BUREAU DE LA SÉCURITÉ DE L'INFORMATION

Six meilleurs moyens de détecter une tentative d'hameçonnage

Qu'est-ce que l'hameçonnage et comment le détecter?

L'hameçonnage est une tentative, généralement menée par courriel, de recueillir des renseignements personnels ou de compromettre une technologie dans le but d'en tirer un gain financier ou de réaliser des activités malveillantes. Les courriels d'hameçonnage contiennent habituellement un lien vers un site frauduleux ou une pièce jointe contenant un logiciel malveillant. Chaque jour, des millions de courriels d'hameçonnage sont envoyés dans le monde à des victimes qui ne se doutent de rien. Certains de ces courriels frauduleux sont faciles à détecter, mais d'autres sont plus difficiles à déjouer. Comment discerner un courriel légitime d'une escroquerie? La tâche n'est pas toujours facile et il n'existe pas de recette miracle. Il nous incombe à tous de protéger l'entreprise, notamment en apprenant comment repérer une tentative d'hameçonnage, car le meilleur moyen de ne pas mordre à l'hameçon est de savoir le repérer.

1 **Le message contient un hyperlien suspect ou incongru :** Si vous avez un doute, vérifiez toujours l'intégrité des hyperliens intégrés. Les hyperliens associés à une tentative d'hameçonnage peuvent avoir l'air tout à fait légitimes, mais si vous survolez le lien avec le curseur de votre souris, vous verrez l'adresse de destination véritable.

2 **Le message contient des fautes de frappe et de grammaire :** Lorsqu'une société d'envergure envoie un courriel en son nom, elle prend des mesures pour vérifier qu'il ne contient pas d'erreur et qu'il est conforme à la loi. Un courriel rempli de fautes d'orthographe ne provient probablement pas du service juridique d'une grande entreprise. Cela dit, ce ne sont pas tous les courriels d'hameçonnage qui contiennent ce type d'erreurs.

3 **On vous demande de fournir des renseignements personnels comme un mot de passe :** Une société respectable ne vous demandera jamais d'envoyer ou de confirmer un mot de passe ou des renseignements de connexion par courriel ni de cliquer sur un lien qui vous mènera à un site Web où ouvrir une session. Si vous doutez de l'authenticité d'un courriel, faites une recherche pour trouver le site officiel de l'entreprise ou ses coordonnées.

4 **Vous n'attendez rien de l'expéditeur :** Vous avez remporté un superbe prix ou un concours! Mais, à bien y penser, avez-vous participé à un concours? Une société financière vous envoie une feuille de calcul que vous lui avez supposément demandée, mais est-ce vraiment le cas? Il y a fort à parier qu'il s'agit de courriels d'hameçonnage. Les pièces jointes à un courriel peuvent compromettre et infecter non seulement votre ordinateur mais toute l'entreprise.

5 **Vous devez agir sans délai :** Les messages qui vous incitent à répondre rapidement pour éviter de perdre de l'argent ou un droit d'accès, ou pour éviter qu'un compte ne soit supprimé, cherchent habituellement à vous faire agir sans réfléchir. Prenez le temps de mener votre enquête; surtout ne cédez pas à la pression. Les courriels d'hameçonnage contiennent souvent une incitation à agir le plus rapidement possible pour éviter que vous preniez le temps de penser.

6 **Il y a quelque chose qui cloche :** Ce serait génial de couvrir tous les types de tentative d'hameçonnage ici, mais la vérité est la suivante : le meilleur moyen de se protéger contre les fraudeurs est de s'en remettre au bon sens. Si quelque chose vous semble louche, apprenez à faire confiance à ce sentiment. Une tentative d'hameçonnage est une forme d'ingénierie sociale dans laquelle on cherche à manipuler votre esprit, vous devez donc faire preuve de vigilance.

Si vous pensez avoir identifié un courriel d'hameçonnage, ne l'ignorez pas!

N'ouvrez pas le message et supprimez-le définitivement (allez aussi dans votre corbeille pour le supprimer complètement). Vous pouvez vérifier si le message provient de Fidelity en écrivant à FICCustService@fidelity.ca.

FCAN-1014049 09/22