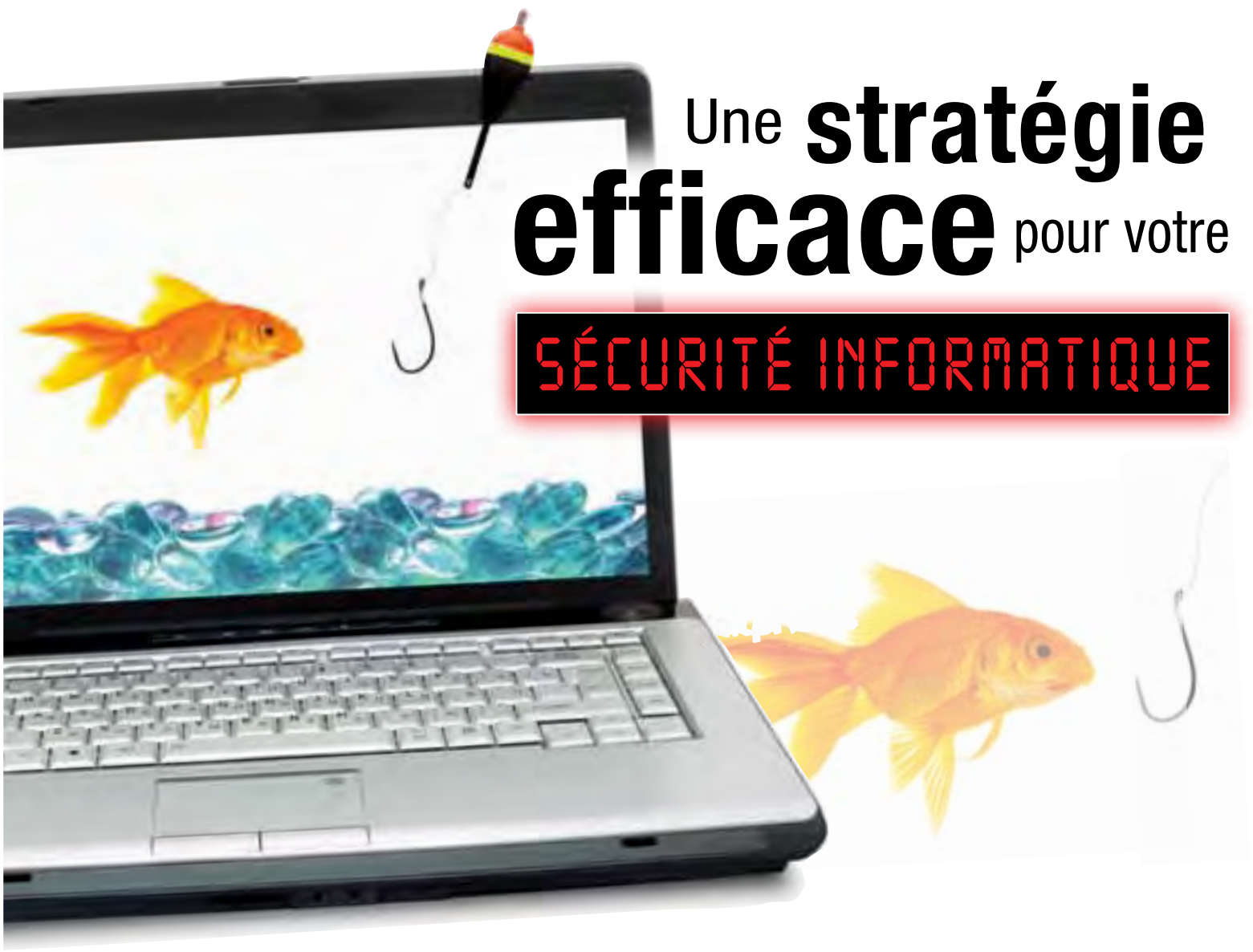
Une **stratégie efficace** pour votre SÉCURITÉ INFORMATIQUE



Jean-François Ferland
Rédacteur en chef
www.directioninformatique.com

Grâce à l'informatique, vous pouvez apprendre, communiquer, partager, créer, jouer et travailler à l'aide des mots, de l'image et du son. Internet constitue une source formidable d'information et d'interaction avec des parents, des amis, des collègues et d'autres personnes. Au fil des années, vous avez accumulé des fichiers de texte, des photos, des fichiers audio et vidéo, des coordonnées et d'autres informations qui ont une grande importance pour vous.

