Utiliser le courriel

GUIDE DU FORMATEUR

Le présent document sert de guide de référence et de préparation pour le formateur, ainsi que de complément au plan de leçon.

Les connaissances que l'apprenant doit avoir acquises au terme du module se trouvent dans la section « Objectifs d'apprentissage ».

La section « Contexte et détail pour le formateur » contient quant à elle une description du contenu ainsi que des liens vers des références permettant au formateur d'en apprendre plus sur le sujet. Il pourra ainsi mener les discussions et répondre aux questions avec assurance, sans être limité par la matière. Par ailleurs, chaque élément de la section « Contexte et détail pour le formateur » vient étayer une partie du scénario.

Objectifs d'apprentissage

- Savoir ce qu'est le courriel.
- Connaître les risques associés au courriel.
- Savoir ce qu'est le pourriel ou courrier indésirable.
- Savoir prendre des décisions quant au courriel.

Contexte et détail pour le formateur

1 Qu'est-ce que le courriel?

1.1 En bref

Le courriel (courrier électronique) est un moyen d'envoyer de la correspondance (messages) par Internet. Chaque courriel est envoyé à une adresse courriel (adresse de messagerie électronique).

1.2 En détail

- Les services de courriel sont fournis par les fournisseurs d'accès Internet (FAI), les lieux de travail et les services en ligne, souvent gratuitement.
- L'envoi d'un courriel se fait dans un programme ou une application sur un ordinateur ou un appareil mobile, ou par un service Web tel que Gmail, Hotmail, Yahoo! et bien d'autres.
  - Le programme ou l'application se connecte à un service de courriel, puis recueille les messages que l'on vous a envoyés et transmet les messages que vous avez rédigés
  - Le service Web de courriel est un site que l'on peut visiter pour envoyer et recevoir ses courriels.
- Les messages ont une adresse courriel de provenance et une adresse courriel de destination.
  - La véracité du nom et des renseignements associés à une adresse n'est pas garantie : aucune vérification n'est faite.
    - Il est très facile de créer une adresse fausse ou trompeuse.
    - Tous peuvent avoir un nombre illimité d'adresses.
      - Bien des gens ont plusieurs adresses : une pour le travail, une pour la maison, une pour les sites susceptibles d'envoyer des pourriels, etc.
      - La plupart des applications de courriel permettent l'utilisation de plusieurs adresses.
        - Profitez-en : si vous ne voulez pas fournir vos renseignements personnels, mais que l'on vous demande une adresse courriel, prenez-en une sans frais qui ne contient pas vos renseignements.
- Les adresses courriel se divisent en trois parties :
  - La partie qui précède le symbole @ est le nom choisi pour le compte. On peut utiliser n'importe quel nom, tant qu'il n'a pas déjà été choisi par un autre utilisateur du même service de courriel (deux personnes ne peuvent avoir la même adresse électronique).
  - Le symbole @ sert à diviser l'adresse. Il est obligatoire dans toutes les adresses.

  - La partie qui suit le symbole @ est le nom du domaine ou du serveur où se fera le triage final des messages. C'est le nom du fournisseur du service de courriel.

  - Un nom associé au compte de courriel de l'expéditeur peut accompagner ou remplacer son adresse. Or, l'expéditeur peut choisir n'importe quel nom et ne mettra pas nécessairement le sien.

- Les courriels contiennent tous les éléments d'information suivants :

  - Un expéditeur, un ou des destinataires, un ou des destinataires en copie conforme, un ou des destinataires en copie conforme invisible, un objet et un corps.

    - ***Champ À*** : Contient l'adresse courriel du destinataire du message.

    - ***Champ De*** : Contient l'adresse courriel de l'expéditeur et est habituellement généré automatiquement.

    - ***Champ C.c.*** (copie conforme) : Sert à envoyer une copie du message à une autre adresse de façon simultanée.

    - ***Champ C.c.i.*** (copie conforme invisible) : Sert à envoyer une copie du message à une autre adresse à l'insu des autres destinataires (seul l'expéditeur pourra voir que cette personne a reçu une copie).

