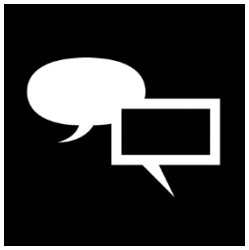
TRANSCRIPTION DE LA VIDÉO POUR L'ATELIER 2



Bonjour

Cette année, la campagne de sensibilisation permet d'approfondir notre connaissance sur le thème de la protection des informations confidentielles.

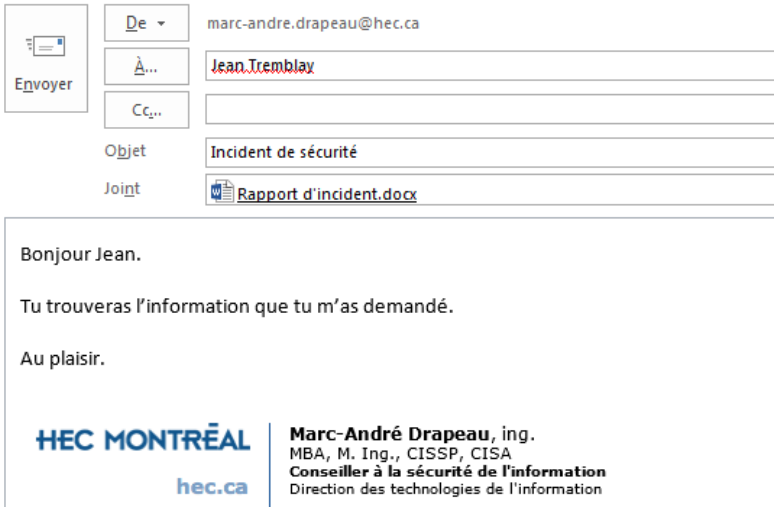
DEUXIÈME ATELIER : LA PROTECTION DE L'INFORMATION CONFIDENTIELLE LORS DES COMMUNICATIONS

Cet atelier couvre deux aspects de sécurité. Le premier consiste aux bonnes pratiques concernant l'utilisation du courriel lorsqu'il est nécessaire d'envoyer de l'information confidentielle via ce médium. Le second couvre les courriels d'hameçonnage.

Le courriel n'est pas un médium qui par défaut est sécuritaire. Lors de l'envoi d'un courriel, des copies de celui-ci peuvent se retrouver à plusieurs endroits notamment :

- sur votre poste local, dans votre boite d'envoi;
- sur le serveur de courriel d'envoi;
- sur le serveur de courriel de réception;
- sur le poste local du destinataire, dans sa boite de réception;
- dans tous les périphériques qui synchronisent vos courriels (iPhone, iPad, portable et autres);
- et possiblement sur d'autres serveurs de transition se trouvant sur l'internet.

Il devient alors important de ne pas utiliser le courriel pour communiquer de l'information confidentielle.



Regardez bien ce courriel. Que remarquez-vous ?

Nous pouvons observer qu'il y a une pièce jointe. Celle-ci porte un nom nous laissant croire que ce fichier contient de l'information confidentielle.

Aussi, le nom de votre fichier qui est en pièce jointe ne devrait pas contenir d'information confidentielle.

Par exemple, éviter des noms tels que : « Restructuration_Service_ABC.docx », « Congédiment_Monsieur_X.docx »

De plus, il est important de protéger vos pièces jointes contenant de l'information confidentielle.

