HELMO
Haute Ecole
Libre Mosane

Identifier et réagir à un e-mail frauduleux

Réagir à un e-mail frauduleux

Si vous avez répondu à un message frauduleux veuillez changer votre mot de passe sans tarder.

Si vous n'y avez pas répondu, ignorez simplement le message et supprimez-le.

Identifier un e-mail frauduleux

Le SPAM représente du courrier indésirable. Il est envoyé:

- par des entreprises qui espèrent, de cette façon, atteindre de nouveaux clients.
- par des attaquants qui espèrent obtenir des informations personnelles (carte de crédits, code pin, mot de passe, ...). On parle alors d'hameçonnage ou de phishing

Le SPAM est difficile à détecter automatiquement. En effet, cela nécessite la mise en place de nombreuses techniques. De plus, le SPAM évolue sans cesse (notamment avec l'arrivée des IA comme ChatGPT) et les techniques pour le combattre doivent également suivre.

A HELMo, plusieurs moyens de protection sont en place pour détecter un spam. Voici les **redflag** à identifier :

- Le mail indique **une personne de HELMo mais le sujet mentionne [EXTERNE]** -> soyez très prudent car le mail n'a pas suivi le chemin attendu. Vérifiez correctement l'adresse de l'expéditeur.
- Un message du type **Vous ne recevez pas beaucoup de courrier de ...** est ajouté au texte du mail -> soyez prudent quant au contenu du mail.
- Le **sujet du mail mentionne [SPAM]** => Il faut être prudent quant au contenu du mail
- On **vous demande une action urgente** (pouvons-nous payer aujourd'hui ...) => probablement mail de spam
- Les liens dans les mails sont toujours à considérer avec beaucoup de précaution. A HELMo, la plupart du temps, ils sont analysés par Microsoft.

Il faut savoir que le service informatique ne communique jamais de mot de passe ou d'information confidentielle par mail simple.

Un autre indice important est l'adresse e-mail de l'expéditeur. Outre le nom affiché, vérifiez que le nom de domaine après le symbole @ appartient bien à l'entreprise à laquelle l'émetteur prétend appartenir. Méfiance cependant, certains fraudeurs introduisent une adresse e-mail fictive à la place de leur nom, ce qui peut vous laisser croire qu'il s'agit de l'adresse de l'expéditeur.

Par prudence, **en cas de doute, il vaut toujours mieux vérifier auprès du service informatique avant d'encoder vos identifiants.** Il faut rester vigilant face au courrier que l'on reçoit et face à son utilisation de l'outil informatique.

Liens utiles

- Testez vos réflexes face au hameçonnage : https://www.safeonweb.be/fr/quiz/test-du-phishing
- Microsoft a publié un article intéressant sur les bons réflexes à adopter face aux tentatives d'hameçonnage : https://aka.ms/LearnAboutSenderIdentification

Pourquoi recevez-vous du SPAM ?

Détecter un SPAM est assez difficile. En fait, le système informatique doit deviner si le courrier en question est, ou non, un SPAM. Pour ce faire, il va analyser le contenu du courrier et, attribuer un score à chaque mail. Les règles d'attribution des points pour le score sont proposées et déterminées par l'administrateur. Le score obtenu détermine si le courrier est :

- un courrier normal. Le score obtenu est alors faible.
- un SPAM probable. Le score obtenu est moyen et le système ajoute dans l'en-tête du courrier les mots [SPAM]. Il faut bien comprendre que dans ce cas, le système n'est pas sûr qu'il s'agit d'un SPAM.
- un SPAM certain. Le score obtenu est élevé et, dans ce cas, le système supprime le courrier en question.

Détecter correctement le SPAM revient à choisir les points pour chaque règle et le seuil pour déterminer si le courrier est normal, SPAM probable ou SPAM certain. Il est toujours possible de durcir les règles et modifier les seuils. Cependant, ces modifications ne sont pas anodines car elles pourraient conduire à décider qu'un courrier normal est un SPAM probable ou qu'un SPAM probable est un SPAM certain et dès-lors, conduire à la non réception de mails pourtant légitimes.

Pourquoi recevez-vous plus de SPAM qu'un autre ?

Pour envoyer du SPAM, il faut disposer des adresses mails valides. Ainsi, vous risquez de recevoir davantage de SPAM si:

- votre adresse mail est mentionnée sur le serveur web de la haute école
- vous utilisez votre adresse mail HELMo pour vous enregistrer sur des sites sur internet
- vous utilisez votre adresse mail HELMo dans des listes de diffusion
- vous mentionnez votre adresse mail HELMo sur les réseaux sociaux tels que Twitter, Facebook, Netlog, ...

Comment vous protéger mieux contre le SPAM?

Bien sûr, la première chose à faire est de ne pas trop exposer son adresse mail, si c'est possible (ne pas enregistrer son adresse mail HELMo sur n'importe quel site par exemple).

La seconde chose à faire est d'utiliser un client mail adéquat. Ainsi, Microsoft Outlook ou encore Mozilla Thunderbird sont largement recommandés car ils disposent chacun de filtres antispam intégrés et fonctionnels. Dans Outlook par exemple,

vous pouvez d'ailleurs affiner le niveau de filtrage souhaité (menu Outils > Options > Courrier indésirable, il est possible de choisir le niveau de filtrage souhaité). Il est important de souligner que les remarques ci-dessus sont d'application dans Outlook.

La troisième chose importante est de rester vigilant. En effet, le mail est une application non sécurisée. Ainsi, vous ne pouvez jamais être sûr de l'expéditeur d'un mail sauf si ce dernier signe son mail numériquement.

Sécuriser mes appareils et identifiants

Retrouvez d'autres informations essentielles pour améliorer la sécurité de vos données dans cet article.