Mais soyons réalistes sans être alarmistes : l'informatique doit être protégée afin d'éviter les pertes de données et les atteintes à la confidentialité. Soyez rassuré : les moyens de prévention et de protection pour l'informatique sont faciles à appliquer. Voici quelques trucs qui vous aideront à sécuriser votre matériel et vos données. Cela nécessite un peu de temps, d'argent et de discipline, mais mieux vaut prévenir que guérir. Avant de poursuivre, procurez-vous un calepin dans lequel vous noterez des informations essentielles pour votre stratégie de sécurité.

PROTÉGEZ VOTRE MATÉRIEL

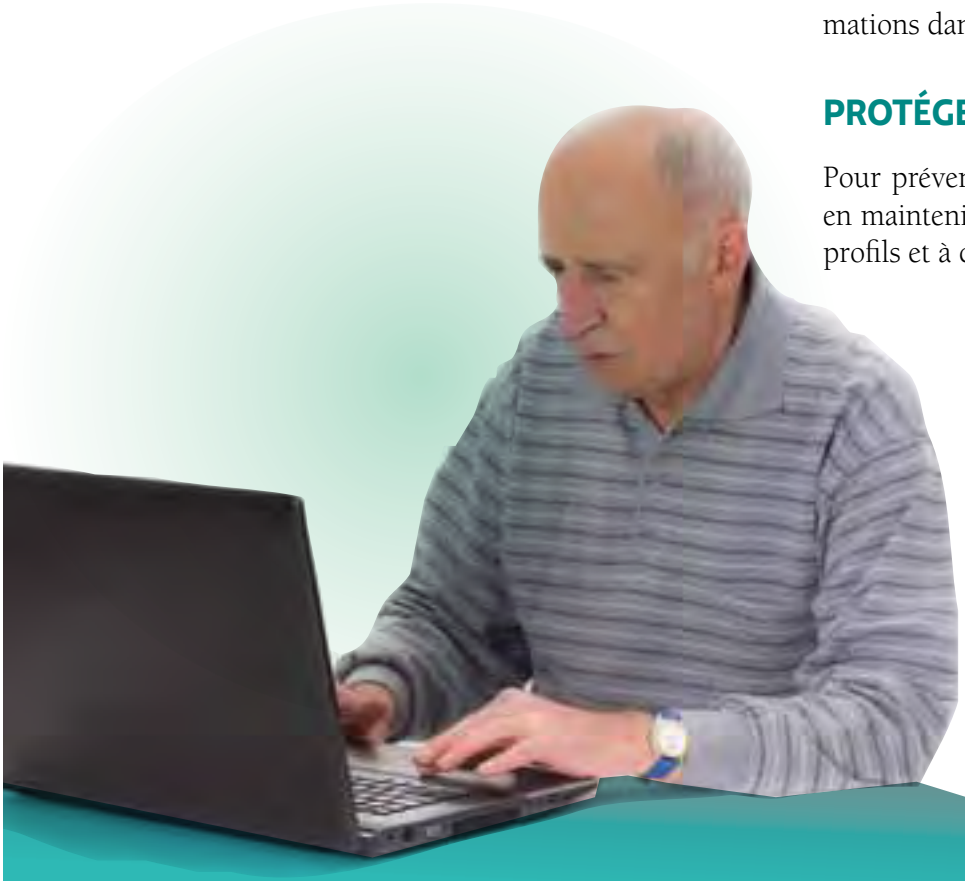
Le vol est une réalité qu'on ne peut ignorer au XXIe siècle. Lorsqu'un malfaiteur s'introduit dans une maison ou un bureau, le matériel informatique fait partie des objets de valeur qu'il tente de subtiliser en premier lieu. Les ordinateurs portatifs, les tablettes numériques, les téléphones évolués et les lecteurs multimédias l'intéressent encore plus parce que ces objets se dissimulent et se transportent facilement. À domicile et dans les endroits publics, comment peut-on protéger son matériel?

