Des réflexes simples pour vous protéger des mails frauduleux

Les mails frauduleux sont de plus en plus fréquents et demandent une vigilance accrue dans le traitement de sa messagerie. Voici 9 réflexes à adopter afin d'éviter d'être piégés.

1. Vérifiez l'adresse de l'expéditeur

Lorsque vous recevez un courriel prétendant être envoyé par les services académiques, si l'adresse ne se termine pas par "@ac-amiens", il s'agit très certainement d'un e-mail frauduleux.
Cependant, il est facile de modifier l'adresse e-mail de l'émetteur : cette information n'est pas suffisante en elle-même pour être sûr de la provenance de l'e-mail.

2. Ne donnez jamais votre identifiant et votre mot de passe académique

Si vous recevez un courriel vous demandant de renseigner vos identifiants académiques, c'est une fraude. En aucun cas les services académiques ne vous demanderont ces informations.

3. N'ouvrez pas la pièce jointe si vous avez un doute au sujet de l'expéditeur

Les pièces jointes peuvent contenir des virus ou des logiciels espions. Ne les ouvrez que si l'expéditeur est de confiance.

4. Lisez attentivement le texte

Si vous observez des traductions aléatoires avec des termes incorrects ou des fautes d'orthographe évidentes, il s'agit sans doute d'un e-mail frauduleux.

5. Méfiez-vous des formules génériques

Redoublez de vigilance avec les e-mails comportant des salutations impersonnelles comme « *Cher utilisateur* » ou « *Cher votre-adresse@e-mail.com* ».

6. Restez calme

Les e-mails frauduleux ont un caractère d'urgence : ils sont conçus pour vous pousser à agir dans la précipitation et oublier les règles de sécurité élémentaires.

7. Vérifiez les liens

Ils semblent corrects, mais peuvent vous induire en erreur. Passez votre souris sur le lien ou sur le bouton contenu dans l'e-mail pour voir l'adresse (URL) s'afficher. Si elle vous semble suspecte, **ne pas cliquer sur les liens** : les liens affichés dans les courriers électroniques peuvent en réalité diriger les internautes vers des sites frauduleux. En cas de doute, il est préférable de saisir manuellement l'adresse dans le navigateur.

8. Apprenez à détecter le filoutage (phishing)

Le document de la division informatique ci-joint est à lire attentivement. Il décrit le filoutage Internet et explique comment ne pas se faire piéger.

9. Envoyez vos mails en utilisant "Cci" :

Lorsque vous envoyez des courriels à plusieurs destinataires, pensez à entrer les adresses dans le champ "Cci" (copie cachée invisible). Ces destinataires ne verront que votre adresse, pas celle des autres. Ainsi, si l'un de ces destinataires a un malware ou un virus sur son PC, cela évitera que les adresses ne soient récupérées et utilisées pour générer du spam.

En cas de problème, prendre contact rapidement avec la division informatique :

Division informatique Laon : 03 23 26 22 46 ; cdti02@ac-amiens.fr
Plateforme académique : 03 22 82 37 40 ; plateforme.assistance@ac-amiens.fr

Jean-Philippe Mary – ERUN – Circonscription du Soissonnais