Aide pédagogique à l'utilisation des ressources numériques

Office 365 : Courriel et sécurité

Il n'est pas rare de découvrir dans sa boite de courriel de curieux messages. Hoax[1], spam, pourriel, virus, cheval de Troie, phishing, … autant d'occasions d'être piégé par des personnes malveillantes. Ceci nous invite à vous conseiller ces quelques comportements à adopter face à des situations critiques[2].

Les **logiciels malveillants** peuvent provenir, en apparence, d'une personne que vous connaissez.
Ils vous trompent pour que vous les ouvriez.

- Ouvrez uniquement les pièces jointes attendues et issues de sources sûres.
- Supprimez tous les messages indésirables sans les ouvrir.
- Vérifiez la correspondance entre l'adresse affichée de l'expéditeur et l'adresse d'envoi réelle.
- Ne jamais cliquer sur un lien dans un courriel sauf si celui-ci est assurément légitime. En cas de doute, survolez (pas cliquer) le lien avec votre souris (voir ci-dessous) afin d'afficher le lien caché derrière le nom de l'adresse.

Dans l'exemple ci-dessus, le lien affiché ne correspond pas à iCampus mais à un lien vers un script dangereux.

Certains messages de **spam** peuvent contenir des propos injurieux ou des liens vers des sites Internet inappropriés.

- Si vous pensez qu'un message électronique est un spam, n'y répondez pas, contentez-vous de le supprimer.
- Vous pouvez aussi le déclarer comme courrier indésirable et bloquer l'expéditeur.
- Si un courrier valide se retrouve dans votre dossier des courriers indésirables, déclarez-le comme courrier légitime.

Les initiateurs d'attaques par **phishing** envoient parfois des messages alarmistes pour vous inciter à répondre sans réfléchir

Les attaques par phishing reposent généralement sur une série de messages électroniques présentant un certain nombre de points communs (les en-têtes et les pieds de page sont de bons indicateurs).

- Traitez avec la plus grande méfiance les messages électroniques vous demandant de fournir des informations confidentielles.
  Les organismes officiels, les banques et les fournisseurs de logiciels ne vous demanderont jamais ces informations par courriel.
- Vérifiez l'authenticité d'une demande suspecte avant de répondre par courrier électronique.

[1] Pour vérifier ces informations fausses qui circulent via les courriels, consultez le site http://www.hoaxkiller.fr/
[2] Inspirés du site http://be.norton.com/security_response/secureemail.jsp