Pratique recommandée en sécurité de l'information

Guide de sensibilisation à la sécurité de l'information
PR-070

ENSEMBLE on fait avancer le Québec

Québec

Pratique recommandée en sécurité de l'information

Guide de sensibilisation à la sécurité de l'information

Cette publication a été réalisée par
le Dirigeant principal de l'information
et produite par la Direction des communications
du Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – juillet 2017
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-79077-8

Remerciements

Le Secrétariat du Conseil du trésor remercie l'équipe de réalisation et le groupe de travail interministériel pour le travail qu'ils ont accompli dans le cadre de la production de ce guide.

Équipe de réalisation

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Socheat Sonn, chargé de projet
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Carmen St-Laurent
Bureau de décision et de révision

Pauline Rodrigue
Institut de tourisme et d'hôtellerie

Sothida Pong
Ministère de l'Immigration,
de la Diversité et de l'Inclusion

Marthe Anaïs Kambou
Ministère de la Santé et des Services sociaux

Alain R. Pagé
Régie de l'énergie

Stéphanie Lavoie
Régie du cinéma

Diane Archambault
Télé-Québec

Notes à l'intention du lecteur

Note 1 : Dans le présent document, le masculin est utilisé comme générique dans le but d'alléger le texte.

Note 2 : L'expression organisme public désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme des réseaux de l'éducation, de l'enseignement supérieur ainsi que de la santé et des services sociaux. [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement]

Note 3 : Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, ces derniers doivent les adapter à leur organisation et aux risques qui leur sont propres.

Table des matières

Liste des figures

Liste des tableaux

1. Introduction

Le présent guide est mis à la disposition des organismes publics (OP) appelés à élaborer et à mettre en œuvre un programme formel et continu de sensibilisation de leur personnel à la sécurité de l'information, élément clé pour assurer la pérennité du patrimoine numérique gouvernemental.

La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics énonce, dans sa quatrième partie, l'objectif d'assurer la sécurité de l'information. Pour réaliser cet objectif, l'une des principales actions envisagées consiste en la promotion de la sensibilisation à la sécurité de l'information par un ensemble d'activités permettant de conscientiser le personnel aux risques encourus et aux comportements à adopter à cet égard. Le présent guide répond à cette préoccupation.

Ce guide demeure générique de façon telle que chaque organisme puisse l'adapter à son contexte en fonction de ses propres enjeux. Il est appuyé par des capsules vidéo et par une présentation PowerPoint qui décrivent les conséquences et les préoccupations de sécurité associées à certains scénarios de risques.

Outre la présente section introductive, les autres sections de ce guide portent sur :

- ✓ le positionnement de la sensibilisation par rapport au système de gestion de la sécurité de l'information (SGSI);
- ✓ le partage des responsabilités des intervenants clés en matière de sensibilisation;
- ✓ la démarche de sensibilisation à la sécurité de l'information, qui s'articule en quatre étapes;
- ✓ les capsules vidéo présentant des mises en situation, les conséquences possibles d'une faille dans la sécurité et les précautions à prendre.

1.1 Contexte

Le présent guide s'inscrit dans une démarche visant à mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information. Celle-ci prend appui sur la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), sur la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics et sur quatre documents définissant le nouveau cadre de gouvernance de la sécurité de l'information dans l'Administration québécoise :

- ✓ la Directive sur la sécurité de l'information énonce, en son article 7, alinéa k), que les organismes publics doivent définir et mettre en place un programme formel et continu de formation et de sensibilisation;
- ✓ le cadre gouvernemental de gestion de la sécurité de l'information décrit, entre autres responsabilités, celles inhérentes à la sensibilisation;
- ✓ l'Approche stratégique gouvernementale en sécurité de l'information fixe les cibles gouvernementales à atteindre en matière de sécurité de l'information, dont la mise en place d'un programme formel et continu de sensibilisation;
- ✓ le Cadre de gestion des risques et des incidents à portée gouvernementale présente une approche de gestion des risques et des incidents susceptibles de porter atteinte à la sécurité de l'information gouvernementale, dont la mise en œuvre exige que des actions de sensibilisation soient menées à tous les échelons de l'organisation.

1.2 Public cible

Ce guide est à l'usage des principaux intervenants suivants :

- ✓ le responsable organisationnel de la sécurité de l'information (ROSI);
- ✓ le conseiller organisationnel en sécurité de l'information (COSI);
- ✓ le coordonnateur organisationnel de gestion des incidents (COGI);
- ✓ le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP);
- ✓ les détenteurs de l'information ou leurs mandataires désignés;
- ✓ les intervenants dans des domaines connexes à la sécurité de l'information (responsable de la vérification interne, responsable de la gestion documentaire, responsable de la sécurité physique, etc.).

Les responsabilités de ces intervenants en matière de sécurité de l'information sont décrites dans le cadre gouvernemental de gestion de la sécurité de l'information. Celles relatives à la sensibilisation sont détaillées à la section 3. Partage des responsabilités.

Objectifs du programme de sensibilisation

Un programme de sensibilisation s'adresse à une clientèle constituée d'utilisateurs de l'information, des équipements ou des infrastructures de l'organisation qui ont le statut d'employé, de contractuel ou autre. Il vise notamment à sensibiliser cette clientèle à l'importance :

- ✓ d'assimiler les dispositions des politiques, directives, règles et procédures en vigueur et de s'y conformer;
- ✓ de comprendre le fonctionnement des systèmes et des applications qu'elle utilise et d'en faire usage sécuritaire;
- ✓ de collaborer avec la direction au repérage et à la prise en charge des problématiques de sécurité de l'information et, si nécessaire, des besoins de formation;
- ✓ des actions à entreprendre afin de protéger l'information et les équipements utilisés. Ces actions comprennent, notamment, l'usage adéquat des mots de passe, la prise de copies de sauvegarde, l'usage des antivirus, le signalement des incidents et anomalies, le respect des consignes établies pour contrer les tentatives d'usurpation d'identité ou la propagation de codes malicieux.

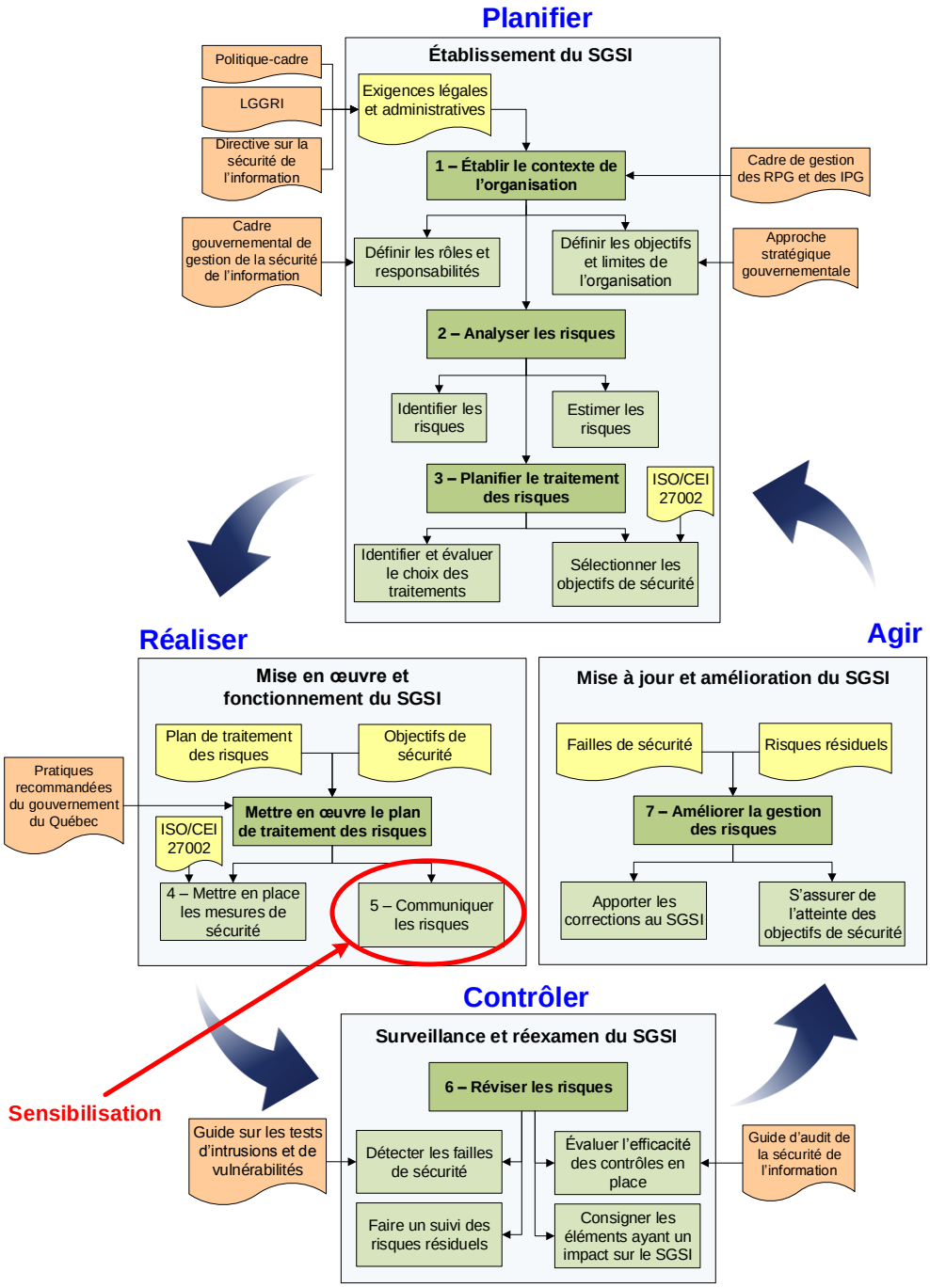
1.3 Cadre légal, administratif et normatif

L'élaboration d'un programme de sensibilisation s'appuie sur des lois, des directives, des pratiques gouvernementales, des normes internationales et des standards de l'industrie. Les principaux éléments constitutifs de ce cadre sont présentés à l'annexe i.

