N’ayez pas une confiance aveugle dans le nom de l’expéditeur

N’importe qui peut vous envoyer un courriel en se faisant passer pour un autre ! Cela n’est pas beaucoup plus compliqué que de mettre un faux nom d’expéditeur au verso d’une enveloppe.

Soyez donc attentif à tout indice mettant en doute l’origine réelle du courriel, notamment si le message comporte une pièce jointe ou des liens : incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie d’habitude, par exemple. En cas de doute, contactez votre interlocuteur pour vérifier qu’il est à l’origine du message.

Et même si l’expéditeur est le bon, il a pu, à son insu, vous envoyer un message infecté. Vous devez admettre que dans le domaine de la messagerie électronique, il n’existe pas d’expéditeur a priori de confiance.

Méfiez vous des pièces jointes

Elles peuvent contenir des virus ou des espiogiciels.

Assurez vous régulièrement que votre anti-virus est activé et à jour.

Si votre poste a un comportement anormal (lenteur, écran blanc sporadique, etc.), faites-le contrôler.

Ne répondez jamais à une demande d’informations confidentielles

Les demandes d’informations confidentielles, lorsqu’elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.). En cas de doute, là encore, demandez à votre correspondant légitime de confirmer sa demande.

Car vous pouvez être victime d’une tentative de filoutage, ou phishing. Il s’agit d’une technique utilisée par des personnes malveillantes, usurpant généralement l’identité d’un tiers ou simulant un site dans lesquels vous avez a priori confiance (une banque, un site de commerce, etc.) dans le but d’obtenir des informations confidentielles, puis de s’en servir.

Les messages du type chaîne de lettres, porte-bonheur ou pyramide financière, appel à solidarité, alerte virale, ou autres, peuvent cacher une tentative d’escroquerie. Évitez de les relayer, même si vous connaissez l’expéditeur.

Passez votre souris au dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français dans le texte ou de la langue pratiquée par votre interlocuteur

En passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncé dans le message. Si l'adresse est différente, soyez méfiant, et évitez de cliquer sur le lien. De manière générale, il est préférable de saisir manuellement l'adresse dans le navigateur.

Dans la plupart des tentatives de filoutage, notamment lorsqu'elles viennent de l'étranger et que le texte a été traduit par un logiciel, l'orthographe et la tournure des phrases sont d'un niveau très moyen, et les caractères accentués peuvent être mal retranscrits. Toutefois, on constate qu'un nombre croissant de tentatives de filoutage emploie un français correct. Soyez donc le plus vigilant possible lors de la réception de tels messages.

Paramétrez correctement votre logiciel de messagerie

Mettez à jour vos logiciels, si possible en activant la procédure de mise à jour automatique

Paramétrez votre logiciel de messagerie pour désactiver la prévisualisation automatique des courriels

Dans les paramètres de sécurité en options, interdisez l'exécution automatique des ActiveX et des plugins et les téléchargements, soit en les désactivant, soit en imposant de vous en demander l'autorisation

Dans un environnement sensible, lisez tous les messages au format texte brut.