À la maison, l'ordinateur de table doit être attaché à une lourde pièce de mobilier à l'aide d'un ensemble de sécurité. Au dos de la plupart des ordinateurs, moniteurs et disques durs externes, on trouve une « fente de sécurité » qui mesure trois par sept millimètres. Elle sert à l'arrimage d'un câble de sécurité offert par des fournisseurs comme Kensington et Targus. Un ensemble de sécurité, qui coûte une cinquantaine de dollars, comprend un câble en métal, une serrure à clé ou à combinaison et le matériel nécessaire pour y attacher jusqu'à trois composantes informatiques. Des ancrages à adhésif puissant peuvent être collés sur les appareils qui n'ont pas de fente de sécurité. Le câble est arrimé à un ancrage qu'on colle au dos d'un bureau ou sur le côté d'un gros classeur. À la vue de tels câbles, un voleur ne perdra pas de temps à tenter d'arracher le matériel qui y est attaché.

Quant à l'ordinateur portatif, des modèles de câble peuvent être passés en boucle autour de la patte d'une lourde table dans un lieu public.

Les appareils portatifs doivent être gardés hors de la vue des mécréants. Rangez-les dans un tiroir ou une armoire à serrure lors d'une absence temporaire ou prolongée.

Afin de faciliter l'identification de vos appareils informatiques en cas de vol, relevez-en la marque, le modèle et le numéro de série, qui sont inscrits sur les boîtiers ou dans le menu « à propos » du système d'exploitation. Si possible, faites graver un numéro d'identification par votre corps policier local, qui offre gratuitement ce service sur demande ou lors d'activités de prévention. Notez ces informations dans votre calepin.



PROTÉGEZ VOS DONNÉES

Pour prévenir l'accès aux données de votre ordinateur et en maintenir l'intégrité, le recours aux mots de passe, aux profils et à certaines fonctions de sécurité est essentiel.

Il est important d'activer un mot de passe qu'on doit fournir à l'ouverture d'une session ou à la sortie d'un état de veille de votre appareil informatique. Cette façon de faire retarde de quelques secondes votre utilisation de l'informatique, certes, mais elle empêche l'accès en clair à vos informations. Ce mot de passe doit être difficile à trouver pour les malfaiteurs et les curieux, mais facile à retenir pour vous (voir l'encadré à la page 23). Notez-le dans votre calepin.

Un système d'exploitation d'ordinateur permet d'établir plusieurs profils d'utilisateurs. Il est recommandé de vous réserver, à vous seulement, l'utilisation d'un profil « d'administrateur », qui donne un accès à toutes les données, permet l'ajout ou l'effacement de logiciels, alloue la modification des configurations et des profils, etc. Si vous accordez à d'autres le droit d'utiliser fréquemment votre appareil, créez des profils personnalisés pour chaque personne ou bien des profils généraux pour des groupes de personnes (p. ex. « Enfants », « Amis ») dans lesquels vous préciserez l'accès à certains logiciels, à certaines données et à certaines fonctions de votre ordinateur, comme l'impression ou la navigation dans Internet. Cette approche est pratique avec les enfants qui peuvent effacer par mégarde des fichiers importants!

Pour chaque profil, définissez un mot de passe et notez-le dans votre calepin. Divulguez ce mot de passe à la personne concernée ou entrez-le vous-même lors d'un changement d'utilisateur.

L'antivirus et le pare-feu

Les fonctions d'antivirus et de pare-feu sont essentielles pour la protection de vos données. Elles prennent la forme de logiciels qu'on se procure pour une cinquantaine de dollars par année, de services offerts par votre fournisseur d'accès Internet ou de fonctions intégrées au système d'exploitation de votre ordinateur.

L'antivirus, qui détecte les virus, les logiciels malveillants, les chevaux de Troie, etc., balaie les données qui se trouvent sur les disques durs, les supports amovibles (CD, DVD, clé USB, carte de mémoire) et les fichiers qui arrivent d'Internet par le courriel, la messagerie ou les téléchargements. Le pare-feu, pour sa part, filtre les paquets d'information qui arrivent et partent de votre ordinateur. Il bloque les tentatives d'intrusion et décèle les tentatives de fuite d'information. Généralement, on indique une seule fois au pare-feu qu'un logiciel est légitime afin qu'il le laisse interagir avec les réseaux informatiques.

La règle d'or est simple, mais doit être appliquée : l'antivirus et le pare-feu doivent être à jour et fonctionnels en tout temps. Automatisez la mise à jour des définitions de votre antivirus et de votre pare-feu, mais aussi de votre système d'exploitation, de votre fureteur Web, de votre suite de bureautique et des lecteurs de contenu Flash et de fichiers PDF. Assurez-vous que le contenu des périphériques externes et des supports amovibles (disque dur, téléphone évolué, CD-ROM, DVD-ROM, carte de mémoire, clé USB) soit balayé dès que ces périphériques sont branchés à votre ordinateur.

