Réflexes à avoir lors de la réception d'un courriel

24 rue du Gabian
98000 MONACO
Tél. : (+377) 98 98 24 93
amsn@gouv.mc

CINQ REFLEXES A AVOIR LORS DE LA RECEPTION D'UN COURRIEL

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.

1. N'AYEZ PAS UNE CONFIANCE AVEUGLE DANS LE NOM DE L'EXPÉDITEUR

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**.

2. MÉFIEZ-VOUS DES PIÈCES JOINTES

Elles peuvent contenir des virus ou des espiogiciels. Assurez-vous régulièrement que votre antivirus est activé et à jour. Si votre poste a un comportement anormal (lenteur, écran blanc sporadique, etc.), faites-le contrôler par votre service informatique.

3. 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, par un autre moyen, sa demande car vous pouvez être victime d'une tentative de filoutage ou de « 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.**

4. 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 annoncée 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.

5. PARAMÉTREZ CORRECTEMENT VOTRE LOGICIEL DE MESSAGERIE

- Assurez-vous que vos logiciels sont à jour, 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, des plug-ins et autres, et les téléchargements, soit en les désactivant, soit en imposant de vous en demander l'autorisation ;
- dans un environnement sensible (manque de confiance, risque important de compromission ou d'attaque), lisez dans la mesure du possible tous les messages au format texte brut (le format HTML est un vecteur important de compromission).