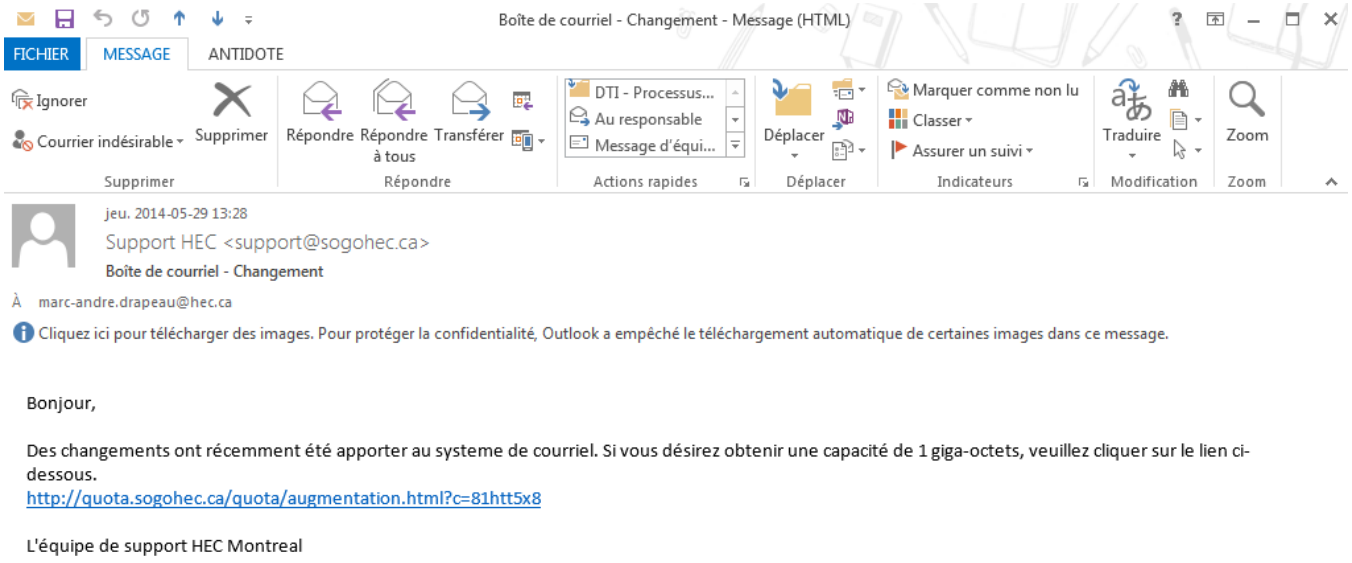
Idéalement, si vous pouvez simplement mettre un lien vers votre document, situé dans un répertoire réseau de votre secteur, cela évite que ce dernier soit transféré par courriel.

Si vous n'avez pas le choix de joindre votre fichier au courriel, vous pouvez utiliser l'outil Winzip pour protéger votre document avec un mot de passe. C'est donc le fichier protégé, produit avec l'outil Winzip, que vous pourrez joindre à votre courriel. Le mot de passe pourra ensuite être communiqué de vive voix à votre destinataire ou via un canal de communication différent.

Qu'est-ce que l'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 — votre banque, votre employeur, 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.

Maintenant, sauriez-vous reconnaître un courriel d'hameçonnage ?



Voici 8 éléments de vigilance qui vous aideront à identifier un courriel d'hameçonnage. Regardons si ces éléments nous aideront.

A Adresse courriel de l'expéditeur et des destinataires.

Si vous recevez un courriel qui semble provenir de HEC Montréal, mais que l'adresse courriel de la source est différente de @hec.ca, cela pourrait être le signe d'une attaque. Vérifiez aussi 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 ?

Dans notre exemple :

- Le courriel semble provenir de HEC Montréal, pourtant l'adresse de l'expéditeur termine par sogohec.ca et non par hec.ca.

B Expéditeur.

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 et des courriels pourraient être envoyés à l'insu de votre ami ou collègue. Ce faisant, si vous recevez un courriel suspicieux d'une personne que vous connaissez, prenez le temps de l'appeler.

C Courriel trop générique.

Si vous recevez des courriels trop génériques tels que « Cher utilisateur », « À qui de droit », etc., questionnez-vous quant à la pertinence de cette communication. Habituellement, une organisation légitime qui communique avec vous devrait connaître votre département, votre nom, votre titre et vos informations personnelles. De plus, les courriels de votre organisation devraient contenir une signature officielle.

Dans notre exemple :

- Le « Bonjour », suivi du nom « Support HEC » qui n'est pas le bon nom du service ensuite, la signature qui ne contient pas le logo de HEC Montréal ni les coordonnées pour rejoindre le service. La somme de ces éléments devrait attirer notre attention.

D Orthographe.

Si vous recevez des courriels contenant des fautes d'orthographe, cela pourrait être le signe d'hameçonnage. Les courriels provenant d'organisations officielles sont vérifiés et revus avant d'être envoyés.

Dans notre exemple :

- Plusieurs fautes d'orthographe sont présentes, telles que les mots : Apport**er**, syst**e**me, giga-octet**s**, Montr**e**al

Des changements ont récemment été apportés au système de courriel. Si vous désirez obtenir une capacité de 1 giga-octet, veuillez cliquer sur le lien ci-dessous.

E Action immédiate.