Assurez-vous que votre ordinateur est balayé fréquemment par votre antivirus, au moins une fois par semaine. Amorcez vous-même ce balayage ou programmez-le à un moment où vous n'avez pas à utiliser votre ordinateur, en vous assurant toutefois que ce dernier est allumé au moment prévu. Il est préférable d'acheter la nouvelle version d'un antivirus ou d'un pare-feu lorsque l'abonnement annuel de sécurité expire afin de tirer profit des améliorations qui ont été apportées aux logiciels.

SÉCURISEZ VOTRE RÉSEAU SANS FIL

L'utilisation des réseaux sans fil, tant pour les appareils mobiles que fixes, a révolutionné l'informatique personnelle. Toutefois, certains « déchantent » lorsqu'ils reçoivent une facture salée de leur fournisseur d'accès Internet en raison d'une consommation excessive de bande passante. L'explication réside souvent dans une protection inadéquate du réseau Wi-Fi à la maison. Des quidams qui trouvent un réseau peu ou mal protégé ne se gênent pas pour l'utiliser afin de télécharger gratuitement beaucoup de contenu...

Trop de gens conservent les configurations d'usine de leur routeur sans fil. Ainsi, il peut être facile pour un « fin finaud » de prendre le contrôle du routeur et d'empêcher son propriétaire de l'utiliser! Changez le mot de passe et même l'identifiant de votre routeur et notez ces informations dans votre calepin. Ne divulguez à personne ces coordonnées d'identification. En outre, trop de personnes conservent les configurations d'accès par défaut de leur réseau sans fil, ce qui équivaut presque à un réseau sans mot de passe pour les voleurs de bande passante. Personnalisez le nom de votre réseau et établissez un mot de passe sécuritaire dont la longueur équivaut à celle de deux mots de passe traditionnels. Notez ces informations dans votre calepin. N'ayez crainte, vous pourrez mémoriser dans vos

appareils informatiques ce long mot de passe afin qu'ils établissent automatiquement une liaison à votre réseau.

Il existe plusieurs protocoles de chiffrement des données pour les réseaux sans fil. Si vos appareils informatiques datent d'au moins 2006, optez pour le protocole WPA2 (*Wi-Fi Protected Access version 2*), qui est plus difficile à déchiffrer. De plus, vous pouvez configurer votre réseau afin qu'il ne soit pas détecté en public par les appareils d'autres utilisateurs. Les personnes à qui vous accorderez un accès à votre réseau sans fil devront entrer manuellement une fois le nom de votre réseau et son mot de passe, mais leurs appareils pourront mémoriser ces informations pour les connexions ultérieures.

Un réseau pour les invités

Pour les amis, qui désirent utiliser votre liaison à Internet à l'aide de leurs appareils mobiles, établissez un réseau sans fil pour invités. La plupart des routeurs sans fil récents offrent cette option. Attribuez à ce réseau pour invités un nom et un mot de passe sécuritaire, qui sont

Des mots de passe sécuritaires et faciles à retenir? Voici la formule!

123456, qwerty, password, motdepasse, football et *dragon* font partie des mots de passe les plus couramment utilisés dans Internet. Or, des malfaiteurs dotés d'ordinateurs personnels puissants et de dictionnaires spéciaux bombardent au hasard les pages d'ouverture de session des sites Web avec des combinaisons d'adresses de courriel, de noms d'usager et de mots de passe. Trop fréquemment, ils ont accès à des comptes mal protégés et les dégâts qu'ils peuvent causer sont bien connus. Comment se doter de mots de passe qui sont à la fois robustes et faciles à retenir?

Un bon mot de passe remplit les conditions suivantes :

- *Il est composé de plusieurs caractères.* Selon un article publié par Ars Technica en 2012, un mot de passe de 7 caractères requiert plus de 10 jours d'essais à temps plein pour l'ordinateur d'un malfaiteur.
- *Il est composé de majuscules et de minuscules.*
- *Il est composé de lettres, de chiffres et de caractères spéciaux* (p. ex. # %*-;?/).
- *Il n'inclut pas de mots du dictionnaire, de répétitions* (p. ex. 111111)*, de substitutions* (p. ex. ch4rl0t) *ou de suites logiques* (p. ex. abcdef)*.*
- *Il n'inclut pas de noms de lieu, de numéros de carte de crédit.*
- *Il n'inclut pas le nom d'usager du service en ligne.*
- Il est unique pour chaque authentification informatique ou chaque service Web.