    - ***Ligne d'objet*** : Décrit idéalement le contenu du message.

    - ***Corps du courriel*** : Sert à rédiger le message.

  - Le corps du courriel peut contenir bon nombre des éléments d'une page Web.

    - Le programme utilisé pour lire le message interprétera le code qu'il contient, le formatera et inclura le texte, les images, les couleurs, les polices, les liens et les autres éléments prévus par l'expéditeur. C'est pourquoi les messages électroniques présentent les mêmes dangers potentiels que les pages Web.

  - Le courriel peut aussi contenir des pièces jointes (fichiers) que le destinataire pourra télécharger et utiliser. Il n'est pas garanti que le nom du fichier indique sa nature réelle. Par exemple, si un fichier est nommé « recette_biscuit.exe », il s'agit probablement plus d'un virus que d'une recette.

1.3 En pratique

Il faut considérer tous les éléments d'un message électronique comme fictifs.

2 Risques associés au courriel

2.1 En bref

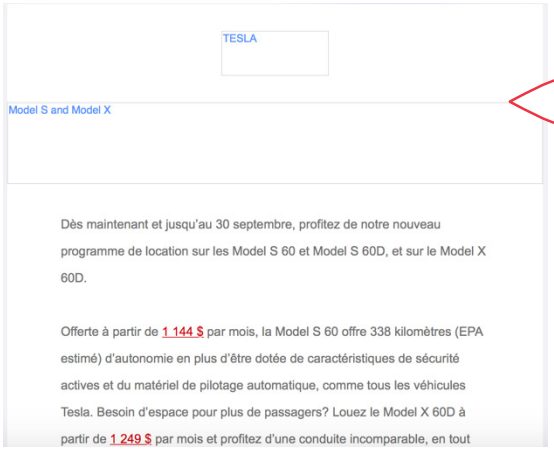
Les courriels ne sont pas dignes de confiance, car ils peuvent contenir des programmes malveillants et être associés à une fraude. Bien des arnaques commencent par un courriel. Il convient donc de se méfier des courriels et d'éviter de cliquer sur les liens qu'ils contiennent.

2.2 En détail

- La messagerie électronique est dépourvue de système de sécurité.
  - Il n'existe aucun moyen de vérifier l'identité de l'expéditeur ou la nature du courriel.
  - Tous les éléments d'un courriel sont falsifiables et manipulables.
  - Les courriels envoyés ne sont pas sécurisés et peuvent être lus ou modifiés en cours d'acheminement.
- La messagerie électronique se prête bien à l'automatisation.
  - On peut envoyer des milliers de messages par seconde.
  - L'expéditeur n'a besoin que de l'adresse courriel du destinataire.
  - On trouve sur Internet beaucoup de listes d'adresses dressées à cette fin, sans compter qu'il est possible de deviner une adresse.
  - Ces listes permettent à des gens d'envoyer un très grand nombre de messages sans trop d'effort.
  - Même s'il n'y a qu'une chance sur un million pour qu'un destinataire réponde, l'effort peut être payant pour quelqu'un qui envoie 100 millions de messages par jour.
- Ce n'est pas parce que l'on reçoit un courriel qu'il a été envoyé intentionnellement.
- Comme les messages électroniques peuvent contenir des pièces jointes, des liens et des éléments de page Web, ils peuvent transmettre des programmes malveillants ou guider le destinataire vers une page Web malveillante.
- ***Programme malveillant***
  - Des programmes malveillants, communément appelés maliciels, peuvent être transmis par courriel de différentes manières :
    - Pièce jointe
      - N'importe quel fichier peut être un programme malveillant.
      - Même les fichiers qui semblent inoffensifs et qui s'ouvrent normalement peuvent contenir un code dangereux s'exécutant à votre insu[1].
      - Ce type de programme malveillant s'appelle cheval de Troie, car il fonctionne selon la même stratégie que dans la légende.
      - Méfiez-vous de toutes les pièces jointes et faites-les balayer par un analyseur de virus.