Soyez vigilant et méfiant des courriels vous incitant à poser des actions immédiates. Plusieurs stratégies tentent de créer un sentiment d'urgence auprès de l'utilisateur afin qu'il agisse sur-le-champ et commette des erreurs. Pour citer un exemple, nous observons généralement des phrases telles que « posez une action immédiate, sinon votre compte sera verrouillé dans les 24 heures ».

Généralement, les changements sont annoncés longtemps d'avance.

F Pièces jointes.

Si vous recevez un courriel contenant une pièce jointe, une question à se poser est : « Est-ce que je m'attends à recevoir une pièce jointe ».

Les pièces jointes sont souvent utilisées pour transporter des logiciels malveillants. Ce faisant, ne cliquez sur celle-ci que si vous êtes certain de la provenance. Sinon, valider avec l'expéditeur qu'il vous a bel et bien envoyé la pièce jointe.

G Hyperlien.

Les personnes malveillantes utilisent les hyperliens pour vous amener vers d'autres serveurs qui contiennent des logiciels malveillants. Par la suite, ces logiciels s'installent et infectent votre poste de travail et peuvent se répandre par le réseau pour infecter d'autres postes de travail et même, dans certains cas, des serveurs institutionnels.

Méfiez-vous des hyperliens et ne cliquez que sur ceux auquel vous vous attendez. Pour vérifier où pointe l'hyperlien, vous pouvez déplacer le pointeur de votre souris par-dessus le lien afin de valider que le lien pointe vers la destination qui est déclarée.

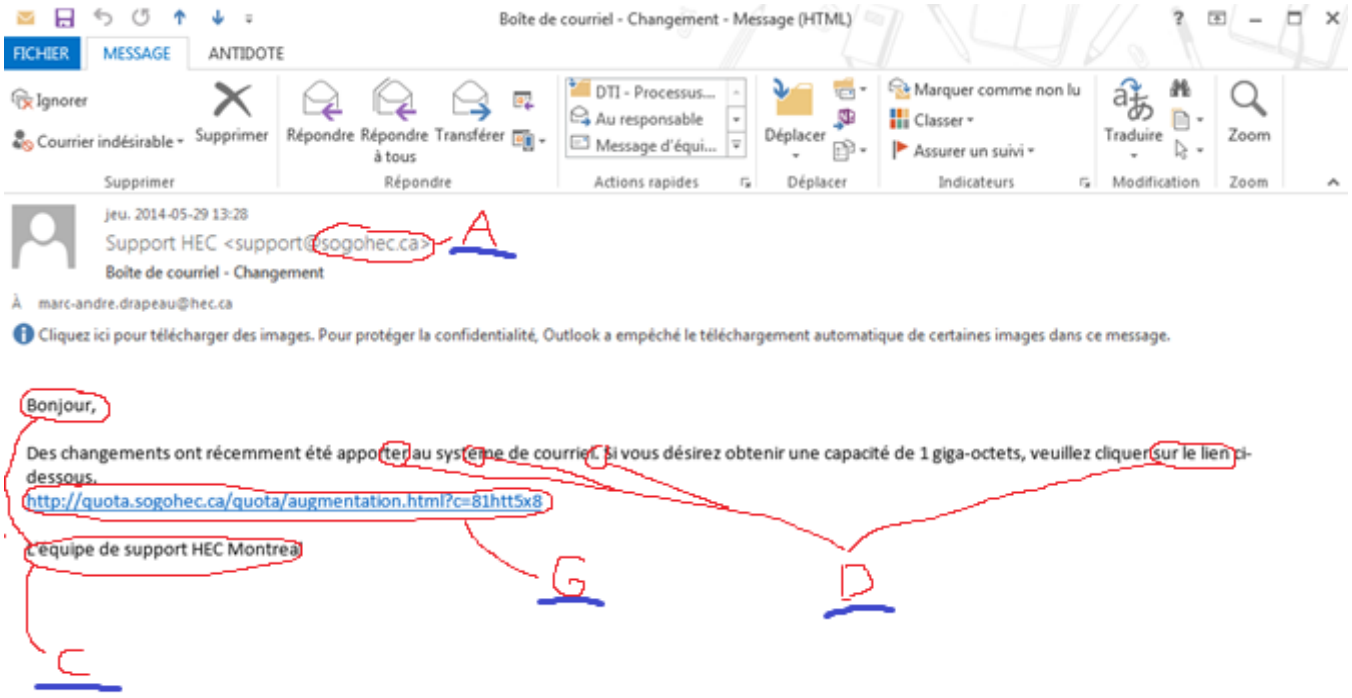
Dans notre exemple :

- Nous recevons un courriel officiel de HEC Montréal qui nous demande de nous connecter sur le serveur de courriels. Cependant, le lien ne pointe pas sur le serveur de HEC, mais pointe sur sogohec.ca. Ainsi, en cliquant sur le lien, nous serons dirigés vers un serveur externe qui n'appartient pas à HEC Montréal. Ce serveur pourrait alors contenir du code malveillant.

