TROUSSE DE SURVIE

Sécurité de l'information

Bonjour,

J'ai le plaisir de partager avec vous cette trousse de survie en sécurité de l'information.

Je vous propose plus de 60 recommandations pratiques qui vous permettront d'adopter de bonnes habitudes dans l'utilisation de données numériques.

Prenez un crayon et cochez celles que vous mettez en pratique.

Bonne lecture !

Mario Lapointe, ing. MBA CISA CGEIT
mario.lapointe@metastrategie.com

Numéro ISBN 978-2-924737-01-9

INTRODUCTION

Comme l'information numérique fait désormais partie de notre quotidien, il est primordial de la protéger. En effet, les failles de sécurité sont trop souvent présentes. Nous devons les contrer à tout prix.

L'accès aux données et aux renseignements personnels est maintenant facile et abordable grâce à l'utilisation généralisée d'internet, des ordinateurs portables, des tablettes, des téléphones intelligents, des technologies mobiles et sans fil. La contrepartie de cette avancée est indéniable, puisque les occasions ne manquent pas d'attaquer ces actifs : vol de données, attaques malveillantes utilisant les virus, piratage, vol d'identité, crime organisé… Ces risques, combinés aux erreurs d'inattention, peuvent entraîner de graves dommages personnels, comme le vol d'identité, ou financiers, comme les détournements de fonds, et peuvent même ternir la réputation d'une entreprise.

Nous avons conçu ce guide pour fournir des conseils essentiels et des outils pratiques aux utilisateurs de tout type d'ordinateurs et de dispositifs personnels (téléphones mobiles, ordinateurs portables et tablettes) afin de les aider à se protéger contre ces risques.

Vous y apprendrez l'importance d'améliorer votre sécurité informatique et comment le faire correctement.

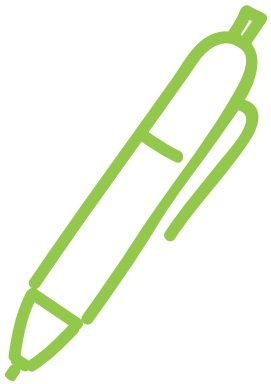
Rassurez-vous, la mise en place d'une bonne sécurité n'entraîne pas nécessairement de grandes dépenses d'argent et de temps. En effet, la sensibilisation au problème, la reconnaissance des risques potentiels et l'utilisation prudente des technologies de l'information (TI) ne coûtent rien. Il existe aussi de nombreuses technologies de protection des actifs peu coûteuses. Par contre, il convient d'adopter de saines habitudes et de bons comportements pour rendre les efforts efficaces à long terme : l'individu contribue à plus de 80 % du facteur de réussite dans la protection de l'information.

POUR COMMENCER

Voici quelques principes qui pourront vous aider dans l'utilisation des services offerts sur internet :

- Tout se paye d'une manière ou d'une autre sur internet, ***la gratuité n'existe pas.***
- Toute information diffusée sur internet, y compris par ***les réseaux sociaux, SMS, courriel,*** etc. :
    - Doit être ***considérée comme publique***,
    - Ne peut pas être effacée et doit donc être ***considérée comme permanente,***
    - ***Engage la responsabilité*** de son auteur ou de l'entreprise dont il origine et doit être considérée comme pouvant être utilisée en preuve dans un recours en justice,
    - Peut devenir la propriété du propriétaire de l'application qui peut ***en disposer à sa guise.***
- Toute activité sur internet comporte un ***danger,*** le risque nul n'existe pas.
- Toute diffusion de photos ou de vidéos sur internet doit préalablement avoir été ***autorisée par les participants.***

- Tout ***renseignement personnel*** permettant de vous identifier et de vous localiser doit être ***protégé en tout temps.***
- Toute information, confidentielle ou secrète, d'une organisation doit être protégée en tout temps.



☐ Cases à cocher

VOUS ÊTES UN UTILISATEUR À RISQUE

Les situations suivantes montrent comment les utilisateurs peuvent être exposés à des risques de sécurité de l'information :

- ☐ ***Ignorer les dangers*** de l'utilisation d'internet.
- ☐ Utiliser un ***logiciel défectueux*** ou peu fiable avec des failles de sécurité.
- ☐ Utiliser un ***vieux système d'exploitation*** sans mise à jour de sécurité.
- ☐ Utiliser de ***vieux logiciels de sécurité*** ou d'application, tels que navigateur et logiciel de messagerie électronique, ce qui augmente la probabilité de pannes du système et de pertes de données.
- ☐ Être exposé à la pornographie et à d'autres ***médias indésirables.***
- ☐ Permettre ***l'utilisation incontrôlée*** par les enfants, les amis, etc.
- ☐ Utiliser l'ordinateur du domicile pour des ***activités d'une entreprise,*** exposant ainsi l'information d'entreprise à de nouveaux risques.