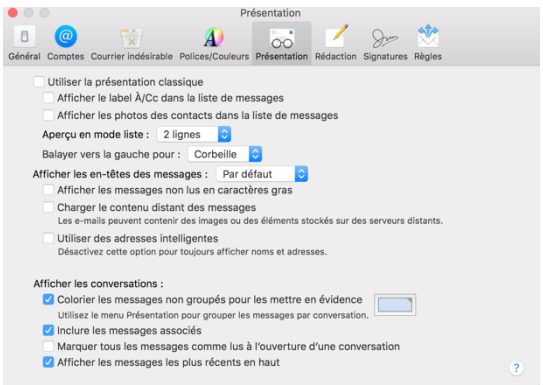
1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

- Lien vers une page
  - Si vous visitez une page à laquelle mène un lien fourni par courriel, un programme malveillant pourrait se retrouver sur votre ordinateur.
  - Méfiez-vous de tous les liens fournis par courriel.
- Contenu du courriel
  - Il se peut qu'à l'ouverture d'un courriel, du contenu soit téléchargé sur Internet.
  - Il est plus prudent de désactiver cette fonction.
  - Si vous le faites, beaucoup de courriels vous paraîtront incomplets. C'est normal : rien n'est brisé pour autant.



> *Courriel avec contenu (images) distant bloqué*

- Pour désactiver le contenu distant sur les appareils ***Apple*** :
  - Dans la barre de menus en haut de l'écran, cliquez sur Mail, puis sélectionnez Préférences.
  - Dans la boîte Préférences, sélectionnez Présentation. Décochez Charger le contenu distant des messages.



- ***Gmail***
    - Ouvrez Gmail.
    - Cliquez sur la roue dentée en haut à droite.
    - Sélectionnez ***Paramètres***.
    - Restez sous l'onglet ***Général***.
    - Faites défiler la page jusqu'à la section ***Images***.
    - Cochez Demander confirmation avant d'afficher des images externes.
    - Cliquez sur ***Enregistrer les modifications*** au bas de la page.
- ***Outlook*** bloque par défaut les images distantes[2].

- ***Hameçonnage***
    - Vos renseignements personnels peuvent avoir beaucoup de valeur pour les criminels.
        - Les authentifiants de compte (noms d'utilisateur et mots de passe) et les renseignements financiers (renseignements de carte de crédit) peuvent être particulièrement payants pour eux.
        - C'est pourquoi ils investissent beaucoup de temps et d'énergie pour vous les soutirer. Cette pratique s'appelle hameçonnage, puisqu'elle consiste à aller à la pêche aux renseignements personnels.
    - Les courriels d'hameçonnage semblent souvent provenir d'une organisation où vous avez stocké des renseignements précieux.
        - Ils contiennent souvent un lien vers une page où l'on vous demandera de vous connecter ou d'entrer des renseignements précieux sous un prétexte, comme une vérification ou une mise à jour.
        - Si un message contient un lien vers une page vous demandant des renseignements personnels ou des authentifiants, faites preuve d'une extrême prudence.
            - Évitez de cliquer sur un lien contenu dans un courriel provenant d'une banque ou d'une entreprise bien connue (p. ex. Microsoft, Apple, eBay, Paypal).
            - Si vous recevez un courriel et voulez vérifier s'il y a réellement un problème avec votre compte, rendez-vous sur le site Web de l'organisation de la manière habituelle (taper l'URL) ou appelez-la directement.
            - Ne cliquez pas sur le lien contenu dans le courriel, et ne copiez-collez pas l'URL dans votre navigateur.

