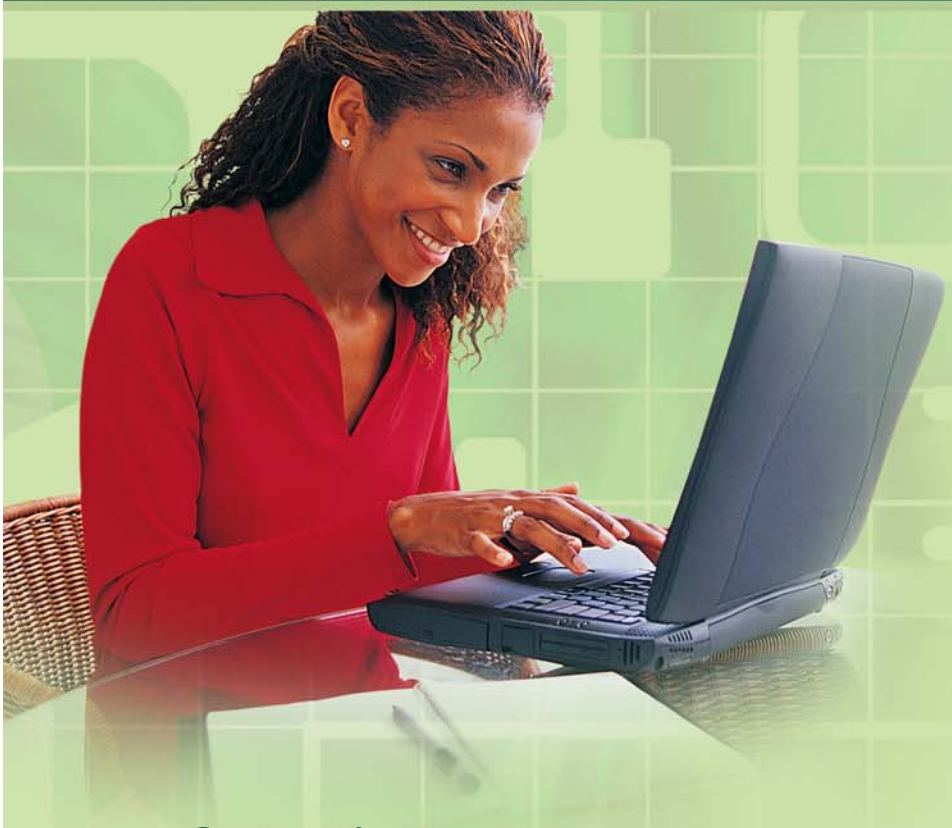
ALBERTA centreducyberfutur



Sécurité sur Internet

Une initiative de :

LIAISONENTREPRISE
Le service d'information sur l'entrepreneuriat en Alberta

Financée par :

Diversification de l'économie de l'Ouest Canada
Western Economic Diversification Canada
Canada

Introduction

Au fur et à mesure qu'Internet devient un élément essentiel dans les petites entreprises, la sécurité est un des sujets d'inquiétude les plus importants. Lorsque les bris de sécurité et les attaques aux virus font la une des journaux, les consommateurs se sentent impuissant. Ce guide vous présentera les sujets de la sécurité sur Internet et vous donnera des conseils pratiques pour vous protéger.

Sécurité physique

Les usagers ont des crises de panique en pensant à des "pirates d'Internet" qui pénètrent dans leur ordinateur et volent leur identité. Et pourtant, il est plus facile de se promener dans l'allée derrière les maisons le jour où on enlève les ordures, et retrouver tous les renseignements

Un des sujets les plus négligés, dans les discussions de sécurité, est la sécurité hors ligne. Les usagers ont des crises de panique en pensant à des "pirates d'Internet" qui pénètrent dans leur ordinateur et volent leur identité. Et pourtant, il est plus facile de se promener dans l'allée derrière les maisons le jour où on enlève les ordures, et retrouver tous les renseignements personnels dont on aurait besoin. De la même manière, il y a eu des cas nombreux d'entreprises vendant de vieux ordinateurs sans effacer de manière adéquate les informations importantes sur le disque dur.

Toutes les entreprises au Canada doivent désormais se conformer aux dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Un des dix principes de cette Loi est le besoin absolu de sécurité. Vous êtes tenu de protéger la sécurité physique et les renseignements personnels dont votre organisation fait la collecte et d'en disposer de manière responsable.

Isolement et sauvegarde des données

Si vous stockez tous les documents de l'entreprise dans un seul endroit, vous réduirez nettement le temps et le risque associé à la réinstallation et le rétablissement de ces données et de ces logiciels..