- ☐ Effectuer des actions qui nous exposent à ***l'usurpation d'identité*** par des virus, des logiciels-espions, de l'hameçonnage, du pourriel et d'autres attaques.

À LA MAISON

La présente section s'adresse à deux types d'individus à domicile :

- ☐ Ceux n'ayant aucune connaissance technique,
- ☐ Ceux dont les connaissances sont plus avancées, mais qui ne sont pas nécessairement informés de tous les risques et enjeux de sécurité.

Deux listes de précautions de base sont fournies pour guider ce large éventail d'individus.

VOS PRÉCAUTIONS DE BASE

Voici les précautions de base à adopter, pour tous les types d'utilisateurs :

- ☐ ***Acquérir un logiciel de sécurité*** complet et reconnu pouvant être obtenu auprès de tous les revendeurs de logiciels d'ordinateurs, et qui dispose de toutes les principales fonctions :

antivirus, anti-logiciels-espions, pare-feu et filtrage de contenu. Si nécessaire, recourir à un spécialiste pour en assurer une bonne installation.

- ☐ S'inscrire pour obtenir les ***mises à jour automatiques*** du système d'exploitation, du logiciel de sécurité, des principales applications, telles que le navigateur et le logiciel de gestion des courriels, ainsi que la maintenance pour veiller à ce que la protection soit active et fonctionnelle.
- ☐ Ne pas ouvrir de ***pièces jointes inconnues,*** et être conscient que les adresses courriel peuvent être truquées. Laisser le soin au logiciel de sécurité de vérifier tous les courriels. Suivre les conseils donnés par l'outil.
- ☐ Obtenir de temps à autre des conseils de techniciens certifiés pour veiller à ce que l'installation de l'ordinateur n'ait pas de ***failles de sécurité*** importantes.
- ☐ Éteindre l'ordinateur ou le déconnecter du réseau internet quand il ***n'est pas utilisé.***
- ☐ Faire des ***sauvegardes régulières*** des données sur des supports amovibles et les entreposer dans une autre pièce que celle où se trouve l'ordinateur, ou idéalement dans un autre bâtiment.
- ☐ Choisir le lieu où est ***placé l'ordinateur*** disponible pour les enfants de manière à ce que son utilisateur ne soit pas isolé et que l'utilisation

soit mieux contrôlée. Activer les filtres de contrôle parental du logiciel de sécurité.

- ☐ Prodiguer des ***conseils aux enfants*** pour les guider dans le choix des sites qu'ils consultent. Demander conseil à un enseignant ou à un spécialiste technique si vous avez de réelles préoccupations au sujet de l'utilisation de l'ordinateur pour les enfants.
- ☐ Éviter des ***copies de données personnelles*** ou confidentielles sur un ordinateur portable, tablette ou téléphone cellulaire. Faire attention de ne pas laisser les appareils dans des endroits où ils peuvent être volés. Activer un code de sécurité sur l'équipement.
- ☐ Utiliser un ***logiciel de cryptage*** qui brouille les données en demandant un mot de passe pour protéger des données personnelles ou confidentielles pendant une transmission sur le réseau internet ou une copie sur une clé USB ou un autre support de transport.
- ☐ Se méfier des ***clés USB*** ou des ***disques durs externes*** avant de les raccorder à votre équipement.
- ☐ ***Visiter uniquement*** des sites web et des fournisseurs reconnus si vous utilisez internet pour des raisons professionnelles ou personnelles, telles que le magasinage. Ne pas fournir plus de renseignements personnels ou d'entreprise que ce qui est vraiment nécessaire.

- ☐ S'inscrire pour un ***soutien technique*** sur votre site si vous comptez sur des ordinateurs personnels pour faire des affaires. S'assurer de la disponibilité sur appel des techniciens en cas de problème.
- ☐ Consulter le ***personnel de l'entreprise*** responsable du soutien technique du système si vous travaillez à domicile sur vos ordinateurs, afin de vous assurer que vous suivez bien les règles de sécurité de l'entreprise.
- ☐ Se rappeler que « ***débrancher l'alimentation électrique*** ou retirer la batterie » peut et va cesser toute attaque si vous pensez que quelque chose va mal ou que l'ordinateur se comporte d'une manière inattendue. Appeler un conseiller spécialiste pour vérifier le système avant de redémarrer l'équipement.