2. Positionnement de la sensibilisation

Comme illustré ci-après, la sensibilisation s'inscrit à l'étape 5 « Communiquer les risques » du système de gestion de la sécurité de l'information (SGSI), comme le préconise la norme ISO/IEC 27001. À titre de rappel, le SGSI, soit la démarche d'amélioration continue de la sécurité de l'information axée sur les risques, se décline en quatre étapes : planifier, réaliser, agir et contrôler.

Figure 1 : Positionnement de la sensibilisation dans un SGSI



3. Partage des responsabilités

La mise en place d'un programme de sensibilisation nécessite la contribution de plusieurs intervenants clés dont les responsabilités en matière de sensibilisation sont décrites dans la présente section.

Il est à noter que le contenu de cette section doit être ajusté par les réseaux (santé, éducation et enseignement supérieur) afin qu'il tienne compte des fonctions de sécurité définies pour les organismes publics qui leur sont rattachés. Ces fonctions découlent de la structure organisationnelle définie dans le cadre de gestion de la sécurité de l'information propre à chacun des réseaux.

3.1 Le responsable organisationnel de la sécurité de l'information (ROSI)

En tant que porte-parole du dirigeant principal de l'information (DPI), le ROSI assiste son dirigeant d'organisme dans la détermination des orientations stratégiques et des priorités d'intervention relativement à la sécurité de l'information. En matière de sensibilisation, le responsable organisationnel de la sécurité de l'information :

- ✓ coordonne l'élaboration et la mise en œuvre du programme de sensibilisation;
- ✓ soumet le programme de sensibilisation à la consultation du comité chargé de la sécurité de l'information et tient compte des éventuelles recommandations et suggestions;
- ✓ soumet le programme de sensibilisation à l'approbation de la haute direction.

3.2 Le conseiller organisationnel de la sécurité de l'information (COSI)

Le COSI apporte son soutien au ROSI, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques touchant la sécurité de l'information. Le conseiller organisationnel en sécurité de l'information élabore et met en œuvre le programme de sensibilisation en matière de sécurité de l'information. À cet effet, il :

- ✓ élabore le programme de sensibilisation;
- ✓ évalue les besoins de sensibilisation et détermine la clientèle cible;
- ✓ fixe les échéanciers des activités de sensibilisation et en assure le suivi;
- ✓ évalue régulièrement le programme de sensibilisation et procède aux ajustements nécessaires.

3.3 Le coordonnateur organisationnel de gestion des incidents (COGI)

Fort de sa connaissance des menaces et des situations de vulnérabilité et s'appuyant sur son expertise en matière de gestion des risques et des incidents, le COGI apporte au ROSI et au COSI le soutien nécessaire à la définition et à la mise en œuvre du programme de sensibilisation aux risques découlant d'une protection inadéquate de l'information.

3.4 Le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP)

Le RAIPRP joue un rôle de conseiller auprès du ROSI et du COSI dans l'élaboration et dans la mise en œuvre du programme de sensibilisation, notamment en raison de la forte interrelation, en ce qui a trait aux conséquences, entre sécurité de l'information, respect de la vie privée des citoyens et exigences légales en matière de protection des renseignements personnels.

3.5 Le détenteur de l'information

Le détenteur de l'information contribue à l'élaboration et à la mise en œuvre du programme de sensibilisation, notamment en raison de sa connaissance du degré de sensibilité de l'information relevant de son autorité. À cet effet, il :

- ✓ exprime les besoins de protection de l'information eu égard à la sensibilité de celle-ci et aux problèmes observés;
- ✓ contribue à la détermination de la clientèle cible du programme de sensibilisation;
- ✓ donne un avis sur la pertinence des activités de sensibilisation proposées et contribue à leur évaluation.

3.6 Le responsable de la vérification interne

Le responsable de la vérification interne joue un rôle clé dans la reddition de comptes en matière de sécurité de l'information. À des fins de sensibilisation, il examine et vérifie si :

- ✓ un programme de sensibilisation a été élaboré et s'il est mis en œuvre;
- ✓ les activités planifiées sont exécutées;
- ✓ les objectifs prévus sont atteints.

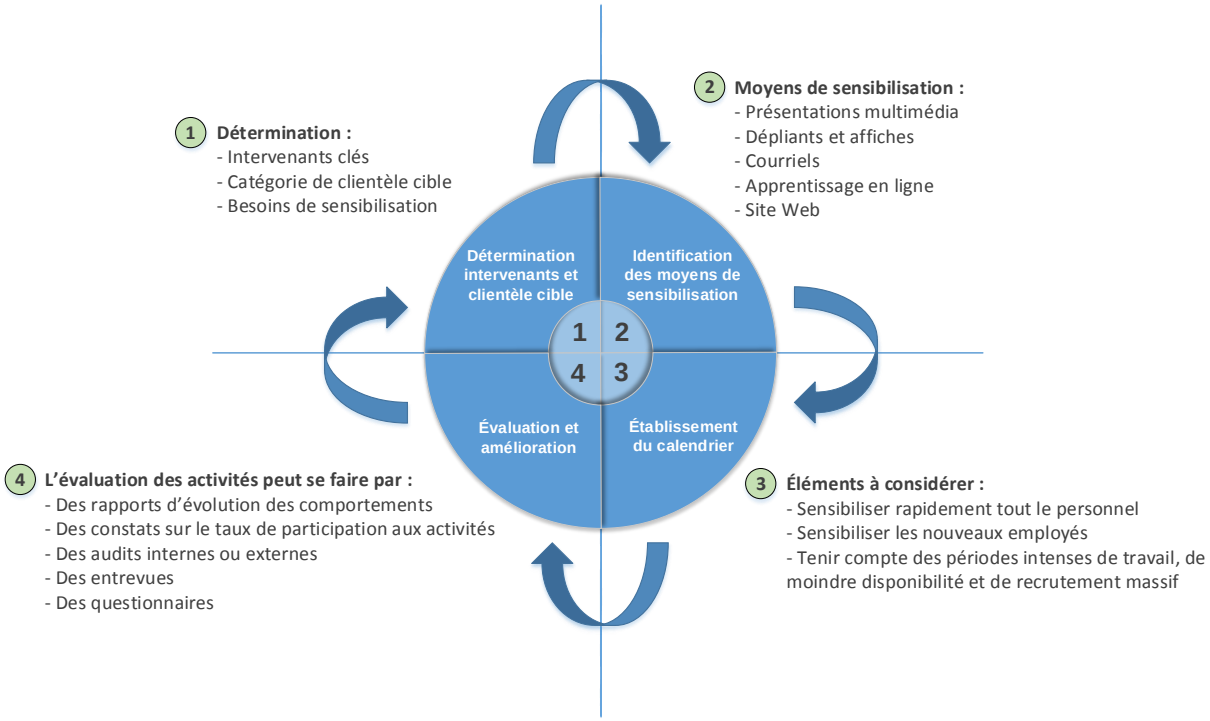
3.7 Les autres intervenants dans des domaines connexes à la sécurité de l'information

D'autres intervenants dans des domaines connexes à la sécurité de l'information peuvent exprimer leurs besoins en matière de sensibilisation et jouer un rôle de conseillers dans l'élaboration et dans la mise en œuvre du programme de sensibilisation. Il s'agit notamment du responsable de la continuité des services, du responsable de la gestion documentaire, du responsable de la sécurité physique, etc.

4. Démarche d'élaboration et de mise en oeuvre

La démarche d'élaboration et de mise en œuvre d'un programme de sensibilisation à la sécurité de l'information s'appuie sur une bonne compréhension des enjeux de l'organisation, sur une connaissance adéquate des risques encourus et sur l'application des meilleures pratiques en cette matière. Elle se décline en quatre étapes.

Figure 2 : Démarche de sensibilisation



4.1 Étape 1 - Détermination des intervenants et de la clientèle cible

L'élaboration et la mise en place d'un programme de sensibilisation nécessite :

- ✓ la contribution d'intervenants clés, dont les principales responsabilités en matière de sensibilisation sont décrites à la section section 3. Partage des responsabilités;
- ✓ la détermination des catégories de clientèles visées par le programme de sensibilisation (gestionnaires, spécialistes en sécurité de l'information, autres employés);
- ✓ l'identification des besoins de sensibilisation pour chaque catégorie de clientèle cible.

4.2 Étape 2 - Détermination des moyens de sensibilisation

Il est possible d'avoir recours à des moyens de sensibilisation différents selon la clientèle visée et les budgets disponibles. Les paragraphes suivants fournissent une description sommaire de ces moyens que les OP pourront utiliser pour élaborer leur propre programme de sensibilisation.

Le présent document ne constitue qu'un survol des moyens de communication disponibles. Pour en savoir davantage, des références sont fournies à l'annexe ii.

Les présentations multimédias (PDF, PowerPoint, etc.)

Les présentations multimédias sont généralement utilisées pour traiter plusieurs sujets ou une problématique particulière. Elles peuvent être enrichies par des objets animés, des capsules vidéo ou des images. Elles sont conçues de façon à faciliter l'interaction entre le présentateur et les participants. À titre d'exemple, des situations concrètes vécues par l'organisation, associées à la sécurité de l'information, peuvent être exposées. À cet égard, les mises en situation présentées à l'annexe iii, sous forme de capsules vidéo, visent à amorcer cette interaction.

Les dépliants et les affiches

Les dépliants peuvent être utilisés pour communiquer certains renseignements, notamment lorsqu'il y a plusieurs éléments à retenir, comme dans les énoncés de politique, les directives et certains documents de référence. Ils doivent être conçus de façon telle qu'on puisse les conserver et les consulter facilement.