2 https://support.office.com/fr-fr/article/Bloquer-ou-d%C3%A9bloquer-le-t%C3%A9l%C3%A9chargement-automatique-d-images-dans-les-messages-%C3%A9lectroniques-15e08854-6808-49b1-9a0a-50b81f2d617a?ui=fr-FR&rs=fr-FR&ad=FR

- ***Arnaques***
  - Beaucoup d'arnaques sont menées par courriel.
  - N'oubliez pas qu'il est possible d'envoyer un courriel à n'importe qui de façon automatisée.
    - Fraude par paiement à l'avance
      - Ce type de fraude consiste à demander un petit paiement en échange d'une grosse récompense. En voici quelques exemples :
        - Un fraudeur prétend avoir accès à une importante somme d'argent et vous indique la provenance de cet argent. Il vous demande de sortir la somme du pays et vous dit pourquoi il ne peut pas le faire lui-même. Si vous lui répondez, il vous demandera de régler différents frais (p. ex. honoraires d'avocat, frais de transaction, taxes) pour débloquer les fonds. Or, les frais s'accumuleront sans fin, et soit l'argent n'arrivera jamais, soit vous recevrez un chèque sans provision ou contrefait.
        - Un faux éditeur, une fausse entreprise de promotion d'inventions ou de brevets ou une fausse agence de mannequins ou de casting promet de lancer votre carrière. L'arnaque commence par une première consultation, mais le fraudeur ajoute ensuite des frais à régler d'avance, souvent dans le but prétendu de financer la poursuite du travail ou des recherches.
        - Vous êtes une personne âgée, et un fraudeur vous appelle ou vous écrit un courriel pour vous annoncer que vous avez gagné un important prix à une loterie ou à un tirage. Cependant, il vous demande de régler des frais d'avance pour recevoir votre prix. Vous ne recevrez jamais votre prix.
      - Les arnaqueurs renouvellent constamment les pièges qu'ils tendent à leurs victimes. Par exemple, certaines personnes disent avoir été appelées par un soi-disant représentant du tirage Reader's Digest ou de la loterie Set For Life. Cette personne leur a dit que pour recevoir leur prix, elles devaient fournir leur numéro de carte de débit et leur date de naissance et, dans certains cas, entrer leur NIP sur le pavé numérique de leur téléphone. Les arnaqueurs ciblent les personnes âgées qui n'utilisent pas les services bancaires en ligne; ils se servent des renseignements pour s'approprier leur compte et blanchir de l'argent et le produit d'autres arnaques par marketing de masse.
      - Signaux d'alarme – Comment se protéger
        - Les entreprises de loterie ou de tirage connues (p. ex. Reader's Digest, Publishers Clearing House) ne demandent jamais au gagnant d'effectuer un paiement pour réclamer son prix.
        - Si des frais sont associés au prix gagné, leur règlement ne se fera jamais par l'intermédiaire d'une entreprise de transfert de fonds (p. ex. Western Union, MoneyGram) ou par l'ajout de fonds à une carte de crédit prépayée (p. ex. Green Dot).

- Si vous recevez un appel non sollicité à propos d'un prix que vous auriez gagné à une loterie, c'est une arnaque.
  - On ne peut participer à une loterie étrangère qu'en se rendant dans le pays en question et en achetant un billet en personne. On ne peut pas acheter un billet au nom de quelqu'un d'autre.
- Ne donnez jamais vos renseignements personnels par téléphone, quelle que soit l'organisation que votre interlocuteur prétend représenter.

– Les arnaqueurs ne font pas toujours miroiter d'importants gains ou une occasion rêvée, par exemple. En effet, certains jouent plutôt sur les émotions.

- Fraude du besoin d'argent urgent

  – Le fraudeur cherche une victime potentielle sur les médias sociaux, sur Internet et dans les journaux. En prétendant être un membre de la famille ou un ami proche, il appelle à propos d'une urgence nécessitant l'envoi immédiat de fonds. Il est souvent question d'un membre de la famille qui a été arrêté ou qui a eu un accident pendant un voyage à l'étranger. Le fraudeur invoque des frais d'hospitalisation, d'avocat ou de cautionnement. Généralement, il demande à la victime potentielle de recourir à une entreprise de transfert de fonds (p. ex. Western Union, MoneyGram).