VOS PRÉCAUTIONS PLUS AVANCÉES

Voici les précautions plus avancées à adopter, pour les utilisateurs techniquement plus compétents :

- ☐ Produire un ***disque de démarrage,*** un CD-ROM ou un DVD pour récupérer le système d'exploitation si l'ordinateur est endommagé ou compromis par des failles de sécurité et d'autres défaillances.

- ☐ Enregistrer sur un disque une ***pièce jointe inconnue,*** si vous avez besoin de l'ouvrir. Exécuter le logiciel antivirus sur ce fichier et éventuellement déconnecter le réseau internet avant son ouverture.
- ☐ Ne pas exécuter des ***programmes d'origine inconnue,*** même s'ils sont attrayants. Être conscient qu'ils peuvent contenir des logiciels malveillants si vous envisagez de les envoyer à d'autres personnes.
- ☐ Utiliser les ***logiciels gratuits*** avec prudence.
- ☐ Ne pas transmettre des logiciels, des fichiers ou des courriels pouvant contenir des virus illégaux. Se rappeler que vous pouvez être ***tenu responsable*** pour avoir contribué à endommager d'autres équipements.
- ☐ Ne pas transmettre de façon inappropriée des renseignements confidentiels ou personnels. Toujours rester vigilant quant à la ***valeur des données*** détenues.
- ☐ Configurer les réseaux sans fil correctement en ***activant le cryptage*** de la télécommunication qui demande un mot de passe pour utiliser le service et veiller à ce que l'accès soit géré correctement.

AU BUREAU

Les utilisateurs professionnels manipulent des données numériques dans le cadre de leur travail en entreprise.

Les exemples suivants montrent comment les utilisateurs professionnels peuvent être exposés à des risques de sécurité de l'information. Les comportements suivants sont à risque :

- ☐ ***Ignorer les politiques*** d'entreprise, les procédures de sécurité et leurs responsabilités personnelles. Ne pas prendre connaissance des politiques d'entreprise et des procédures de sécurité, et ne pas assumer ses responsabilités personnelles pour la sécurité.
- ☐ ***Sous-estimer la valeur*** de l'information de l'entreprise.
- ☐ ***Partager un identifiant*** ou un mot de passe avec des collègues ou des amis.
- ☐ Utiliser, hors du bureau, un ordinateur, des appareils portatifs et d'autres supports informatiques comprenant des ***données de l'entreprise.***
- ☐ ***Conserver, à son domicile,*** de l'information d'entreprise sur des dispositifs qui contiennent des renseignements personnels ou confidentiels. Le risque est accru si cet équipement est portable.

VOS HABITUDES À PRIVILÉGIER

Voici les comportements qu'un utilisateur professionnel dans une entreprise doit adopter :

- ☐ ***Comprendre la responsabilité*** personnelle à l'égard de la sécurité de l'information et maintenir à jour les connaissances des politiques de l'entreprise sur l'utilisation des logiciels, du réseau de télécommunication, d'internet, des logiciels antivirus, des anti-logiciels-espions, etc.
- ☐ ***Rester informé*** sur les règles de sécurité établies, les appliquer et obtenir toute l'information nécessaire pour bien les comprendre dans un environnement en évolution.
- ☐ ***Être conscient*** des types d'incidents de sécurité qui peuvent se produire.
- ☐ ***Signaler les incidents*** et les problèmes de sécurité, notamment :
    - o violations d'accès,
    - o sauvegardes insuffisantes,
    - o indisponibilité du système,
    - o transactions électroniques mal contrôlées ou sujettes à l'erreur,
    - o problèmes d'équipements, présence d'équipements inconnus, bris d'équipements, etc.,

- o présence de personnes non identifiées sur le lieu de travail.

☐ ***Changer les mots de passe*** immédiatement à la prise de possession d'un dispositif ou d'un équipement, puis régulièrement conformément à la politique. S'assurer que le mot de passe choisi est difficile à deviner et répond aux meilleures pratiques établies pour la longueur, la complexité, les mots inacceptables car trop communs. Par exemple, un mot de passe qui comprend plus de 11 caractères est une bonne pratique.

☐ Ne pas ***inscrire son mot de passe*** dans un document pouvant être lu par une autre personne.