Les affiches peuvent être utilisées pour rappeler certaines scènes des vidéos utilisées pour la sensibilisation. Elles peuvent avoir un effet subliminal si le message ou le slogan véhiculé est original, court et évocateur.

Les courriels

Le courriel peut être utilisé pour communiquer avec le personnel. Il doit cependant se limiter aux messages importants, voire urgents, pour éviter que les utilisateurs soient inondés et que l'efficacité de ce mode de communication s'en trouve diminuée.

L'apprentissage en ligne

L'apprentissage en ligne est basé sur l'utilisation des nouvelles technologies. Il permet l'accès à de la formation en ligne, interactive et parfois personnalisée, diffusée par l'intermédiaire d'Internet, d'un intranet ou d'un autre média électronique afin de perfectionner les compétences tout en rendant le processus d'apprentissage indépendant de l'heure et de l'endroit.

Le matériel de communication, tel que des capsules vidéo, des présentations ou des tests de connaissances, peut être disponible en ligne et être utilisé par le personnel dans une perspective d'autosensibilisation à la sécurité de l'information. Ce matériel devra être facilement accessible, régulièrement mis à jour et faire l'objet de promotion auprès du personnel concerné.

Autres moyens

Vidéoclips : les vidéoclips présentant des situations vécues ou réalistes ayant trait à diverses problématiques de sécurité de l'information peuvent être utilisés.

Sites Web : différents messages peuvent être communiqués au moyen de sites Web, notamment par la publication de questionnaires sur les comportements à éviter et sur ceux à adopter, sur des exemples d'incidents, de menaces et de situations de vulnérabilité, et ce, dans la perspective d'une bonne gestion des risques en matière de sécurité de l'information.

4.3 Étape 3 - Établissement du calendrier des activités de sensibilisation

L'évaluation des besoins de sensibilisation facilite le choix des moyens afférents et la définition du calendrier de mise en œuvre. À cet égard, il faut notamment :

- ✓ prévoir une période intense d'activités permettant de sensibiliser rapidement tout le personnel;
- ✓ prévoir des activités de sensibilisation des nouveaux employés;
- ✓ profiter de tendances ou d'événements fortuits pour tirer profit d'une plus grande réceptivité;
- ✓ tenir compte des périodes intenses de travail (fin de l'année budgétaire), de moindre disponibilité (vacances) ou de recrutement massif de personnel.

4.4 Étape 4 - Évaluation et amélioration des activités de sensibilisation

L'évaluation d'un programme de sensibilisation porte sur des éléments tels que : la qualité des séances de sensibilisation, la méthode de diffusion de l'information, le niveau de difficulté constaté par l'organisme et par la clientèle cible, la facilité d'utilisation des moyens de communication, la durée de l'activité de sensibilisation, sa pertinence par rapport aux besoins de la clientèle cible, l'actualité des éléments couverts et des suggestions d'amélioration des activités prévues.

L'évaluation du programme de sensibilisation peut être faite par :

- ✓ des rapports d'évolution des comportements en matière de sécurité de l'information (statistiques, tendances observées, accidents, erreurs, actes malveillants, demandes d'assistance ou d'information);
- ✓ des vérifications des comportements par le gestionnaire;
- ✓ des constats sur le taux de participation des utilisateurs (mesure de l'adhésion des utilisateurs) aux activités de sensibilisation. Ce taux peut refléter l'adéquation ou non des moyens de sensibilisation en ce qui a trait à la durée ou au contenu;
- ✓ des audits internes ou externes;
- ✓ des entrevues, des questionnaires généraux ou propres à une séance de sensibilisation (voir un modèle à l'annexe iv).

Les résultats de l'évaluation des activités de sensibilisation permettent d'ajuster le programme afin d'en assurer l'efficacité par rapport aux objectifs établis.

5. Exemple de programme de sensibilisation

Cette section présente un exemple de programme de sensibilisation adopté par un organisme fictif.

5.1 Étape 1 - Identification des intervenants et de la clientèle cible

Les intervenants clés dans l'élaboration et dans la mise en œuvre du programme de sensibilisation sont désignés. Le tableau suivant présente le nom de ces intervenants, leur fonction et leur rôle.

Tableau 1 : Intervenants clés

No	Nom	Fonction	Rôle
1	Prénom Nom 1	Responsable organisationnel de la sécurité de l'information (ROSI)	Agit en tant que maître d'ouvrage chargé de la coordination de la mise en œuvre du programme de sensibilisation; Approuve les activités de sensibilisation proposées; Analyse les rapports d'évaluation des activités de sensibilisation et propose des orientations pour améliorer le programme de sensibilisation.
2	Prénom Nom 2	Conseiller organisationnel en sécurité de l'information (COSI)	Agit en tant que maître d'œuvre, chef de projet responsable de l'élaboration et de la mise en œuvre du programme de sensibilisation; Désigne les groupes ou les catégories de personnes qui doivent être sensibilisées; Détermine, pour chaque groupe de personnes, les besoins particuliers en matière de sensibilisation; Sélectionne les activités de sensibilisation les mieux adaptées à chaque clientèle ciblée par le programme de sensibilisation; Établit le calendrier des activités du programme de sensibilisation; Évalue régulièrement le programme de sensibilisation et procède à son ajustement.
3	Prénom Nom 3	Coordonnateur organisationnel de gestion des incidents (COGI)	Définit les risques et les incidents qui peuvent survenir en matière de sécurité de l'information afin d'alimenter les activités de sensibilisation; Définit les principales tendances en matière de menaces et de vulnérabilités pouvant faire l'objet de sensibilisation.
4	Prénom Nom 4	Responsable de l'accès à	Conscientise le personnel concernant les exigences légales en matière d'accès à l'information et de protection

		l'information et de la protection des renseignements personnels (RAIPRP)	des renseignements personnels; Définit les conséquences d'une protection inadéquate des renseignements personnels et indique comment les éviter; Définit les bonnes pratiques à suivre pour s'assurer de la conformité aux exigences légales en matière d'accès à l'information et de protection des renseignements personnels.
5	Prénom Nom 5	Responsable de la sécurité physique (RSP)	Conscientise le personnel concernant les bonnes pratiques en matière de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités de son organisation; Définit les procédures recommandées pour accéder de façon sécuritaire aux locaux abritant des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle.
6	Prénom Nom 6	Responsable de la vérification interne (RVI)	Vérifie la réalisation de toutes les activités de sensibilisation prévues; Vérifie la réalisation des objectifs du programme de sensibilisation; Propose des recommandations pour ajuster le programme de sensibilisation.

Les catégories d'utilisateurs de l'information ciblées par le programme de sensibilisation sont précisées. Le tableau suivant présente le besoin de l'organisation en matière de sécurité de l'information pour chacune de ces catégories et les moyens de sensibilisation afférents.

Tableau 2 : Utilisateurs ciblés par le programme de sensibilisation

Catégorie d'utilisateur	Besoins	Moyens
Gestionnaires	Connaissance des risques, des menaces et des situations de vulnérabilité auxquels l'organisation est exposée; Connaissance des exigences légales en matière de sécurité de l'information; Connaissance des mesures de sécurité en place.	Site Web; Séance de sensibilisation (en personne); Capsules vidéo de sensibilisation; Dépliants, affiches, etc.
Spécialistes en TI	Connaissance des risques, des menaces et des situations de vulnérabilité propres aux technologies de l'information;	Site Web; Séance de sensibilisation (en personne);

	Connaissance des procédures technologiques de sécurisation de l'information (p. ex. : chiffrement).	Capsules vidéo de sensibilisation; Apprentissage en ligne; Guides de bonnes pratiques; Dépliants, affiches, etc.
Spécialistes en sécurité de l'information	Connaissance de l'évolution des menaces pouvant porter atteinte à la disponibilité, à l'intégrité et à la confidentialité de l'information; Connaissance générale et particulière relative aux bonnes pratiques en matière de sécurité de l'information.	Site Web; Séance de sensibilisation (en personne); Capsules vidéo de sensibilisation; Apprentissage en ligne; Guides de bonnes pratiques; Dépliants, affiches, etc.
Autres employés	Connaissance générale des bonnes pratiques en matière de sécurité de l'information.	Site Web; Séance de sensibilisation (en personne); Capsules vidéo de sensibilisation; Apprentissage en ligne; Dépliants, affiches, etc.

5.2 Étape 2 - Détermination des moyens de sensibilisation

L'analyse du contexte organisationnel et des besoins en matière de sensibilisation a mené à la sélection des moyens de sensibilisation suivants :

Tableau 3 : Activités et moyens de sensibilisation

No	Moyen de sensibilisation	Description
1	Séance de sensibilisation générale	Présentation des risques, des menaces et des situations de vulnérabilité auxquels le personnel est exposé quotidiennement. Cette séance décrit les bonnes pratiques à adopter et les comportements à proscrire. Une séance de 1 h 30 à 2 h par groupe de 30 personnes est recommandée.
2	Séance de sensibilisation technique	Présentation des risques, des menaces et des situations de vulnérabilité propres aux applications informatiques. Cette séance présente les actions à faire pour prévenir les risques ainsi que les procédures à suivre en cas d'incident. Une séance de 1 h 30 à 2 h par groupe de 30 personnes est recommandée.

