autres formats de compression, mais il est peu probable que vous les trouviez en pièce jointe de mails.

L'extension d'un fichier, c'est les quelques dernières lettres qui suivent le dernier point dans le nom d'un fichier. Malheureusement, Windows n'affiche pas automatiquement toutes les extensions de tout les fichiers, du coup, vous ne pouvez facilement connaitre l'extension d'un fichier dans l'explorateur Windows. Cependant, certains logiciels comme les logiciels de messagerie les affichent. C'est aussi à double tranchant : si vous avez un doute sur un fichier, que celui-ci affiche par exemple une extension « .jpg » et que l'icône est correcte, vérifiez sur d'autres mails sûr que le logiciel affiche bien l'extension.

De plus, le fait que ce soit une extension « .jpg » (extension correspondant à une image, souvent une photo) ne signifie en rien que le fichier soit sûr, car il existe des virus qui exploitent des failles de sécurité dans Windows afin de s'introduire dans votre ordinateur. Ces virus peuvent se cacher dans des images et le simple fait d'afficher / d'ouvrir la photo peut vous infecter !

Les images aux formats EMF et WMF sont parfois vecteurs de virus. Donc si vous en recevez par mail, ne les ouvrez surtout pas à moins d'être vraiment sûr. Car très rares sont les personnes susceptibles de générer des images dans ces deux formats.

Bref, n'ouvrez jamais une pièce jointe de quelqu'un que vous ne connaissez pas. Car n'importe quel fichier peut abriter n'importe quel virus.

Si vous avez un doute sur la légitimité d'un message, n'hésitez pas à contacter (uniquement dans le cas ou vous connaissez la personne) l'expéditeur du mail pour savoir si le contenu d'un message est légitime.