Selon des outils gratuits dans Internet, un mot de passe qui est composé d'une dizaine de lettres majuscules et minuscules, de chiffres et de caractères spéciaux peut nécessiter entre un siècle et un million d'années d'essais continus avant d'être déchiffré! Donc, il faut des mots de passe qui sont longs et incompréhensibles. Mais comment se souvenir de tous ces mots de passe, alors que l'internaute, selon diverses études, aurait en moyenne 25 comptes en ligne?

Un exemple de formule

Une approche consiste à créer une formule personnalisée où vous utilisez le nom d'un service en ligne ou l'adresse d'un site Web pour « assembler » un mot de passe unique. La beauté de l'approche est que vous pouvez définir votre propre formule, pourvu qu'elle inclue des majuscules (M), des minuscules (m), des chiffres (c) et des caractères spéciaux (s), et qu'elle réponde aux autres conditions indiquées ci-dessus.

Voici un exemple de formule : mMmccsmMmscc (minuscule, majuscule, minuscule, chiffre, chiffre, caractère spécial, minuscule, majuscule, minuscule, caractère spécial, chiffre, chiffre).

Un élément clé de cette formule est la définition d'au moins deux combinaisons de chiffres et de caractères spéciaux qui seront communs à tous vos mots de passe. Par exemple, dans la formule ci-dessus, ces séries pourraient être « 09% » et « /31 ».

Ainsi, votre formule unique serait mMm09%mMm/31.

Prenons l'exemple du site Web *www.professeur.com*. En observant l'adresse du site (et en omettant les *www*), votre mot de passe serait pRo09%fEs/31.

Vous pouvez ajouter des conditions spéciales à votre formule. Si vous éliminez les voyelles, le mot de passe serait pRf09%sSr/31.

Ou encore, si vous commencez par la deuxième lettre de l'adresse Web, le mot de passe serait rOf09%eSs/31.

Personnalisez votre formule à votre goût. Notez votre formule et ses exigences particulières dans votre calepin.

Si l'adresse d'un site Web est trop courte pour avoir toutes les lettres nécessaires, utilisez les lettres de son domaine (p. ex. *.com*, *.ca*) ou complétez en reprenant du début de l'adresse Web.

Vous ferez un peu de gymnastique cérébrale les premières fois que vous vous identifierez à un compte, mais au fil du temps, vous inscrirez sans faute le bon mot de passe.

Pour chaque service en ligne, notez dans votre calepin le nom du service, son adresse Web, votre nom d'usager, votre mot de passe et l'adresse de courriel inscrite lors de l'ouverture d'un compte. Notez aussi la question secrète et votre réponse, si vous avez eu à définir ces informations.

Des applications pour les téléphones évolués et les tablettes numériques permettent de conserver les informations d'identification pour les services en ligne.

Validez un exemple de votre formule avec les outils suivants :

- **http://www.passwordmeter.com/**
- **http://howsecureismypassword.net/**

différents de ceux de votre réseau principal. Cochez l'option qui permet la communication et l'échange de fichiers entre les appareils présents sur ce réseau. Ainsi, vos amis auront accès à Internet, mais pas à vos disques durs ni aux autres ressources privées de votre réseau.

Réseaux publics : Prudence!

Dans un nombre croissant de lieux publics, comme les cafés, les foires alimentaires des centres commerciaux ou les aérogares, on offre un accès gratuit à Internet sans fil. La prudence doit toujours être de mise. N'utilisez que les accès offerts par des organisations réputées et limitez la transmission d'informations confidentielles par ces réseaux. Assurez-vous que la liaison avec un site Web d'achats en ligne, de banque ou de réseau social est sécurisée en confirmant l'utilisation d'une adresse Web débutant par « HTTPS » ou la présence d'une icône comme un cadenas dans votre fureteur. L'utilisation de liaisons sécurisées pour ces sites s'applique aussi à votre navigation en ligne à la maison.

SAUVEGARDEZ VOS DONNÉES

Vos données informatiques sont précieuses. Elles totalisent des mégaoctets, des gigaoctets ou des téraoctets d'espace disque! Toutefois, si vous les perdez, c'est à tout jamais. Il

est important de les sauvegarder le plus souvent possible. Voici quelques astuces faciles à appliquer.