  – Signaux d'alarme – Comment se protéger

  - Vérifiez où se trouve votre proche auprès de votre famille ou de vos amis.
  - Sachez que jamais un policier, un juge ou une entité juridique ne vous demandera de lui envoyer de l'argent par l'intermédiaire d'une entreprise de transfert de fonds.
  - Ne donnez jamais le nom ou les coordonnées d'un membre de votre famille à un appelant inconnu.
  - Méfiez-vous toujours des demandes d'argent urgentes.

- Si vous croyez qu'une de vos connaissances ou vous-même avez été victimes d'une fraude, appelez le Centre antifraude du Canada au 1 888 4958501 ou faites un signalement à http://www.antifraudcentre.ca/. Vous pouvez aussi demander conseil à un ami, à un membre de votre famille ou à une autre personne de confiance.

2.3 En pratique

Réfléchissez avant de cliquer, et cliquez rarement, voire jamais.

Méfiez-vous des courriels. Ils ne sont pas dignes de confiance.

Arrêtez-vous pour réfléchir un peu, et résistez à la pression que les arnaqueurs exercent pour vous soutirer de l'information.

3 Pourriel

3.1 En bref

Les pourriels sont des messages indésirables qui peuvent se retrouver dans votre boîte de réception. Ils sont souvent filtrés par l'application ou le fournisseur de services de courriel. Vous pouvez régler la sensibilité du filtre. Vous pouvez aussi signaler les pourriels à http://fightspam.gc.ca.

3.2 En détail

- Le mot pourriel évoque généralement les courriels publicitaires agaçants qui se retrouvent à l'occasion dans notre boîte de réception.
  - Selon la loi, la définition de pourriel comprend non seulement l'envoi de messages électroniques commerciaux non sollicités, mais aussi la modification non autorisée de données de transmission, l'installation non autorisée d'un programme informatique, les indications fausses ou trompeuses dans un message électronique (y compris les sites Web), la collecte non autorisée d'adresses électroniques et la collecte de renseignements personnels au moyen d'un ordinateur en contravention d'une loi fédérale[3].
  - Si vous pensez qu'une entreprise enfreint la loi en vous envoyant des courriels non sollicités, informez-vous et faites un signalement à http://fightspam.gc.ca.
- Les fournisseurs d'accès Internet (FAI), de services de courriel et de logiciels travaillent d'arrache-pied pour limiter les pourriels. Ils font beaucoup de filtrage automatique de sorte que seule une petite fraction des pourriels arrivent à destination.
- Les applications de courriel peuvent marquer les messages possiblement indésirables, les plaçant normalement dans un dossier distinct nommé « Pourriel » ou « Courrier indésirable ».
  - Vous pouvez vérifier si des messages légitimes s'y sont retrouvés par erreur, ce qui peut arriver de temps à autre.
    - Le cas échéant, il y a habituellement un bouton pour indiquer à l'application que le message est sécuritaire (et non indésirable). Ainsi, le système apprend ne pas indiquer comme indésirables les messages semblables à l'avenir.
  - Certaines applications de courriel permettent de régler la sensibilité du filtre antipourriel.
    - Si vous utilisez un réglage à faible sensibilité, des pourriels se retrouveront peut-être plus souvent dans votre boîte de réception, mais moins de messages légitimes risquent de se retrouver par erreur parmi les pourriels.
    - Si vous le réglez au maximum, le filtre attrapera la plupart des pourriels, mais risque de classer à tort des messages légitimes dans les pourriels. Vous devrez donc récupérer ces messages manuellement dans le dossier « Pourriel » ou « Courrier indésirable ».

3 http://fightspam.gc.ca/eic/site/030.nsf/fra/00303.html#ic-subnav-2

- Trouvez le réglage qui vous convient.
- Voici comment régler les filtres antipourriel :
  - Apple Mail
    - Dans la barre de menus de l'application de courriel d'Apple en haut de l'écran, cliquez sur ***Mail***, puis sélectionnez ***Préférences***.
    - Dans la boîte ***Préférences***, sélectionnez ***Courrier indésirable***. Assurez-vous que la case ***Filtrer le courrier indésirable*** est cochée.

