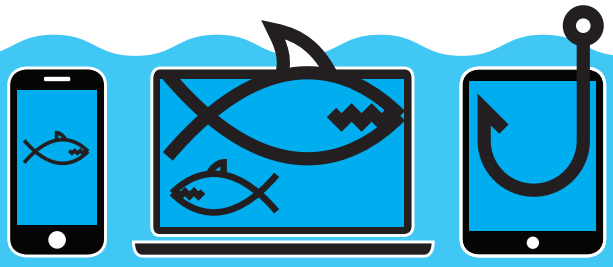
HEC MONTRÉAL

HAMEÇONNAGE



L'hameçonnage est une technique frauduleuse utilisée 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. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par des courriers électroniques, par des sites web falsifiés ou par divers moyens électroniques.

A ADRESSE ÉLECTRONIQUE. Soyez vigilant et vérifiez l'adresse courriel. Si l'adresse semble provenir de HEC Montréal, mais que l'adresse courriel de la source « FROM » est une adresse différente de @hec.ca, cela pourrait être le signe d'une attaque. Vérifiez également les destinataires et les personnes en copie conforme. Est-ce que ceux-ci sont des personnes que vous ne connaissez pas ou avec qui vous ne travaillez pas ?

B EXPÉDITEUR. Soyez vigilant et même si vous recevez un courriel d'un étudiant, d'un collègue ou d'un ami, cela n'est pas une certitude que c'est bien lui qui l'a envoyé. L'ordinateur de votre ami pourrait être infecté. Si vous recevez un courriel suspicieux d'une personne que vous connaissez, prenez le temps de l'appeler.

C ADRESSE GÉNÉRIQUE. Soyez vigilant et méfiant des courriels trop génériques tels que « Cher utilisateur », « À qui de droit », etc. Habituellement, une organisation légitime qui communique avec vous devrait connaître votre nom et vos informations personnelles. Questionnez-vous quant à la pertinence de cette communication.

D ORTHOGRAPHE. Soyez vigilant et méfiant des courriels contenant des fautes d'orthographe. Les courriels provenant d'organisation officielle sont vérifiés et revus avant d'être envoyés.

Sécurité de l'information

Direction des technologies de l'information

Marc-André Drapeau

Courriel : securite-info@hec.ca

Site Web : hec.ca/dti/securite

Téléphone : 514 340-7039

E ACTION IMMÉDIATE. Soyez vigilant et méfiant des courriels vous incitant à poser des actions immédiates. Généralement, les changements sont annoncés longtemps d'avance. Plusieurs stratégies tentent de créer un sentiment d'urgence auprès de l'utilisateur afin qu'il agisse sur-le-champ et commette des erreurs.

F PIÈCES JOINTES. Soyez vigilant et méfiant des pièces jointes. Ne cliquez que sur les pièces jointes dont vous êtes certain de la provenance.

G HYPERLIEN. Soyez vigilant et méfiant des hyperliens et ne cliquez que sur ceux auquel vous vous attendez. Vous pouvez aussi déplacer le pointeur de votre souris par-dessus le lien afin de valider que le lien pointe vers la destination qui est déclarée.

H RÉCOMPENSE. Soyez vigilant et méfiant des messages qui semble trop beaux pour être vrai tel que « vous venez de gagner [...] », « Vous pouvez augmenter vos fonctionnalités en cliquant ici », etc.