3	Séance de sensibilisation pour gestionnaires	Présentation des risques, des menaces et des situations de vulnérabilité auxquels l'organisation est exposée. Cette présentation a pour objectif de sensibiliser les gestionnaires aux mesures que doivent prendre les employés et les partenaires pour assurer la sécurité de l'information. Une séance de 1 h 30 à 2 h regroupant les gestionnaires est recommandée.
4	Site Web ou intranet	Le site officiel de l'organisation ou son intranet peuvent être utilisés pour publier : les nouvelles en matière de sécurité de l'information; la politique et la directive en matière de sécurité de l'information dans l'organisation; les guides de bonnes pratiques; les capsules (textes ou vidéos) de sensibilisation.
5	Capsules vidéo de sensibilisation	Courtes séquences vidéo portant sur des mises en situation fictives mettant en jeu la sécurité de l'information. Ces capsules sont publiées sur le site Web de l'organisation et elles ont pour objectif de conscientiser le personnel aux conséquences possibles de leurs actions et aux précautions à prendre.
6	Dépliants, affiches, etc.	Les dépliants sont utilisés comme aide-mémoire. On y trouve notamment : les bonnes pratiques à adopter au quotidien; la procédure à suivre en cas d'incident; quelques énoncés de la politique de sécurité de l'organisation; etc. Les affiches sont utilisées pour rappeler les bonnes pratiques à adopter. Elles sont accompagnées d'un message ou d'un slogan original, court et évocateur.
7	Apprentissage en ligne	Sensibilisation en ligne à l'aide de moyens interactifs de promotion des pratiques sécuritaires à adopter au quotidien. Cet apprentissage se termine par l'application d'un questionnaire général sur les notions apprises. Note : L'apprentissage en ligne est accessible en tout temps à partir du site officiel de l'organisation. L'utilisateur peut suspendre sa progression à n'importe quel moment et la reprendre au moment voulu.
8	Guides de bonnes pratiques en sécurité de l'information	Guides expliquant les principaux concepts en matière de sécurité de l'information. Ces guides sont publiés sur l'intranet de l'organisation et ils ont pour objectif de conscientiser le personnel aux bonnes pratiques et aux comportements à adopter pour assurer la protection de l'information.

5.3 Étape 3 - Établissement du calendrier de sensibilisation

Le calendrier des activités est divisé en deux phases. La première, exécutée en début d'année, vise à sensibiliser assez rapidement l'ensemble du personnel. Après une première évaluation du programme de sensibilisation, réalisée au mois de juin, des ajustements à son contenu pourront être faits.

La deuxième phase, exécutée à l'automne, permet de mettre à jour les connaissances assimilées et de sensibiliser d'éventuels nouveaux employés.

Chacune de ces phases fera l'objet d'une évaluation afin que les ajustements nécessaires soient apportés au programme de sensibilisation.

Tableau 4 : Planification des activités de sensibilisation

No	Activité	Date Début	Date Fin	Clientèle cible
	Phase 1	1er janvier	30 juin	-
1	Publication de nouvelles et de bonnes pratiques en matière de sécurité de l'information sur le site Web de l'organisation	1er janvier	31 décembre	Tous les employés
2	Séance de sensibilisation pour gestionnaires	30 janvier	30 janvier	Gestionnaires
3	Séance de sensibilisation pour spécialistes en TI	6 février	6 février	Spécialites en TI
4	Séance de sensibilisation générale 1	9 février	9 février	Autres employés
5	Séance de sensibilisation générale 2	11 février	11 février	Autres employés
6	Séance de sensibilisation générale 3	13 février	13 février	Autres employés
7	Déploiement de la plateforme d'apprentissage en ligne	16 février	16 février	Spécialistes en TI et autres employés
8	Évaluation du programme de sensibilisation	30 mai	12 juin	-
9	Ajustement du programme de sensibilisation	15 juin	30 juin	-
	Phase 2	1er septembre	23 décembre	-
10	Séance de sensibilisation pour gestionnaires	1er septembre	1er septembre	Gestionnaires
11	Séance de sensibilisation pour spécialistes en TI	8 septembre	8 septembre	Spécialistes en TI
12	Séance de sensibilisation générale 4	14 septembre	14 septembre	Autres employés
13	Séance de sensibilisation générale 5	16 septembre	16 septembre	Autres employés
14	Séance de sensibilisation générale 6	18 septembre	18 septembre	Autres employés

15	Évaluation du programme de sensibilisation	20 novembre	4 décembre	-
16	Ajustement du programme de sensibilisation	9 décembre	23 décembre	-

5.4 Étape 4 - Évaluation et amélioration des activités de sensibilisation

L'évaluation des activités de sensibilisation vise principalement à s'assurer de l'efficacité du programme déployé. Deux évaluations sont planifiées. La première permettra de vérifier si le programme de sensibilisation convient aux employés. Le contenu du programme ainsi que l'intérêt du personnel sont évalués.

À la suite d'un ajustement du programme de sensibilisation, la deuxième évaluation permettra de vérifier l'évolution du comportement de l'ensemble du personnel après une année de sensibilisation.

Les évaluations seront faites notamment par :

- ✓ un rapport mesurant le niveau d'adhésion des employés :
  - taux de participation du personnel aux séances de sensibilisation;
  - niveau de satisfaction par rapport au contenu et à la durée des séances de sensibilisation;
  - taux de participation du personnel à l'apprentissage en ligne;
  - niveau de satisfaction par rapport au contenu et à la durée de l'apprentissage en ligne;
- ✓ un rapport sur l'évolution des comportements des employés (statistiques, tendances observées, accidents, erreurs, actes malveillants, demandes d'assistance ou d'information);
- ✓ des entrevues sur un échantillon aléatoire d'employés pour évaluer leur comportement au quotidien et leur connaissance des bonnes pratiques en matière de sécurité de l'information.

ANNEXE I Cadre legal, administratif et normatif

L'élaboration d'un programme de sensibilisation s'appuie sur des lois, des directives, des pratiques gouvernementales, des normes internationales et des standards de l'industrie. Les principaux éléments constitutifs de ce cadre sont :

- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);
- ✓ la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1);
- ✓ la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ la Directive sur la sécurité de l'information gouvernementale;
- ✓ le cadre gouvernemental de gestion de la sécurité de l'information;
- ✓ le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- ✓ les pratiques gouvernementales en matière de sécurité de l'information;
- ✓ les politiques et directives relatives à la sécurité de l'information propres à chaque organisme;
- ✓ les lois sectorielles régissant la mission de chaque organisme;
- ✓ la norme internationale ISO/IEC 27001.

ANNEXE II Références

Sophie Malavoy (dir.), Suzanne Grenier et Sylvie Bérard, Guide pratique de communication scientifique – Comment captiver son auditoire, Montréal, Acfas, 2002, 47 p.

Brigadoon Software Inc. BSI Computer Theft Survey Results 2003, États-Unis, 2003, 27 p.

Mark Wilson et Joan Hash, Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50, octobre 2003, 70 p.

ANNEXE III Mises en situation

Le présent guide est accompagné de 13 capsules vidéo portant sur les 15 mises en situation suivantes :

- ✓ la navigation Internet (deux mises en situation);
- ✓ le piratage psychologique (une mise en situation);
- ✓ les assistants numériques personnels (une mise en situation);
- ✓ la protection contre les virus (deux mises en situation);
- ✓ les copies de sécurité (une mise en situation);
- ✓ les courriels, polluriels et fichiers joints (deux mises en situation);
- ✓ la gestion et l'usage des mots de passe (trois mises en situation);
- ✓ l'usage personnel des ressources de l'organisation (une mise en situation);
- ✓ la réponse aux incidents (une mise en situation);
- ✓ la sécurité des ordinateurs portables (une mise en situation).

D'un point de vue scénographique, les capsules vidéo présentent un univers permettant de centrer l'action et le contenu sur l'utilisateur et son poste de travail. Ces capsules mettent en scène des situations comportant des risques sur le plan de la sécurité et montrent les comportements à éviter.

Les mises en situation sont d'intérêt général et conviennent à tous les organismes publics. Leur structure est la suivante :

- ✓ objectif et importance du sujet;
- ✓ description du ou des scénarios;
- ✓ principales conséquences;
- ✓ précautions à prendre;
- ✓ autres sujets de discussion proposés (questions pour lancer la discussion ou pour alimenter la réflexion à la suite de la présentation de la mise en situation).

Navigation Internet

Objectif

Internet est un outil puissant, utilisé par près de 30 % de la population mondiale[1]. Son usage comporte cependant plusieurs risques.

Une navigation adéquate sur Internet permet ainsi :

- ✓ de limiter certains problèmes de sécurité (p. ex. : divulgation d'information confidentielle, vol d'identité, installation de virus informatiques, etc.);
- ✓ d'assurer le respect des politiques ou des directives en vigueur;
- ✓ de s'assurer que l'utilisation des ressources informatiques est reliée au travail à accomplir.

L'objectif des mises en situation suivantes est d'illustrer le type de navigation permise comparativement à celle qui est prohibée.

Scénario 1a - Le concours[2]

C'est l'heure du dîner et Michelle décide de naviguer sur Internet. Elle désire suivre les aléas du dernier concours de chanson. Vincent lui dit qu'il préfère s'instruire avec Internet et magasiner un peu. Justement, il cherchait un cadeau (un calendrier) pour sa sœur et, tout en magasinant, il est tombé (par l'intermédiaire d'une fenêtre contextuelle) sur des choses plutôt surprenantes… Il s'empresse de montrer le tout à sa collègue en disant que cette fenêtre est apparue d'elle-même. Lorsqu'il la ferme, une autre s'ouvre et il s'agit d'un concours. Vincent demande alors à Michelle si elle veut y participer. Elle accepte et ils saisissent les renseignements demandés pour s'y inscrire (nom, prénom, courriel, etc.). Une fois la saisie terminée, Michelle doit choisir le prix qu'elle réclamera si elle gagne (un voyage, une moto, etc.). Cependant, si elle clique sur un de ces liens, vers où sera-t-elle redirigée?