  - Office 365[4]
    - Pour ouvrir la page ***Courrier indésirable*** à partir de la page principale d'Outlook Web App, sélectionnez ***Options*** dans le coin supérieur, puis sélectionnez ***Courrier indésirable*** dans la liste du volet de navigation.
    - Assurez-vous que l'option ***Ne pas filtrer le courrier indésirable*** n'est pas sélectionnée[5].
  - Gmail
    - Dans la page de messagerie Web Gmail, le filtre antipourriel est activé par défaut et vous aide à classer les courriels.
    - Si vous attendiez un message et que celui-ci semble s'être perdu, sélectionnez ***Pourriel*** dans les options à gauche.
    - Si vous trouvez un message classé à tort dans les pourriels, pour annuler son marquage, sélectionnez le courriel, puis cliquez sur le bouton ***N'est pas un pourriel*** situé en haut et en bas de la vue active.
    - L'annulation du marquage entraîne automatiquement la réintégration du message dans la boîte de réception[6].

4 Pour Office 2010 : https://support.office.com/fr-fr/article/%C3%80-propos-du-filtre-Courrier-ind%C3%A9sirable-5ae3ea8e-cf41-4fa0-b02a-3b96e21de089?ui=fr-FR&rs=fr-FR&ad=FR

5 https://support.office.com/fr-fr/article/Options-Courrier-ind%C3%A9sirable-068FA430-F8D7-4518-A8DA-8BC74958F05F?ui=fr-FR&rs=fr-FR&ad=FR

6 https://support.google.com/mail/answer/9008?hl=fr

3.3 En pratique

Sachez que votre application de courriel dispose d'un filtre qui attrapera les pourriels pour ne pas qu'ils se retrouvent dans votre boîte de réception.

Réglez le filtre et donnez-lui autant d'indications que possible.

4 Décisions concernant le courriel

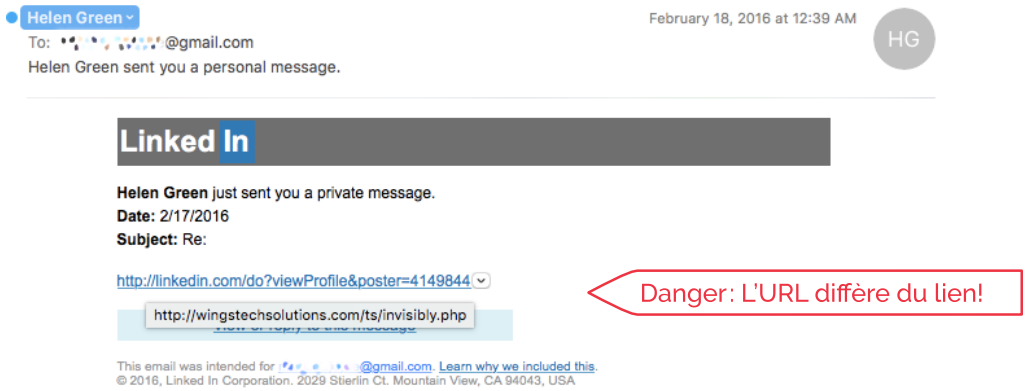
4.1 En bref

Si le courriel est attendu et semble authentique, il est probablement acceptable. Vous n'êtes jamais obligé de cliquer, et vous pouvez prendre votre temps avant de décider de faire quoi que ce soit.

