Vigipirate - Sécurité du numérique, l'hameçonnage

samedi 13 octobre 2018, par MARTENS MARIE-AGNES (Date de rédaction antérieure : 1 av. J.C.).

Voici deux extraits de la fiche°4-« Vigipirate sécurité du numérique », extraits choisis parce qu'ils nous concernent tous, professeurs et personnels, à titre personnel ou en tant que professionnels d'un établissement public, mais aussi élèves et parents. A lire avec attention.

SÉCURITÉ DU NUMÉRIQUE
L'HAMEÇONNAGE (OU PHISHING)

Comment renforcer ma vigilance et bien me protéger ?

Qu'est-ce que l'hameçonnage ?

L'hameçonnage est une technique d'attaque prenant la forme d'un courriel qui vous est adressé et qui semble provenir d'un expéditeur de confiance. Ce courriel peut contenir un **fichier**, une **pièce jointe** ou un **lien de redirection vers un site frauduleux**, avec une incitation à cliquer sur ces éléments, ce qui permettra à l'attaquant de recueillir de l'information ou d'installer un programme malveillant dans le système d'information de votre organisme.

Adopter les bonnes pratiques au quotidien

- Méfiez-vous des courriels exigeant de vous une réponse ou une action immédiate et vous intimant de ne pas en informer votre hiérarchie ou vos collaborateurs.
- Soyez prudents vis-à-vis des courriels comportant des visuels a priori officiels mais dont la résolution est mauvaise.
- Ne cliquez jamais sur un lien ou une pièce jointe dont l'origine ou la nature vous semblent douteuses. **Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse** dans la barre de recherche.
- Soyez à l'affût des fautes d'orthographe ou de syntaxe dans l'adresse de l'expéditeur, l'objet du courriel ou le corps du texte.
- Ne répondez jamais à un courriel vous demandant des informations confidentielles (identifiants, coordonnées bancaires, etc.). **Au moindre doute, n'hésitez pas à contacter l'expéditeur** par un autre canal, par exemple téléphonique.
- Méfiez-vous des courriels d'expéditeur connu mais dont l'adresse électronique ou la nature du message sont inhabituelles ou catégorisés comme « spam / indésirable » par le logiciel de messagerie.
- Procédez régulièrement au redémarrage de votre poste, notamment lorsque le système vous y invite.

Je pense avoir été victime d'une attaque. Que faire ?

Qui prévenir ?

Si vous pensez avoir été victime d'une attaque informatique :

- prévenez immédiatement le support informatique de votre organisme et vos supérieurs hiérarchiques ;
- procédez sans délai au renouvellement de vos identifiants si vous les avez transmis lors de l'attaque.

Pour nous, professeurs, le signalement peut se faire sur le site de l'observatoire Académique de la Sécurité de l'Information OASI.
où l'on peut suivre l'actualité de la sécurité du numérique dans l'académie (vous pouvez y trouver aussi les informations sur l'antivirus gratuit pour le personnel, voir article 891 à ce sujet.)