Scénario 1b - La bande passante concours[3]

Michelle reçoit un courriel de Vincent qui lui indique un lien à suivre contenant une vidéo résumant en 15 minutes l'épopée de son chanteur préféré. Elle clique donc sur le lien et écoute très attentivement la vidéo. Vincent travaille à la saisie d'information dans un système de gestion interne et il observe un retard du temps de réponse. Il appelle alors les services informatiques qui, en analysant les journaux de connexion sur Internet, constatent qu'un poste à l'étage utilise une bonne partie de la bande passante. Vincent fait alors immédiatement le lien avec la vidéo que Michelle regarde.

Conséquences

- ✓ Le visionnement, le téléchargement, la copie, le partage ou l'expédition de fichiers ayant un contenu non autorisé peuvent contrevenir à certaines politiques;
- ✓ La divulgation d'information (p. ex. : donner l'adresse de courriel du bureau lors d'une inscription non reliée au travail);
- ✓ L'augmentation du nombre des polluriels causée par la divulgation d'une adresse de courriel à divers endroits inappropriés;

---

1 Référence : http://www.planetoscope.com/developpement-durable/Internet-
2 Voir la vidéo « 1a - Navigation sur Internet (Le concours).mpg ».
3 Voir la vidéo « 1b - Navigation sur Internet (La bande passante).mpg ».

- ✓ En cliquant sur des liens Internet douteux, on s'expose à divers risques (virus informatique, fraude, etc.);
- ✓ L'occupation des ressources (p. ex. : utilisation de la bande passante en visualisant une vidéo ou en écoutant la radio en provenance d'un serveur externe).

Mise en garde : surveillance et responsabilisation

- ✓ Le respect de la notion de vie privée;
- ✓ La surveillance se justifie par la présomption raisonnable et suffisamment fondée qu'un comportement fautif ou illégal se produit ou se produira;
- ✓ Le moyen de surveillance utilisé permet de constater l'acte reproché ou anticipé;
- ✓ Le moyen de surveillance utilisé doit être le moins intrusif possible.

Précautions

- ✓ S'assurer que les dernières mises à jour ont été faites sur le navigateur;
- ✓ Ne pas cliquer sur des liens Internet douteux dans un courriel ou dans un polluriel.
- ✓ Ne pas accéder à des sites Web inappropriés. Certains sites peuvent attaquer le système en y installant un code malicieux simplement en y accédant;
- ✓ N'utiliser que les moyens mis en place par l'organisation pour transmettre de l'information sensible;
- ✓ Lors de l'utilisation d'Internet, être conscient :
  - qu'une fois déposée sur Internet, l'information est indépendante de la volonté de son détenteur;
  - que certains sites peuvent colliger de l'information sur l'utilisateur, à son insu, et la communiquer à un tiers;
  - que certains renseignements peuvent être conservés pendant des années;
  - que la politique de sécurité doit être lue et comprise par le personnel concerné.

Autres sujets de discussion proposés

- ✓ Votre organisation dispose-t-elle d'une directive sur l'usage d'Internet?
- ✓ Surveillez-vous l'activité de votre réseau (accès Internet, bande passante)? Est-ce que les utilisateurs sont informés de ces pratiques?
- ✓ Avez-vous un exemple concret d'un incident causé par une navigation inadéquate sur Internet?

Piratage psychologique[4] (abus de confiance)

Objectif

Démontrer comment le piratage psychologique peut se manifester. Celui-ci consiste en l'acquisition d'information sensible ou de privilèges d'accès inappropriés par un étranger qui crée une fausse relation de confiance. Cette technique exploite les particularités du comportement humain qui s'apparentent généralement à l'altruisme (désir d'aider les autres), à la confiance en autrui et à l'évitement des problèmes.

Lorsque la fraude psychologique est réalisée en personne ou par téléphone, les actions suivantes peuvent être observées :

- ✓ la recherche préalable d'information pertinente sur la victime (p. ex. : numéros de téléphone, nom, prénom, fonction, loisirs, etc.);
- ✓ la personnification (p. ex. : prendre l'identité d'une personne importante, d'un employé du soutien technique, etc.);
- ✓ la déstabilisation psychologique (p. ex. : inventer un problème fictif, mettre la victime dans une situation d'urgence, etc.);
- ✓ le faux soutien technique;
- ✓ la fouille du bureau et des poubelles en l'absence de la victime.

Lorsque la fraude psychologique est réalisée par ordinateur, elle peut prendre plusieurs formes :

- ✓ le courriel qui incite l'utilisateur à cliquer sur un lien Internet (p. ex. : faux site bancaire) ou à télécharger un logiciel (p. ex. : faux antivirus);
- ✓ les programmes cachés dans un fichier joint à un courriel en apparence crédible (p. ex. : virus, logiciel espion, etc.);
- ✓ le polluriel (p. ex. : fausses annonces ou publicités);
- ✓ l'utilisation des réseaux de discussion (réseaux sociaux, forums, etc.) et des messageries instantanées pour soutirer des renseignements confidentiels à la victime;
- ✓ les sites Web qui offrent des promotions alléchantes.

Scénario 2 - Le faux technicien[5]

Un technicien arrive au bureau d'un utilisateur et lui dit qu'il vérifie le réseau et qu'il cherche un poste qui aurait un problème. Il lui explique qu'il est nouveau et qu'il a été envoyé sur place pour faire la vérification du matériel informatique. Après quelques manipulations, il demande à l'utilisateur de se connecter au réseau. Il observe bien le mot de passe saisi par l'utilisateur. Après quelques soi-disant vérifications, il conclut que ce poste de travail cause le problème qu'il cherche à résoudre et qu'il doit partir avec l'équipement pour le réparer. L'utilisateur ne reverra jamais son ordinateur…

Conséquences

- ✓ Le vol de matériel et d'information;

---

4 Piratage psychologique ou fraude psychologique : « Tromperie qui résulte d'échanges entre individus afin d'extorquer des informations dans le but de pénétrer frauduleusement un système ». La désignation ingénierie sociale constitue un calque de l'anglais. Source : Office québécois de la langue française.

5 Voir la vidéo « 2 – Piratage psychologique (Le faux technicien).mpg ».

- ✓ L'accès non autorisé à de l'information sensible;
- ✓ La modification ou la destruction de l'information;
- ✓ La divulgation d'information confidentielle (p. ex. : nom d'utilisateur, mot de passe, etc.) et perte de confidentialité;
- ✓ L'escalade de privilèges (par le pirate en possession de l'équipement volé);
- ✓ La perte de productivité attribuable à la non-disponibilité de l'équipement ou de l'information;
- ✓ L'installation de virus (p. ex. : fichier joint à un courriel);
- ✓ L'installation de portes dérobées (c.-à-d. cheval de Troie) permettant un accès à distance non autorisé au poste de travail;
- ✓ L'utilisation des ressources du système à l'insu de l'utilisateur à la suite de l'installation d'un virus.

Précautions

- ✓ Lorsque la fraude psychologique est réalisée en personne ou par téléphone, réagir en demandant :
  - l'orthographe correcte du nom de l'interlocuteur;
  - un numéro pour pouvoir le rappeler ultérieurement;
  - les raisons pour lesquelles l'interlocuteur a besoin de l'information demandée;
  - qui a autorisé la demande.
- ✓ Également :
  - vérifier l'identité de la personne et l'authenticité de sa mission auprès de sa direction;
  - aviser le responsable de la sécurité de tout comportement inhabituel observé.
- ✓ Lorsque la fraude psychologique est réalisée par ordinateur :
  - ne pas ouvrir un courriel ou un fichier joint douteux;
  - si le message reçu semble trop beau pour être vrai, c'est sans doute le cas. Supprimer ce message immédiatement;
  - utiliser un mécanisme sécuritaire de transmission des données sensibles (p. ex. : le chiffrement);
  - s'assurer que les données sont stockées dans des endroits sécurisés (p. ex. : serveur interne de l'organisation).

Autres sujets de discussion proposés

- ✓ Est-ce que vos techniciens font bien la preuve de leur identité lorsqu'ils font du soutien informatique sur place?
- ✓ Attention, un pirate cherche dans votre organisation une personne ou un groupe de personnes chez qui il peut déceler une faiblesse. Savez-vous quel groupe de personnel est à risque (p. ex. : personnel du soutien technique)?
- ✓ Saviez-vous que les trois types d'attaques les plus courants en piratage psychologique s'appuient sur l'ego d'une personne, sur le fait d'attirer sa sympathie et sur l'intimidation?

- ✓ Avez-vous un exemple concret d'un incident causé par la fraude psychologique?
- ✓ La clé reste l'éducation du personnel, car il s'agit souvent du maillon le plus faible, et donc celui exploité par les pirates.

Assistant numérique personnel

Objectif

Prendre conscience de la croissance de l'utilisation des assistants numériques personnels et de la multiplication des dangers associés. Selon une enquête réalisée par le CEFRIO[6] en 2013, plus de la moitié des adultes au Québec possèdent un téléphone intelligent ou une tablette numérique (52 %[7]), une augmentation de 15,8 % par rapport à 2012.

Peu de gens prennent l'habitude de chiffrer leurs données ou d'utiliser la fonction de verrouillage par mot de passe. De plus, étant donné leur petite taille, les assistants numériques personnels peuvent facilement être perdus ou volés.

Scénario 3 – Communications sans fil[8]

Deux utilisateurs veulent échanger des numéros de téléphone importants, soit ceux des membres d'un groupe de travail dans un projet particulier. Leur nouvel assistant numérique personnel est équipé d'une technologie de communication sans fil (ex. : Bluetooth). Il est alors possible pour eux d'échanger de l'information par cette technologie.

Le rayonnement du Bluetooth est d'environ 30 mètres (100 pieds). Malheureusement, cette technologie n'est pas infaillible et comporte des points vulnérables. Une tierce personne non loin de là peut capturer l'information échangée entre ces deux personnes si elle possède les applications et le matériel nécessaires.