Regroupez vos données dans un nombre restreint d'endroits dans votre ordinateur. Utilisez les dossiers *Documents, images, vidéos*, etc., de votre système d'exploitation. Sauvegardez-y les fichiers créés dans votre ordinateur, les fichiers téléchargés d'Internet ou d'un support amovible et les fichiers reçus par courriel. Prenez l'habitude de bien gérer vos documents en leur donnant des noms significatifs, en les classant de façon ordonnée et en effaçant les fichiers et les courriels inutiles.

Effectuez fréquemment des sauvegardes de vos fichiers. Établissez une routine quotidienne ou hebdomadaire à cet effet. Par exemple, chaque vendredi soir, prenez une heure pour gérer vos fichiers et vos sauvegardes. Copiez les fichiers de vos documents précieux sur des CD ou des DVD réinscriptibles et notez dans le boîtier la date de la sauvegarde. Il est préférable d'utiliser un logiciel de sauvegarde ou de gravure, qui permet d'établir un mot de passe pour vos sauvegardes sur disque. Notez ce mot de passe dans votre calepin.

Par ailleurs, vous pouvez faire une copie conforme de votre disque dur principal sur un disque externe. L'avantage de cette approche est qu'en cas de vol ou de bris du disque de votre ordinateur, vous pourrez recourir à ce disque externe temporairement pour accéder à vos données, mais aussi utiliser vos logiciels. Effectuez régulièrement une telle sauvegarde sur un disque externe de qualité.

Il est important de conserver vos sauvegardes dans un endroit sécuritaire. Si vous avez un coffre-fort à la maison, rangez-y vos DVD et votre disque dur externe. Rangez-y aussi le calepin, qui contient vos mots de passe et les informations d'identification de votre matériel.

COMBATTEZ LES POURRIELS ET L'HAMEÇONNAGE

Le courrier électronique est un moyen pratique de communication. Or, il peut être aussi une source de problèmes lorsque des inconnus tentent d'ennuyer des internautes au hasard avec des pourriels ou de les frauder au moyen de l'hameçonnage.

Le pourriel a perdu un peu de terrain en 2012, mais selon la firme Kaspersky Labs, il aurait constitué 72,1 % des courriels en circulation dans Internet! Avec son texte sans queue ni tête ou son offre de faux médicament, le pourriel est une nuisance. Pour empêcher que de tels messages n'atteignent votre boîte de réception, ayez recours à la fonction d'antipourriel, qui existe sous forme de logiciel comme service offert par votre fournisseur de services Internet ou comme fonction intégrée à votre logiciel de courriel. Généralement, on confirme une seule fois que l'adresse d'un ami ou d'une connaissance est légitime afin que ses courriels vous parviennent sans faute. Toutefois, si l'ordinateur de cette personne a été infecté à son insu, la fonction antipourriel bloquera les courriels malveillants qui pourraient vous être envoyés. Si vous recevez dans votre dossier de pourriels un courriel d'un ami qui ne contient que quelques mots en anglais et un hyperlien, c'est mauvais signe! Téléphonez-lui pour l'aviser que son ordinateur est peut-être infecté.

L'hameçonnage, par le courriel ou la messagerie instantanée, est plus pernicieux. Parfois, on veut vous faire croire que votre compte de banque, de média social ou de service en ligne a été compromis et qu'il faut changer votre mot de passe. Parfois, on vous informe qu'une transaction d'achat n'a pas fonctionné et qu'il faut entrer à nouveau votre numéro de carte de crédit. Or, l'hyperlien contenu dans un tel message mène au serveur d'une organisation criminelle qui sera bien contente de recueillir votre nom d'usager, votre mot de passe ou votre numéro de carte bancaire…

Longtemps, les tentatives d'hameçonnage ont eu peu de répercussions au Québec parce qu'elles étaient rédigées en anglais ou qu'elles utilisaient des marques de compagnies étrangères, mais ce n'est plus le cas à présent, puisque des messages écrits en français et arborant le nom d'entreprises locales sont maintenant en circulation.

La meilleure façon de combattre l'hameçonnage est l'élimination pure et simple de tels messages. Si une transaction en magasin ou un compte bancaire sont réellement compromis, jamais une institution légitime ne vous demandera des données personnelles et confidentielles par courriel ou par téléphone. Elle vous avisera plutôt par la poste et vous invitera à vous rendre sur place pour résoudre le problème. On vous fait part d'un problème urgent à régler par téléphone ou par courriel? Raccrochez ou effacez le message, point à la ligne.

Prudence et vigilance !