Si vous connaissez bien les ordinateurs, vous savez que vous aurez besoin inévitablement de réinstaller un jour votre système d'exploitation. Les composants matériels tombent en panne. Gonflé et alourdi par des programmes partiellement désinstallés ce système ralentit et puis malgré vos meilleurs efforts, les virus et les logiciels espions peuvent l'endommager au point où on n'est plus capable de le réparer. Le temps d'arrêt d'un système essentiel pendant que vous réinstallez votre système d'exploitation peut coûter cher à l'entreprise.

Séparez habituellement les logiciels de vos documents et données. Un système idéal aurait un répertoire principal (avec un nombre indéterminé de sous-répertoires) renfermant tous les documents de l'entreprise capables d'être transférés d'un ordinateur à l'autre si nécessaire. Certaines applications, les plus anciennes surtout, préfèrent sauvegarder les fichiers au même directoire que le logiciel applicatif. Il faut donc être vigilent. Si vous stockez tous les documents de l'entreprise dans un seul endroit, vous réduirez nettement le temps et le risque associé à la réinstallation et le rétablissement de ces données et de ces logiciels.

Quand tous les fichiers importants se retrouvent au même endroit, l'établissement d'un répertoire de secours est plus facile. Puisque les graveurs de CD sont peu chers, vous devriez être en train de sauvegarder ces données vitales sur un support mobile comme des disques lisibles/modifiables de façon régulière. Il existe des logiciels excellents pour sauvegarder et rétablir vos données mais le fait de respecter un calendrier établi pour le faire de façon manuelle devrait suffire dans la plupart des cas. Si votre logiciel de graveur le permet, il est bon de faire vérifier les données après les avoir fait graver sur le CD-ROM.

Systèmes essentiels et Internet

Quel est le moyen le plus facile de limiter les attaques contre un système d'exploitation vital ? La réponse est simple -- ne pas le brancher à un réseau externe. Ce n'est peut-être pas pratique dans une petite entreprise où un seul ordinateur suffit pour faire la comptabilité, le traitement de texte, la sauvegarde des fichiers et le furetage sur Internet. D'un autre côté, si vous utilisez un seul ordinateur pour le bureau et la maison et si les enfants s'en servent pour naviguer sur Internet et pour faire des jeux, vous aurez certainement un jour un problème grave de sécurité. Étant donné que les ordinateurs sont peu chers, il est certainement moins dispendieux à long terme d'avoir un ordinateur différent pour ces activités.

Mots de passe

Les pirates entrent dans uns système souvent en trouvant seul mot de passé.

Est-ce que pour vos cartes bancaires le PIN est la date de votre anniversaire ? Est-ce que votre mot de passe est le même que votre nom d'utilisation, un mot simple dans un dictionnaire français, ou pire, un vide ? Est-ce que vous vous servez du même mot de passe pour tout ? Si la réponse à une de ces questions est "oui," il faut repenser votre stratégie. Il vous faut des mots de passe « forts » comprenant au

moins 6 à 8 caractères alphanumériques à tout moment. Vous ne devrez pas utiliser un mot de passe multi usage. Personne ne porte sur son trousseau de clés une seule clé pour démarrer la voiture, ouvrir la maison et accéder à son coffret de sûreté.

Mise à jour régulière de votre système

De nouvelles vulnérabilités apparaissent sans cesse à l'intérieur du système d'exploitation et dans les logiciels. Vous devez minimiser ces menaces potentiellement dévastatrices en gardant votre système à jour autant que possible. Il existe bien sûr le risque que le système puisse devenir instable après des mises à jour, mais ce risque est moins grand que la possibilité d'un trou de sécurité dans une application particulière. Les vendeurs de systèmes d'exploitation fournissent des notifications gratuites de mises à jour au niveau de la sécurité pour que l'usager soit capable de devancer les risques.

Coupe-feu

Si le coupe-feu est la porte fermée à clef de votre maison, le logiciel c anti-virus serait votre système d'alarme.

Un coupe-feu est du matériel ou un logiciel (ou les deux) qui inspecte et permet ou bloque l'accès à un réseau particulier. On l'installe, d'habitude, entre l'usager et Internet. Le composant matériel qui relie les deux réseaux s'appelle le routeur. Une partie de sa fonction est d'être un coupe-feu entre les réseaux. Le logiciel de routage sur les ordinateurs personnels, de plus en plus courants, est assez simple pour être mis en place par un usager ordinaire.

Ce que nous appelons souvent des virus sont en fait des logiciels malveillants assez distincts.

Le coupe-feu est souvent votre protection de choix contre les intrusions venant d'Internet. Pour cette raison, leur configuration et entretien sont le domaine du professionnel. L'approche normale est de fermer tout au départ puis ouvrir peu à peu des « trous » dans le coupe-feu pour permettre l'accès aux services d'Internet que vous utilisez ou que vous fournissez à l'extérieur.