Conséquences

- ✓ Les mêmes conséquences que celles liées à la navigation sur Internet;
- ✓ La divulgation d'information par la technologie de communication sans fil (p. ex. : Bluetooth, Wi-Fi, NFC[9]);
- ✓ La modification ou la destruction d'information;
- ✓ L'accès non autorisé à de l'information sensible;
- ✓ En cas de vol :
  - la divulgation d'information sensible, la perte de confidentialité;
  - la perte de productivité en raison de la non-disponibilité de l'équipement ou de l'information;
  - la perte financière.

---

6 CEFRIO : Centre facilitant la recherche et l'innovation dans les organisations, à l'aide des technologies de l'information et de la communication (TIC).

7 Référence : NETendances 2013, volume 4, numéro 7 [http://www.cefrio.qc.ca/media/uploader/2013-12-11_mobilit_HR.pdf.]

8 Voir la vidéo « 3 – Assistant numérique personnel (Communication sans fil).mpg ».

9 NFC : Near field communication.

Précautions

- ✓ Désactiver les technologies de communication sans fil (p. ex. : Bluetooth, Wi-Fi, NFC), à moins qu'elles ne soient absolument nécessaires;
- ✓ Garder l'assistant numérique personnel sous surveillance;
- ✓ Toujours verrouiller l'assistant numérique personnel (p. ex. : mot de passe avec chiffres et lettres);
- ✓ Utiliser un mécanisme de chiffrement lors de la transmission de données critiques;
- ✓ Prendre régulièrement des copies de sécurité;
- ✓ Ne pas installer d'applications non reconnues ou d'apparence douteuse.

Autres sujets de discussion proposés

- ✓ Désactivez-vous les mécanismes de communication sans fil sur les assistants numériques personnels?
- ✓ Protégez-vous les cartes mémoire utilisées dans les assistants numériques personnels?
- ✓ Avez-vous un exemple d'incident lié à l'utilisation d'un assistant numérique personnel dans votre organisation?

Protection contre les virus

Objectif

Décrire comment se propagent les virus informatiques et indiquer quelques actions à accomplir pour s'en protéger. Les virus ont généralement les caractéristiques suivantes :

- ✓ Ce sont des programmes malveillants autoréplicatifs conçus pour se propager à plusieurs ordinateurs;
- ✓ Ils peuvent se répandre dès qu'il y a partage d'un fichier entre des ordinateurs, soit par pièce jointe à un courriel, par le réseau, par la mémoire amovible, etc.;
- ✓ Ils infectent principalement les programmes légitimes (exécutables) et les fichiers (données);
- ✓ Ils peuvent ralentir le système, détériorer certaines fonctions ou détruire complètement toutes les données de l'ordinateur;
- ✓ Lorsqu'un programme ou un fichier infecté est lancé, les virus sont activés et peuvent se répandre dans d'autres programmes ou fichiers.

Scénario 4a – Mémoire amovible[10]

Un utilisateur entre dans le bureau d'un de ses collègues et lui montre sa nouvelle clé USB. Il décide de l'essayer et il la connecte au port USB de l'ordinateur de son collègue. Le contenu de la clé apparaît automatiquement. L'utilisateur dit : « Regarde le petit jeu que j'ai reçu hier ». Il l'exécute et… un virus s'installe à son insu, car l'antivirus de l'ordinateur n'est pas à jour.

[10] Voir la vidéo « 4a – Protection contre les virus (Mémoire amovible).mpg ».

Scénario 4b – Le fichier joint[11]

Un utilisateur d'une grande organisation arrive au bureau et démarre son ordinateur. Il ouvre son logiciel de gestion des courriels et voit un nouveau message marqué comme étant hautement prioritaire venant de support@mon.organisation.com et intitulé « Avertissement sur votre compte de courriels ». Sans hésiter, il l'ouvre immédiatement. Le courriel se lit comme suit :

Cher employé du serveur de courriels @mon.organisation.com, votre compte de courriels sera désactivé d'ici les deux prochains jours pour utilisation non conforme à notre politique. Toutefois, si vous désirez continuer à utiliser votre compte, vous pouvez le réactiver. S.v.p., utilisez le fichier joint à ce courriel. Pour ouvrir le fichier compressé en format .zip ci-joint, utilisez le mot de passe 83045.

Notre utilisateur commence à se sentir mal. « Mais qu'est-ce que j'ai fait de mal avec mon courriel? » Il pense aux courriels contenant des blagues qu'il envoie tous les jours, aux courriels sur les échanges des paris sportifs, etc. Rongé par les remords, il ouvre le fichier joint et entre le mot de passe. Il exécute ensuite le programme pour réactiver son compte. Voilà son ordinateur infecté par un nouveau virus.

Conséquences

- ✓ L'installation ou l'utilisation de programmes non autorisés est dangereuse, car ceux-ci peuvent contenir des virus;
- ✓ Mis à part les effets usuels (se propager ou modifier ou détruire de l'information, etc.), les virus installés sur le poste peuvent :
  - utiliser les ressources de l'ordinateur pour envoyer des polluriels;
  - installer une porte dérobée qui permettra au pirate de se connecter à distance et en tout temps à l'ordinateur et de l'utiliser à d'autres fins (p. ex. : balayage d'un réseau pour trouver d'autres victimes);
  - effectuer une attaque de déni de service sur un site en particulier (indisponibilité de l'information et perte de productivité);
  - recueillir les mots de passe en installant un enregistreur de frappe (keylogger);
  - recueillir certains renseignements confidentiels contenus dans l'ordinateur (p. ex. : renseignements personnels, documents de travail, etc.).

Précautions

- ✓ S'assurer que le logiciel antivirus est à jour;
- ✓ S'assurer que le système d'exploitation est à jour;
- ✓ Effectuer un balayage complet des disques et des mémoires portables (clé USB, carte mémoire SD/micro SD, disque dur externe, etc.) à l'aide de l'antivirus avant de les utiliser;
- ✓ Être vigilant à l'égard du fonctionnement de son ordinateur (comportement inhabituel, ralentissement, etc.) et avertir son responsable en cas d'anomalie.

Autres sujets de discussion proposés

- ✓ Balayez-vous les mémoires portables avec un logiciel antivirus lorsqu'elles sont connectées à l'ordinateur?

---

[11] Voir la vidéo « 4b – Protection contre les virus (Le fichier joint).mpg ».

- ✓ Avez-vous un exemple concret d'un incident causé par un virus?
- ✓ L'utilisation de logiciels à des fins personnelles est-elle contrôlée efficacement? (p. ex. : jeux informatiques, systèmes de messagerie instantanée, etc.)
- ✓ Combien de virus sont bloqués quotidiennement par votre infrastructure de sécurité?
- ✓ Quelles sont les causes d'infection les plus fréquentes (p. ex. : les portables branchés au réseau, le courriel, etc.)?
- ✓ Quelle est la procédure à utiliser pour signaler un virus?

Copie de sécurité

Objectif

Démontrer l'importance des copies de sécurité. La prise d'une copie de sécurité consiste à dupliquer les données contenues dans un système informatique de manière à pouvoir les récupérer en tout temps. Cette pratique de sécurité permet d'éviter des conséquences fâcheuses, notamment en cas de vol, de bris de matériel, de corruption des données, d'effacement accidentel des fichiers, etc.

Scénario 5 – Le bris du portable[12]

Un utilisateur apporte toujours son ordinateur portable avec lui dans ses déplacements et le soir à la maison. Après quelques mois d'utilisation, il entend un petit bruit lorsqu'il le démarre. Le bruit se produit aussi parfois en cas d'accès intensif au disque dur. Un soir, il se dit qu'il serait temps de prendre une copie de sécurité de ses fichiers... déjà qu'il ne se souvient pas de la date à laquelle remonte sa dernière prise de copie. Il décide cependant de terminer son travail avant de prendre sa copie de sécurité pour ne pas avoir à la refaire plus d'une fois. Quelques heures plus tard, soulagé d'avoir terminé son travail, il se souvient de la copie de sécurité. Malheureusement, il est trop tard : au moment de sauvegarder son document, l'ordinateur ne fonctionne plus. Tout se fige et l'écran affiche une erreur de lecture du disque… N'ayant aucune copie de sécurité, notre utilisateur doit reprendre la totalité de son travail de plusieurs semaines.

Conséquences

- ✓ L'effacement par erreur d'un fichier peut nécessiter la reprise totale du travail;
- ✓ Une panne du réseau local ou du disque dur peut survenir sans avertissement et neutraliser l'utilisation pendant plusieurs jours;
- ✓ L'infection du système par un virus peut corrompre ou détruire des fichiers dont la reconstruction nécessitera des jours, voire des mois de travail;
- ✓ Sans une copie de sécurité, le vol d'un équipement entraîne une perte d'information sans possibilité de récupération des données.

Précautions

- ✓ S'assurer qu'une copie de sécurité des données est faite régulièrement dans un délai raisonnable. Les données corrompues ou perdues peuvent ainsi être récupérées;
- ✓ S'assurer d'avoir le nombre de copies de sécurité nécessaires. Un trop grand nombre de copies rendrait le processus de gestion des fichiers trop lourd et inefficace;

[12] Voir la vidéo « 5 – La copie de sécurité (Le bris du portable) ».

- ✓ Stocker les données sur le disque du réseau interne de l'organisation, laquelle est responsable d'en assurer la sauvegarde.

Autres sujets de discussion proposés

- ✓ Existe-t-il une procédure indiquant aux utilisateurs comment faire une copie de sécurité de leurs répertoires essentiels?
- ✓ Existe-t-il une procédure automatique de copie de sécurité pour les ordinateurs connectés au réseau de l'organisation?
- ✓ Les sauvegardes sont-elles effectuées régulièrement selon les consignes?
- ✓ Où les copies sont-elles généralement conservées? Et dans quelles conditions?
- ✓ Avez-vous déjà essayé de récupérer des fichiers à partir d'une copie de sécurité?
- ✓ Qui est responsable de la prise des copies?
- ✓ Quels sont les événements les plus fréquents qui nécessitent le recours à une copie? (p. ex. : panne de disque dur, panne de réseau, etc.)
- ✓ Avez-vous un exemple concret d'une perte d'information liée à l'absence de la prise de copies de sécurité?

