Objet : Note de service - STI :

1. Capsules d'informations – Nous sommes tous vulnérables

Saviez-vous que « L'**hameçonnage**, ***phishing*** ou **filoutage** est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. »
Dans un tel cas, le plus souvent, une copie d'un site internet est réalisée dans le but de faire de vous une victime et de vous faire croire que vous êtes bien sur le site internet officiel d'un organisme ou d'une entreprise que vous connaissez ou qui vous semble être de confiance. Le courriel vous incite à confirmer des renseignements personnels ou confidentiels, en cliquant sur un lien. Les renseignements demandés peuvent alors être enregistrés sur le site des fraudeurs, ou encore un programme malveillant peut être lancé à votre insu et enregistrer ce que vous tapez sur le clavier de votre poste de travail, y compris, notamment, les identifiants et mots de passe.

Un événement concret est arrivé à un employé de l'UQAC en décembre dernier : un courriel semblant provenir d'un service de messagerie visait à obtenir des informations complémentaires pour la livraison d'un colis. Cette demande lui paraissait plausible, elle a donc donné l'information demandée.
Quelque temps plus tard, quelques milliers de dollars étaient retirés de son compte bancaire. Le site sur lequel elle a été dirigée était tellement réaliste que la victime s'est rendu compte de la fraude seulement lors de l'accès au site de son institution financière.
Prenant conscience du possible hameçonnage, la victime a contacté le service de messagerie qui a confirmé l'usurpation de leur site internet à des fins frauduleuses.
L'institution financière, suite à une enquête, a remboursé la victime.
Heureusement, l'histoire se termine bien, cependant ce n'est pas toujours le cas.

Voici quelques règles de base à appliquer lors de la réception d'un courriel :

- Ne remplissez jamais une demande de données personnelles, si celle-ci vous parvient par courriel.
- Ne cliquez jamais sur des liens ou images d'un courriel vous demandant des informations personnelles ou de nature confidentielle.
- Au besoin, n'hésitez pas à contacter une entreprise si vous avez des doutes sur la provenance du courriel.
- N'ouvrez pas les pièces jointes d'un courriel provenant d'une source inconnue.
- Soyez aux aguets si certains des éléments suivants sont présents. Ils peuvent être révélateurs d'une tentative d'hameçonnage:
  - La qualité de la langue écrite ne reflète pas le professionnalisme de la prétendue entreprise.

- Le lien de la page Web indiqué dans le courriel pour entrer vos données possède une adresse différente du site sur lequel vous vous attendiez à être redirigé.
- L'adresse courriel de l'expéditeur provient d'un fournisseur tel Gmail, Hotmail, Yahoo etc.
- L'affichage des images est à basse résolution. Certains fraudeurs créent de faux sites rapidement, et cela se voit souvent à la piètre qualité du site. Si le logo ou le texte est affiché à un niveau de résolution faible, il est fort probable que le site ne soit pas le site officiel de l'organisme ou de l'entreprise prétendue.

Malgré ces quelques règles de base, n'hésitez pas à contacter votre service des technologies de l'information, si vous croyez avoir été hameçonné ou être en présence d'un programme malveillant sur votre poste de travail. Votre vigilance peut faire toute la différence.

En conclusion, voici certaines recommandations importantes, en tout temps :

- Saisissez vos informations personnelles uniquement dans une page Web sécurisée d'une institution ou entreprise que vous connaissez. Vous saurez si une page web est sécurisée si celle-ci possède une adresse commençant par « https:// » et si l'icône d'un cadenas fermé apparait à gauche de l'adresse du site. Vous pouvez cliquer sur cette icône afin de voir le certificat de sécurité du site.
- Utilisez des mots de passe différents pour chaque site fréquenté.
- Protégez vos mots de passe et ne les révélez à personne.
- Changez fréquemment vos mots de passe.

Renseignements :
Service des technologies de l'information
Université du Québec à Chicoutimi
418 545-5011, poste 6000 | Capsules_Securite@uqac.ca

UQAC