4.2 En détail

- Identification des courriels authentiques
  - Il y a lieu de penser que le courriel vous est destiné si :
    - vous connaissez l'expéditeur;
    - le message est personnalisé (le contenu concorde avec celui des communications habituelles de l'expéditeur);
    - la grammaire est bonne ou conforme à la maîtrise de la langue de l'expéditeur.
  - Méfiez-vous :
    - des courriels inattendus;
    - des courriels qui proviennent d'une banque ou d'une entreprise avec laquelle vous n'avez aucune relation;
    - des courriels qui vous demandent des renseignements sur vos comptes ou qui évoquent de graves conséquences (p. ex. fermeture d'un compte) en cas de refus de fournir ou de mettre à jour vos renseignements personnels;
    - des courriels qui proviennent soi-disant d'une entreprise, mais qui présentent des fautes d'orthographe ou de grammaire;
    - des courriels professionnels qui ne sont pas envoyés à partir du nom de domaine habituel de l'entreprise en question;
    - des courriels qui exigent une action urgente ou immédiate;
    - des courriels qui vous demandent d'envoyer des fonds par Western Union ou MoneyGram ou par carte de crédit prépayée.
- Signaux d'alarme – Comment se protéger
  - Pas de panique. Vous avez le temps de réfléchir. Rien ne presse.

- Réfléchissez avant de cliquer sur une pièce jointe ou un lien.
- Vérifiez manuellement les URL des hyperliens en plaçant votre curseur dessus (cette pratique est dangereuse et déconseillée).



- Règle générale, vous n'êtes pas obligé de cliquer sur un lien contenu dans un courriel. Si c'est important, vous pouvez vous rendre sur le site Web de l'expéditeur en tapant l'URL ou prendre le téléphone.

– Voici quoi faire si vous recevez un courriel inquiétant :

- Ne cliquez pas sur le courriel. À la place :
  - pour vérifier votre compte, allez à la source en tapant l'adresse habituelle dans votre navigateur;
  - appelez votre fournisseur de services pour vérifier la légitimité du message.

- À retenir :

– Si l'offre semble trop belle pour être vraie, c'est probablement le cas.

– Ne divulguez pas vos renseignements personnels ou vos renseignements de carte de crédit simplement parce que l'on vous le demande par courriel.

– Ne cédez pas à la pression.

- Vous avez toujours amplement de temps.
- Vous pouvez toujours quitter, raccrocher et faire des vérifications (rappeler au numéro principal, parler à un proche et aux autorités) avant de procéder.
- Parlez de vos inquiétudes : c'est un bon moyen de vous faire rassurer et de conscientiser les autres.

– Si c'est une fraude, identifiez-la, signalez-la et enrayez-la!

- Appelez le Centre antifraude du Canada au 1 888 4958501 ou faites un signalement à http://www.antifraudcentre.ca.

4.3 En pratique

Avec les courriels, soyez calme et lucide et prenez votre temps.

Glossaire

Adresse courriel	Nom unique auquel on peut envoyer un message électronique. Exemple : info@serene-risc.ca.
Analyseur de virus	Logiciel de sécurité vérifiant la présence de virus, soit automatiquement à l'ouverture ou au téléchargement d'un fichier, soit manuellement pour certains fichiers ou tous les fichiers.
Application ou programme	Ensemble programmé d'instructions s'exécutant sur un ordinateur ou un appareil. Exemples : logiciel de traitement de texte, jeu.
Arnaque	Procédé malhonnête ou trompeur créé à des fins criminelles.
Centre antifraude du Canada (CAFC)	Organisme central du Canada qui amasse de l'information et des renseignements criminels sur la fraude et le vol d'identité. Site : http://www.antifraudcentre-centreantifraude.ca.
Cheval de Troie	Programme dissimulé dans un fichier. À l'ouverture du fichier, le programme exécute une fonction inattendue et souvent malveillante.
Fournisseur d'accès Internet (FAI)	Entreprise fournissant un accès Internet à ses abonnés.
Nom de domaine	Nom d'un site ou d'un service en ligne. Exemples : outlook.com, Canada.ca, serene-risc.ca, gmail.com.
Pièce jointe	Fichier accompagnant un courriel.

Pourriel	Courriel non sollicité et agaçant.
Programme malveillant	Logiciel créé dans un mauvais dessein.
Serveur	Ordinateur transmettant de l'information ou exécutant des fonctions pour d'autres ordinateurs à l'intérieur d'un réseau.