Courriel, polluriel et fichier joint

Objectif

L'un des outils les plus populaires liés à Internet est sans doute le courriel. L'objectif des mises en situation de la présente section est de démontrer toute la vigilance et le discernement dont il faut faire preuve à l'égard du traitement des courriels, notamment en ce qui concerne les polluriels. À titre indicatif, le polluriel est un message inutile, souvent provocateur et sans rapport avec le sujet de discussion, qui est diffusé massivement à de nombreuses adresses de courriel, causant ainsi une véritable pollution des réseaux.

Entrée en vigueur le 1er juillet 2014, la Loi canadienne anti-pourriel a pour objectif de freiner la croissance de cette pratique au Canada. À cet effet, la Loi énonce de nouvelles exigences applicables à l'envoi de messages électroniques commerciaux[13] à une adresse électronique (courriel ou message texte), dont les suivantes :

- ✓ Il est interdit d'envoyer des messages électroniques commerciaux sans le consentement du destinataire;
- ✓ L'identification de l'organisation qui envoie les messages commerciaux est obligatoire;
- ✓ Un mécanisme d'exclusion (de désinscription) doit être inclus dans les messages commerciaux.

Scénario 6a – Le polluriel[14]

Un utilisateur entre au travail le matin et ouvre son outil de gestion des courriels. Plus de 40 messages l'attendent. De ce nombre, environ 25 à 30 messages sont des polluriels. Les autres

---

13 Un message électronique commercial peut être une offre d'achat ou de vente d'un bien ou service, une annonce, une promotion, une offre d'investissement, etc.

14 Voir la vidéo « 6a – Courriels – Le polluriel.mpg ».

viennent de personnes connues de l'utilisateur. Un courriel sur les prêts hypothécaires à très bas taux attire son attention. Il l'ouvre et y trouve un lien vers un site Web. Doit-il cliquer sur ce lien?

Un autre de ces courriels attire aussi son attention. Il vient d'une source légitime (une personne qu'il connaît). Le message est plutôt étrange et comprend une invitation à ouvrir le fichier joint. Ce fichier se nomme « proposition_mandat.doc.vbs ». Que doit faire l'utilisateur? Il ne devrait pas ouvrir ce courriel s'il a l'air suspect.

Scénario 6b – Le colis[15]

Le réseau Internet est mondial et est ouvert à tous. La communication d'information confidentielle pourrait donc être interceptée, et son contenu modifié ou utilisé à tort (p. ex. : divulgation dans les journaux) par un internaute mal intentionné et suffisamment habile.

Une personne envoie un document sensible par la poste traditionnelle (l'enveloppe est bien collée et porte la mention « Confidentiel »). Le destinataire l'appelle et lui demande si, entre-temps, elle peut lui envoyer l'information à son adresse de courriel à la maison. Elle envoie aussitôt ce courriel sensible…

L'information confidentielle transmise sur Internet doit faire l'objet d'un chiffrement pour être protégée. Cela veut dire que l'expéditeur, après avoir écrit son texte en clair, doit le rendre illisible en utilisant un mécanisme de chiffrement, puis l'envoyer à son destinataire. Le destinataire, qui a déjà la clé de déchiffrement, pourra utiliser le même mécanisme pour rendre à nouveau le texte lisible.

Conséquences

- ✓ La gestion des polluriels constitue une perte importante de temps et d'argent pour l'organisation;
- ✓ Les fichiers joints à un courriel sont une voie idéale pour transmettre des virus et autres programmes malveillants à des utilisateurs curieux;
- ✓ Le nom de l'expéditeur d'un courriel peut facilement être forgé (contrefait);
- ✓ Si le fichier joint est un virus, on peut observer les conséquences suivantes :
  - utilisation des ressources du système à l'insu de l'utilisateur;
  - non-disponibilité de l'information (perte de productivité);
  - destruction d'information;
  - accès non autorisé à de l'information sensible;
  - impact financier des mesures de restauration à la suite de la propagation des virus par courriel.

Précautions

- ✓ Supprimer les courriels suspects. Un courriel suspect peut être un courriel :
  - non relié au travail (blague, image, etc.);
  - non attendu ou qui contient un fichier joint non prévu;
  - contenant un fichier joint avec un nom de fichier suspect (*.exe, *.vbs, *.bin, *.com, *.pif, etc.);

[15] Voir la vidéo « 6b – Courriel et polluriel (Le colis).mpg ».

- contenant un lien suspect vers une page Web.

- ✓ Ne pas ouvrir les pièces jointes sans raison valable (oublier la curiosité!);
- ✓ S'assurer que toute pièce jointe d'un courriel est balayée par l'antivirus;
- ✓ Éviter d'utiliser les systèmes de messagerie externes à l'organisation (p. ex. : Gmail, Outlook, Yahoo, etc.);
- ✓ Envoyer un courriel de vérification avant l'envoi d'information sensible;
- ✓ Tenir compte de la confidentialité de l'information et des conséquences associées lors de l'envoi de courriels;
- ✓ Chiffrer les fichiers joints à un courriel pour en assurer la confidentialité et l'intégrité;
- ✓ Utiliser avec précaution les options « Faire suivre », « Répondre à tous » ou une liste de distribution (risque de divulgation non intentionnelle d'information sensible);
- ✓ Même si un courriel est effacé du poste de l'utilisateur, il peut y en avoir plusieurs copies en circulation (p. ex. : serveur, archives, etc.).

Autres sujets de discussion proposés

- ✓ Quel pourcentage de polluriels recevez-vous dans votre organisation?
- ✓ Avez-vous un exemple concret d'un incident lié aux courriels (p. ex. : suivre un lien douteux, ouvrir un fichier joint, etc.)?
- ✓ Votre organisation a-t-elle une directive sur l'utilisation du courriel?
- ✓ Faites-vous la surveillance des courriels? Est-ce que les utilisateurs sont informés de cette pratique?

Gestion et usage du mot de passe

Objectif

Démontrer l'importance à accorder à son mot de passe. Il représente généralement la forme la plus courante d'authentification.

Scénario 7a – Usurpation d'identité[16]

Un utilisateur se présente au bureau de son patron. Il lui demande une information particulière à propos d'un courriel qu'il lui a envoyé. Comme le patron arrive tout juste à son travail, il ouvre son logiciel de courriel et entre son mot de passe : 123456.

L'employé a capté le mot de passe de son patron. Il peut alors usurper son identité (s'il connaît son identifiant), transférer et même supprimer ses courriels à son insu.

Scénario 7b – Les règles[17]

Un utilisateur doit changer son mot de passe aujourd'hui. De nouvelles règles ont été implantées pour le choix des mots de passe :

[16] Voir la vidéo « 7a – Gestion et usage du mot de passe (Usurpation d'identité).mpg ».
[17] Voir la vidéo « 7b et 7c – Gestion et usage du mot de passe (Les règles et le rangement).mpg ».

- ✓ Lorsque l'utilisateur saisit son nouveau mot de passe, le système lui répond qu'il ne peut choisir l'un de ses dix derniers mots de passe;
- ✓ Il saisit donc un autre mot de passe (p. ex. : « bateau »). Le système lui répond que son mot de passe doit avoir au moins huit caractères;
- ✓ Il entre les six caractères de son nom d'utilisateur avec deux chiffres (p. ex. : « martin12 »). Le système lui répond qu'il ne doit pas utiliser son nom d'utilisateur en tout ou en partie dans son mot de passe;
- ✓ Il entre alors un mot de passe de huit caractères (p. ex. « bateau12 »). Le système lui répond que son mot de passe doit contenir au moins trois des quatre éléments suivants :
  - des majuscules (p. ex. : A, B, C …);
  - des minuscules (p. ex. : a, b, c…);
  - des chiffres (p. ex. : 1, 2, 3…);
  - des caractères spéciaux (non alphanumériques) (p. ex. : !, $, %…);
- ✓ Il entre alors « Bateau12 ». Le système accepte le mot de passe;
- ✓ Sans réfléchir, il prend un crayon et écrit son mot de passe sur une note adhésive qu'il colle derrière une photo déposée sur son bureau.

Scénario 7c – Le rangement[18]

Une personne qui fait l'entretien ménager des bureaux raconte comment elle connaît les mots de passe de plusieurs utilisateurs :

« Vous voyez, celui-ci l'inscrit sur une note adhésive sous son clavier. Celui-ci colle la note adhésive carrément sur son écran. Celle-là le place dans son tiroir. Et d'ailleurs, cette personne place la clé de son classeur dans son tiroir, bien à la vue. Et lui, il colle une note adhésive sur la photo de son fils. »

Conséquences

- ✓ Divulgation d'information confidentielle;
- ✓ Usurpation d'identité;
- ✓ Accès non autorisé à de l'information sensible;
- ✓ Vol d'information;
- ✓ Perte ou destruction d'information;
- ✓ Perte de productivité attribuable à la non-disponibilité de l'information;
- ✓ Perte financière.

Précautions

- ✓ Ne pas partager ni divulguer les mots de passe;
- ✓ Changer régulièrement de mot de passe;
- ✓ Ne pas employer le même mot de passe sur plusieurs applications;

---

18 Voir la vidéo « 7b et 7c – Gestion et usage du mot de passe (Les règles et le rangement).mpg ».

- ✓ Sélectionner des mots de passe de qualité (suffisamment complexes et faciles à mémoriser);
- ✓ Changer le mot de passe en cas de doute;
- ✓ Ne jamais écrire un mot de passe sur une note adhésive collée sur l'écran, sous le clavier ou ailleurs;
- ✓ Toujours entrer soi-même le mot de passe, même lorsqu'on reçoit de l'aide technique;
- ✓ Être prudent lors de la saisie d'un mot de passe dans un programme, sur un site Web ou sur un serveur.