Logiciels malveillants

Quand nous pensons aux programmes malveillants, nous nous servons souvent du terme « virus », ce qui n'est pas tout à fait précis puisque le virus possède un comportement distinctif. Le terme « programme malveillant, » plus général, se réfère à l'ensemble de ces entités.

- **Virus** – Bien qu'il n'existe aucune définition universellement acceptée de ce qui constitue un virus, la plupart des spécialistes s'accordent à dire que le virus est un programme dont le but premier est de répliquer des fichiers existants, généralement avec un résultat malveillant.
- **Vers** – Au lieu d'infecter des fichiers existants, le ver se réplique et infeste le réseau, s'accaparant de ressources en le faisant. Un ver du courrier électronique, p.ex. passera de l'ordinateur infecté à d'autres ordinateurs en s'envoyant à toutes les adresses électroniques dans la liste d'adresses de l'appareil.
- **Cheval de Troie** – Comme le cheval de Troie en mythologie grecque, le cheval de Troie se passe pour un programme légitime dans le but d'obtenir des informations confidentielles chez un usager qui ne soupçonne pas qu'il est là.
- **Logiciel publicitaire** -- Ce type de programme malveillant, qui fait paraître sur l'écran des bannières publicitaires non-voulues, est difficile à enlever du système.
- **Logiciel espion** – Ce type de programme fait la collecte en secret des renseignements utiles pour les vendeurs potentiels pendant que vous utilisez l'ordinateur. Le logiciel espion malveillant s'efforce d'obtenir des renseignements personnels ou confidentiels sans que vous soyez prévenus.

Protection contre des logiciels malveillants

Le virus peut corrompre le système d'exploitation, infecter les disques durs, détruire des fichiers et se répandre comme un feu de forêt. Les vers sur Internet ont causé l'arrêt complet des grandes corporations. Le cheval de Troie peut permettre aux pirates informatiques d'avoir accès à votre système. Et pire, la plupart des attaques de nos jours combinent ces trois approches. La meilleure protection contre de telles attaques est de ne pas se laisser infecter du tout.

Les logiciels anti-virus sont très employés de nos jours, mais bon nombre d'entrepreneurs négligent de faire une mise à jour des définitions de façon régulière. Une telle mise à jour est obligatoire car de nouvelles menaces apparaissent tous les jours. La plupart des logiciels vous donnent la possibilité de faire faire une mise à jour régulière. Quand l'ordinateur n'est pas branché à Internet, il faut faire faire une mise à jour manuelle en même temps que se font les autres mises à jour.

Les faiseurs de logiciels anti-virus commencent à considérer les logiciels publicitaires comme des menaces comme les virus et les vers. Heureusement, on peut aussi enlever ces logiciels en se servant d'outils destinés à le faire. En attendant que le logiciel anti-virus et celui qui enlève les logiciels publicitaires soient mis ensemble dans un seul ensemble, vous aurez besoin de faire fonctionner séparément les deux types de programmes de façon régulière.

Chiffrement SSL

Le SSL est la méthode la plus utilisées pour faire des communications sécurisées sur Internet

La sécurité de votre ordinateur est très importante mais il faut aussi sécuriser toutes vos communications avec le monde extérieur. Imaginez les secrets disponibles aux autres si quelqu'un pouvait écouter toutes vos conversations téléphoniques. Le programme *Secure Sockets Layer*, connu par le sigle SSL est devenu la technologie la plus utilisée pour le cryptage ou le chiffrement des données dans Internet.

Nous rencontrons le chiffrement SSL le plus souvent quand un site Web sécurisé nous demande d'envoyer des informations de nature délicate. Ces sites Web commencent par *https://* et non pas *http://*. Votre navigateur d'Internet vous signalera que les données expédiées à ce site seront codés. Le système SSL peut fonctionner avec d'autres services Internet mais c'est surtout les sites Web sécurisés qui s'en servent.

Un autre aspect de SSL est qu'on peut s'en servir pour valider ou authentifier l'identité de l'expéditeur et du récepteur. Cette caractéristique étonnante vient de l'algorithme utilisé par le système SSL. Le domaine du cryptage est très évolué mais en termes simples le SSL vous permet de mettre sur vos messages une *signature digitale* vous identifiant. On appelle cette signature digitale parfois une *clé*, indiquant soit l'identité du serveur soit l'identité de la personne qui s'en sert.

Une autorité de certification est l'équivalent en ligne d'un notaire public. .

Pour toutes les personnes qui résistent encore à ce discours technique, vous vous rendez compte peut-être qu'il manque un élément important quand il s'agit d'établir un niveau suffisant de confiance entre deux personnes. Si vous voyez une signature sur un document digital, ce n'est pas important à moins qu'une autre personne à qui vous faites confiance accepte de garantir que la signature est

authentique. Nous connaissons cette situation hors ligne quand nous nous servons des notaires publics pour porter garant sur l'identité d'une personne.

