L'utilisation des portables, déplacements et télétravail

La sécurité des informations, j'y veille! *Volume 2, Numéro 3, Avril 2012*

Avec les nouvelles technologies de l'information et de la communication, il est maintenant beaucoup plus simple pour les employés d'exercer leurs activités en dehors des locaux professionnels, de continuer de travailler lors de leurs déplacements, de formation à l'extérieur ou de réunions et d'effectuer du télétravail. Des portables sont souvent mis à la disposition des employés pour faciliter leurs déplacements ou le télétravail. Mais qu'en est-il des risques pour la sécurité de l'information?

L'utilisation des ordinateurs portables!

Il est primordial de conscientiser les utilisateurs à propos des bonnes pratiques lors de l'utilisation de l'équipement de l'organisation, à l'extérieur de ses locaux. La possibilité d'effectuer le travail à la maison comporte son lot d'avantages, mais comporte également des risques pour la sécurité de l'information.

Voici quelques bonnes pratiques :

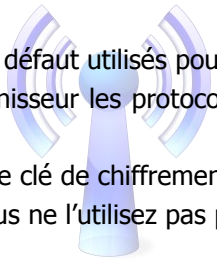
⇒ Utilisez l'équipement mis à votre disposition uniquement à des fins professionnelles.

⇒ Ne laissez personne d'autre que vous utiliser l'équipement fourni par votre employeur.

⇒ Évitez de conserver de l'information sur des équipements personnels.

⇒ Si vous avez un réseau sans fil à la maison et que l'ordinateur utilisé pour le travail est relié à ce même réseau, prenez soin de bien le sécuriser :

- Changez le nom et le mot de passe par défaut utilisés pour gérer votre point d'accès sans fil;
- Activez ou faites activer par votre fournisseur les protocoles de chiffrement (WPA2) au lieu de WEP et WPA;
- Utilisez un mot de passe robuste comme clé de chiffrement;
- Éteignez votre point d'accès lorsque vous ne l'utilisez pas pour une période prolongée.



L'utilisation des mobiles!

L'utilisation des mobiles et des tablettes dans le système d'information représente une nouvelle source d'insécurité. L'utilisation du téléphone intelligent et des tablettes, aussi bien à titre personnel qu'à titre professionnel, présente des risques de perte de données non négligeables. La perte du mobile, les fuites d'information ou encore le vol sont autant de dangers qui guettent la sécurité du système d'information, sans parler du partage de données sensibles sur les réseaux sociaux externes ou de la propagation des logiciels malveillants par le téléchargement d'applications.

Agence de la santé et des services sociaux de la Côte-Nord
Québec

De plus, peu de gens utilisent la fonction de mot de passe intégrée. Il est donc important de verrouiller l'accès au mobile à l'aide d'un mot de passe afin d'assurer la confidentialité des données. Limitez l'information que vous stockez sur l'appareil mobile. Conservez uniquement l'information nécessaire. Désactivez le service Bluetooth lorsqu'il n'est pas utilisé. Joignez uniquement les réseaux WiFi autorisés.

Déplacements et lieux publics!

Plusieurs d'entre vous, dans le cadre de leur travail, doivent se déplacer pour des formations, des colloques, des réunions, etc. Dans les périodes d'attente, certains profitent de ces moments pour s'avancer dans leur travail. Mais attention, la prudence est de mise dans les lieux publics, tels les aéroports, les hôtels, les cybercafés, etc.

Voici quelques bons conseils :

⇒ Ne laissez jamais votre ordinateur portable ou tout autre média à la vue ou dans la voiture, sans surveillance. Les portables sont des biens de grande valeur, extrêmement vulnérables au vol. De plus, l'équipement informatique laissé dans la voiture pourrait être endommagé par la chaleur ou par le froid intense.

⇒ Méfiez-vous du « shoulder surfing ». Cette expression anglophone fait référence à une méthode consistant à utiliser des techniques d'observation directe pour recueillir de l'information (regarder par-dessus l'épaule). Cachez les frappes au clavier lorsque vous saisissez un NIP par exemple.

⇒ Lorsque l'équipement est identifié à l'aide d'un autocollant arborant le logo de l'organisation ou le nom, essayez de cacher cette identification pour éviter d'attirer l'attention.

⇒ Si vous devez transporter des données sensibles, assurez-vous qu'elles sont protégées par un mot de passe et chiffrées, si possible.

⇒ Évitez les réseaux sans fil non sécurisés, qui n'utilisent pas de chiffrement. Vos communications seront interceptées plus facilement sur ceux-ci.

⇒ Désactivez les protocoles de communication sans fil (WiFi, Bluetooth), lorsqu'ils ne sont pas utilisés.

⇒ Évitez toute discussion relative à des dossiers confidentiels.

Et enfin…

⇒ **Utilisez le service d'accès à distance sécurisé (jeton téléaccès).** Les données sont cryptées et protégées, même en naviguant sur un réseau public comme Internet. Si votre travail le justifie, une demande d'accès au service téléaccès peut être effectuée auprès de votre gestionnaire dans votre organisation ou encore auprès du RSAI de votre établissement.

Anne Paquet
Officier de sécurité régional
Direction régionale des ressources informationnelles (DRRI)
Pour questions ou commentaires : anne.paquet.09siles@ssss.gouv.qc.ca

Dépôt légal
Bibliothèque et Archives nationales du Québec, 2012
ISSN : 1927-7911

Source : *Formation générale sur la sécurité de l'information et la protection des renseignements personnels,* Ministère des Services gouvernementaux du Québec / ISIQ / 2010.