H Récompense.

Ce type de courriel vous demande généralement de remplir un formulaire afin de gagner ou d'être éligible à un tirage. Bien entendu, ce formulaire vous demande de saisir de l'information confidentielle.

Il faut ainsi être méfiant des messages qui semble trop beaux pour être vrai tel que « vous venez de gagner […] », « Vous pouvez augmenter vos fonctionnalités […] », « Courrez la change de gagner une croisière […] », etc.



Nous venons de voir les 8 éléments de vigilance. Maintenant c'est à vous de jouer.

Voici un courriel qui a été envoyé en décembre 2014 à l'ensemble de la communauté HEC Montréal, soit : les étudiants, les enseignants et les employés administratifs.

Utiliser les 8 éléments de vigilance afin de déterminer si ce courriel est légitime ou si nous sommes en présence d'un courriel d'hameçonnage. Je vous invite à appuyer sur « pause » afin d'avoir le temps de réaliser l'exercice. Par la suite, nous passerons ensemble les 8 éléments de vigilance.

From: eduain@server2.itakhost.com [mailto:eduain@server2.itakhost.com] **On Behalf Of** Daniel Dussart
Sent: Tuesday, December 23, 2014 12:19 PM
To: [redacted]
Subject: Accès ZoneCours

Cher utilisateur,

Votre accès à la ZoneCours expire bientôt, donc il faut l'activer à nouveau immédiatement ou il sera fermé automatiquement.
Pour ce faire, cliquez sur l'adresse Web ci-dessous ou copier et le coller dans votre navigateur Web. Une fois connecté, votre accès est réactivé et vous serez redirigé vers la ZoneCours.

https://zonecours2.hec.ca/login_v0LGTuQB0oJA4fuyI2X613JELU8L9NGY4GTNIZR8LBB23A7EG5T4K4D66Ym8QHTLGTuQGm8Buy5Nl9TD8yYIEjfD8nYJiH8nYZtG2p1sJDFM3LF-13507/

Si vous n'êtes pas capable de se connecter, se il vous plaît contacter Daniel Dussart à daniel.dussart@hec.ca pour une assistance immédiate.

Cordialement,

Daniel Dussart
Direction des technologies de l'information
HEC MONTRÉAL
514 340-6964
daniel.dussart@hec.ca

Voici ce que nous pouvons observer :

A Adresse courriel de l'expéditeur et des destinataires.

- Ne provient pas d'une adresse de HEC Montréal.

B Expéditeur.

- Rien de particulier, nous pourrions néanmoins en cas de doute communiquer avec le centre d'assistance technique.

C Courriel trop générique.

- « Cher utilisateur », semble générique et non personnalisé.
- Ce n'est pas la signature officielle de la Direction.
- Lors de la réception de ce courriel, aucune personne du nom de Daniel Dussart n'était à l'emploi de HEC Montréal.

D Orthographe.

- Il y a beaucoup de fautes d'orthographe et de syntaxe.

E Action immédiate.

- Nous demande de poser une action immédiatement : « **Immédiatement sinon le compte sera fermé automatiquement**. »

F Pièces jointes.

- Ne s'applique pas, car il n'y a pas de pièce jointe.

G Hyperlien.

- Nous avons effectivement un hyperlien qui peut attirer notre attention. Ici il faut mettre notre souris par-dessus le lien pour voir que l'adresse URL est différente de ce qui est affiché. Le URL pointe en réalité sur http://zonecours2.hec.ca**.cnea.tk**.

H Récompense.

- Ne s'applique pas, car il n'y a aucune récompense offerte.

Les cinq éléments de vigilance découverts dans le courriel nous permettent d'affirmer que nous sommes en présence d'un courriel d'hameçonnage.

Maintenant, vous êtes en mesure de reconnaître un courriel d'hameçonnage !