☐ Se rappeler qu'un courriel ne peut être effacé et qu'il peut être retenu contre l'auteur ou son entreprise et que cette preuve peut être ***conservée pour toujours.***

☐ Effectuer des ***sauvegardes régulières*** des données critiques et les essayer périodiquement pour s'assurer que les données puissent être restaurées. S'assurer que l'entreprise a clairement défini une responsabilité et nommé une personne responsable pour réaliser les sauvegardes, afin qu'elles puissent être restaurées, ou s'assurer qu'un service de l'entreprise s'occupe des sauvegardes.

☐ ***Verrouiller votre session*** de travail dès que vous vous absentez.

- ☐ ***Vérifier le bureau*** au moment de quitter la session afin que les supports contenant des données, les documents ou les équipements importants ne soient pas visibles et facilement disponibles. Verrouiller le bureau à votre départ.
- ☐ ***Éliminer des renseignements*** confidentiels efficacement et définitivement, déchiqueter le support papier, détruire mécaniquement les disques et les médias, etc.
- ☐ Utiliser ***l'impression sécurisée*** avec un mot de passe pour les documents confidentiels.
- ☐ Utiliser les ***espaces disques sécurisés*** pour y enregistrer les documents produits pour l'entreprise.
- ☐ Remettre, à la bonne personne, tout le ***matériel de l'entreprise,*** y compris les fichiers de données, à la cessation de l'emploi.

VOS HABITUDES À ÉVITER

Voici les comportements qu'un utilisateur professionnel dans une entreprise doit éviter :

- ☐ Utiliser les ressources informatiques de l'entreprise à des ***fins non autorisées*** (par exemple, violation intellectuelle, protection de la propriété, contenu illégal).
- ☐ ***Négliger la valeur*** des renseignements confidentiels entre vos mains et la protection adéquate de ces derniers (sur un support portable, par exemple, CD, DVD, clé USB, carte mémoire, téléphone mobile, tablette, ordinateur, portable, etc.).
- ☐ ***Divulguer des données confidentielles*** à tous ceux qui ne sont pas autorisés à les recevoir ou qui n'ont pas besoin de les connaître.
- ☐ ***Sortir des données confidentielles*** de l'entreprise sans autorisation.
- ☐ ***Dire à d'autres*** personnes votre ***mot de passe*** ou partager votre carte d'accès ou tout autre mécanisme d'authentification avec quelqu'un.
- ☐ ***Ignorer les incidents*** de sécurité.
- ☐ Laisser vos équipements informatiques ***sans surveillance*** et accessibles pour des périodes prolongées.

- ☐ ***Contourner les règles*** de connexion réseau établies (par exemple, en créant un réseau WIFI supplémentaire avec votre téléphone mobile).
- ☐ ***Contourner les logiciels*** de contrôle de sécurité, de surveillance d'antivirus, d'anti-logiciels-espions ou d'autres logiciels similaires.
- ☐ Télécharger ou utiliser des ***logiciels piratés*** ou ***gratuits*** sans autorisation sur un ordinateur de l'entreprise.
- ☐ ***Introduire ou enlever*** des équipements informatiques sans autorisation.

Au sujet de

Mario Lapointe est un passionné des technologies de l'information. Il conseille les travailleurs autonomes et les entreprises à sélectionner les bonnes technologies pour mieux répondre à leurs besoins d'affaires.

N'hésitez pas à lui soumettre vos problèmes en matière de technologie. Il saura optimiser vos besoins d'affaires grâce à sa rigueur, à son intégrité et à sa longue expérience du domaine.

Offre de services :

1. **Accompagnement dans vos décisions d'affaires et de technologie**

2. **Conception de solutions**

3. **Surveillance de l'atteinte de vos objectifs**

Mario Lapointe, ing. MBA CISA CGEIT
mario.lapointe@metastrategie.com

Métastratégie cabinet-conseil
1651, ch. Ste-Foy, bur. 200
Québec (Québec) G1P 2P1

Cette trousse est une adaptation et une mise à niveau de : Cobit Security Baseline, *An information security survival kit*, 2nd edition, Isaca, 2007.

Passez à l'action !

L'information numérique est très présente dans notre environnement, à la maison comme au travail. Elle est devenue un actif important dont la sécurité est un enjeu essentiel à comprendre et à considérer dans nos décisions.

Cette trousse de survie contient plus de 60 pratiques à intégrer dans vos habitudes de vie afin de protéger ce qui est précieux : votre identité et votre entreprise ou employeur.

Passez à l'action et cochez les pratiques que vous adoptez.

Conservez ce guide pratique !

MÉTASTRATÉGIE
CABINET CONSEIL

978-2-924737-01-9