L'équivalent d'un notaire public dans Internet est une autorité de certification (AC). Si un AC met sa signature sur un document SSL vérifié, vous pouvez avoir confiance que l'AC garantit l'identité de la personne ou du site Web. Il existe assez peu d'autorités de certification à qui votre navigateur fera confiance. VeriSign est l'AC le plus connu du public.

Mettons ensemble le processus. Quand vous visitez un site Web sécurisé, ce site Web envoie un certificat à votre navigateur qui retient avec le message le nom du domaine pour obtenir par la suite une vérification signée par un AC reconnu. Si le nom de domaine retenu n'est pas celui de l'adresse électronique, votre navigateur générera un avertissement avant de continuer. Il génère le même avertissement si le certificat n'est pas signé par un AC de foi ou si le certificat n'est plus valide. (Un certificat signé par un AC est valide de façon générale pendant un ou deux ans puis il doit être renouvelé). Si vous remarquez cet avertissement, vous ne pouvez pas faire confiance au site Web -- le nom donné et le site ne coïncide pas --. Il faut dans ce cas ne plus visiter le site.

On estime que la confiance ne fonctionne que dans un sens puisque le site Web sécurisé n'exige pas que vous ayez vous même une identité digitale. En général, l'authentification du visiteur se fait par d'autres moyens -- la possession d'un compte d'utilisateur muni d'un mot de passe, par exemple. L'exigence que les usagers s'identifient en se servant d'une identité digitale est une technique puissante mais qui coûterait un peu au niveau du consommateur. Un des endroits où l'identité de l'usager est exigée est le courriel électronique sécurisé. Ce système n'a pas encore été adopté par le public. En attendant la résolution de problèmes associés aux entreprises, aux gouvernements et aux problèmes de logistique, cette méthode de vérification de l'identité digitale ne sera que rarement utilisé par le public.

Sommaire

La sécurité sur Internet ne doit être prise à la légère. Vous aurez besoin des méthodes efficace, proactives, pour protéger les informations personnelles des clients et aussi vos communications et fichiers personnels. Le plus important est de suivre toujours les méthodes les plus sécuritaires possibles pour vous protéger contre les menaces. Vous pourriez faire venir un expert en sécurité pour faire une vérification de votre système comme vous feriez dans le cas de votre état financier en faisant venir un vérificateur certifié. Nous espérons que ce guide a augmenté votre connaissance des problèmes de sécurité et que les renseignement ci-dessus vous aidera à établir un plan d'action en sécurité dans votre entreprise.

Ressources

- About.Com – « Logiciels anti-virus »
  http://antivirus.about.com
- CIO.com: Securit´sur Internet
  www.cio.com/research/security
- Microsoft – « Sécurité fiable en informatique » "
  www.microsoft.com/security
- Commissarait à la protection de la vie privée du Canada
  www.privcom.gc.ca
- Securité des opérations
  www.operationsecurity.com
- Soltrus Inc
  www.soltrus.com/english/corporate/library.html
- Réponses aux problèmes de sécurité chez Symantec
  www.sarc.com
- Thawte: Certificat digital
  www.thawte.com
- Verisign: Certificat Digital
  www.verisign.com

ALBERTA centreducyberfutur

Contactez-nous

Le Centre cyberfutur de l'Alberta, une initiative de *Liaison entreprise*, est votre premier point de contact en Alberta pour tout renseignement concernant le cybercommerce. Nous offrons des conseils et des renseignements gratuits, impartiaux et faciles à comprendre sur le cybercommerce pour les petites et moyennes entreprises. Notre but est d'aider les entrepreneurs à prendre des décisions éclairées en vue de leur adaptation aux changements technologiques. Si vous avez des questions, une simple visite, un appel téléphonique ou un simple clic de la souris vous permettront d'y trouver réponse.

Le Centre du cyberfutur de Liaison Entreprise

Ligne d'information sur les affaires : 1 800 272-9675

Edmonton : 10237, 104e Rue N.-O., bureau 100, Edmonton (Alberta) T5J 1B1
Tél. : 780 422-7722 **Téléc. :** 780 422-0055

Calgary : 639, 5e Avenue S.-O., bureau 250, Calgary (Alberta) T2P 0M9
Tél. : 403 221-7800 **Téléc. :** 403 221-7817

Courriel : info@cyberfutur.ca **Site Web :** www.e-future.ca/alberta

Ce guide a été préparé par *le Centre du cyberfutur du Manitoba*

Membre de l'Équipe d'affaires électroniques de l'Ouest