Autres sujets de discussion proposés

- ✓ Comment choisir et gérer son mot de passe?
  - Ne jamais choisir un mot du langage courant;
  - Ne jamais choisir comme mot de passe un renseignement personnel évident (p. ex. : son adresse de domicile, sa date de naissance, son numéro de téléphone, le nom d'un proche parent, etc.);
  - Ne jamais choisir un mot de moins de six lettres;
  - Choisir un mot de passe constitué de chiffres et de lettres, de majuscules et de minuscules ou de caractères spéciaux;
  - Peut être mnémonique (c.-à-d. facilement mémorisable), par exemple : G1grosPom.
- ✓ Votre ministère ou organisme a-t-il déjà vécu un problème relié à la divulgation d'un mot de passe?
- ✓ Quelles sont les erreurs les plus fréquentes dans ce domaine (p. ex. : mot de passe affiché, mot de passe trop simple, oubli du mot de passe, etc.)?
- ✓ Vérifiez-vous la force des mots de passe des utilisateurs?

Usage personnel des ressources de l'organisation

Objectif

Démontrer l'attention particulière qu'il faut porter à l'utilisation des ressources de l'organisation, tant à l'intérieur qu'à l'extérieur de celle-ci. À titre indicatif, voici quelques éléments à prendre en considération :

- ✓ L'usage des ressources de l'organisation doit respecter l'éthique et les règles établies par celle-ci;
- ✓ Un usage abusif des ressources de l'organisation peut avoir des conséquences néfastes sur l'ensemble des usagers (p. ex. : ralentissement du réseau, contamination par un virus informatique, etc.);
- ✓ Un usage responsable des ressources de l'organisation permet de réduire les risques d'incidents, notamment d'une atteinte à l'image de cette organisation (p. ex. : installation de logiciels illégaux ou de ceux protégés par une licence).

Scénario 8 – Les fichiers musicaux[19]

Un utilisateur télécharge à la maison des chansons en format MP3 et les grave sur un CD. Le lendemain, il apporte le CD au bureau pour les écouter.

Si les chansons contenaient des virus, ceux-ci pourraient contaminer le poste dès l'ouverture des fichiers. Un pirate informatique pourrait également prendre le contrôle du poste à distance une fois l'ordinateur contaminé;

Lorsque l'utilisateur écoute ses chansons favorites, le logiciel de lecture des fichiers MP3 lui propose de visiter un site consacré à la musique. En arrivant sur ce site, il peut lire différents articles sur la musique et participer au forum de discussion. Il s'inscrit sur le forum et entre son adresse de courriel, mon.adresse@organisation.com. Tout en naviguant dans le forum, il lit un commentaire négatif sur un de ses chanteurs préférés. Mécontent, il décide de répondre au commentaire par la bouche de ses canons, sans prêter attention au fait qu'il utilise l'adresse de son employeur pour laisser ses commentaires personnels…

Conséquences

- ✓ Ralentissement du réseau de l'organisation;
- ✓ Divulgation d'information confidentielle;
- ✓ Installation de programmes malveillants;
- ✓ Accès non autorisé à de l'information sensible (si un virus est installé par mégarde);
- ✓ Perte ou destruction d'information;
- ✓ Vol d'information;
- ✓ Atteinte à la réputation de l'employeur.

Précautions

- ✓ Ne pas dupliquer ni télécharger sans autorisation, à partir d'Internet, du matériel protégé par le droit d'auteur;
- ✓ N'utiliser que les applications agréées par l'administration;
- ✓ Se souvenir qu'Internet n'est pas privé. Une trace de chaque visite d'un site Web est toujours gardée;
- ✓ Pour une meilleure gestion des risques associés à l'utilisation de personnel externe à l'organisation :
  - fournir à chaque personne un poste de travail;
  - limiter les accès réseau aux seuls répertoires associés aux travaux à accomplir;
  - rappeler la politique de sécurité en vigueur et faire signer par chaque personne un engagement de confidentialité.

Autres sujets de discussion proposés

- ✓ Protégez-vous les communications lorsqu'un utilisateur distant se connecte aux infrastructures de l'organisation?

[19] Voir la vidéo « 8 – Usage personnel des ressources de l'organisation (Les fichiers musicaux).mpg ».

- ✓ Avez-vous déjà eu un incident informatique parce qu'un utilisateur a partagé son ordinateur avec un utilisateur externe (famille, ami, collègue)?
- ✓ Est-ce que les utilisateurs peuvent désactiver le pare-feu ou l'antivirus lorsqu'ils utilisent leur ordinateur portable à l'extérieur du bureau? Sont-ils administrateurs de leur poste informatique?
- ✓ Comment vous assurez-vous que l'information demeure confidentielle si une tierce partie (p. ex. famille, ami, collègue) utilise l'ordinateur portable?

Réponse aux incidents

Objectif

Un incident de sécurité de l'information est un événement aux conséquences néfastes, prévisibles ou confirmées qui compromet la disponibilité, l'intégrité ou la confidentialité de l'information. L'objectif de cette section est de sensibiliser les utilisateurs aux différents types d'incidents potentiels et aux réactions à adopter lorsqu'un incident se produit.

On distingue, entre autres, quatre types d'incidents :

- ✓ Accès physique ou logique non autorisé;
- ✓ Infection par code malicieux;
- ✓ Perte, vol ou dégradation d'un équipement informatique, d'un service ou d'un fichier;
- ✓ Divulgation d'information confidentielle.

À titre indicatif, la liste suivante présente quelques symptômes révélateurs d'un incident de sécurité :

- ✓ Le système est hors service;
- ✓ Plusieurs tentatives de connexion ont échoué;
- ✓ La performance du système se dégrade;
- ✓ Des connexions suspectes sont établies;
- ✓ Des fichiers sont modifiés de façon non volontaire, sans l'intervention de l'utilisateur;
- ✓ De nouveaux fichiers douteux apparaissent;
- ✓ La taille d'un fichier change de façon anormale.

Scénario 9 – La bonne décision[20]

Un utilisateur curieux a cliqué sur un courriel douteux durant l'avant-midi. Au cours de l'après-midi, son disque dur semble agité de temps à autre ou, du moins, il fait un bruit plus perceptible que la normale. De plus, la lumière d'accès réseau clignote à une fréquence beaucoup plus élevée. Son ordinateur est plus lent. Plusieurs personnes de l'organisation se plaignent d'avoir reçu plusieurs courriels en provenance de notre utilisateur dans la journée. L'utilisateur fait alors le lien avec le courriel douteux qu'il a ouvert ce matin :

- ✓ Il essaie de régler lui-même son problème;

[20] Voir la vidéo « 9 – Les incidents (La bonne décision).mpg ».

- ✓ Il active l'antivirus, redémarre son poste, discute avec des collègues;
- ✓ Il ne veut pas appeler le soutien technique, car c'est le troisième incident qu'il provoque cette semaine;
- ✓ Il a vu le technicien travailler et sait maintenant comment faire.

Rien à faire, toutes ses tentatives ont échoué. Il décide finalement de rappeler le soutien technique. Il s'agissait en fait d'un nouveau virus qui utilisait les ressources de son poste pour envoyer massivement des polluriels.

Conséquences

Tout dépend de la nature de l'incident, mais on peut penser à la liste suivante :

- ✓ divulgation d'information confidentielle;
- ✓ perte ou destruction d'information;
- ✓ vol d'information;
- ✓ accès non autorisé à de l'information sensible;
- ✓ installation de programmes malveillants;
- ✓ perte de productivité attribuable à la non-disponibilité de l'équipement ou de l'information;
- ✓ perte financière.

Précautions

Marche à suivre en cas d'incident :

- ✓ signaler l'incident aux personnes concernées, conformément au processus de gestion des incidents mis en place par l'organisation;
- ✓ prendre les mesures nécessaires selon la procédure établie;
- ✓ rester discret et ne révéler l'incident qu'aux personnes concernées;
- ✓ éviter de tenter de résoudre l'incident soi-même sans avoir l'expertise requise, au risque de détruire des preuves utiles à l'analyse et à l'enquête post-incident.

Autres sujets de discussion proposés

- ✓ Avez-vous eu récemment un incident informatique dans votre organisation?
- ✓ En cas d'incident, que doit faire l'utilisateur pour ne pas empêcher ou limiter la collecte des preuves?
- ✓ Est-ce que les employés, les consultants et autres tierces parties sont au courant de la procédure de déclaration d'un incident?
- ✓ Avez-vous des statistiques sur les types d'incidents les plus fréquents, le coût estimé pour le rétablissement, leur fréquence, les infrastructures ciblées, etc.?

Sécurité des ordinateurs portables

Objectif

Démontrer l'importance et l'ampleur du phénomène des vols d'ordinateurs portables. D'après une étude menée en 2008 par l'Institut Ponemon pour le compte de DELL, plus de 800 000 ordinateurs sont perdus ou volés chaque année dans les aéroports aux États-Unis et en Europe. Plus de la moitié des professionnels interrogés disposent d'information confidentielle (sur les clients, les consommateurs, les activités de l'entreprise, etc.) dans leurs ordinateurs portables et n'ont pris aucune disposition pour la protéger.

Scénario 10

Il n'y a pas de capsule sur la sécurité des ordinateurs portables, la notion de vol de matériel informatique ayant été couverte dans le scénario 2.

Conséquences

- ✓ Vol de l'ordinateur portable (manque de vigilance);
- ✓ Divulgation d'information (peut-être même dans les médias) – perte de confidentialité si les données n'étaient pas chiffrées;
- ✓ Perte ou destruction d'information;
- ✓ Non-disponibilité de l'information (perte de productivité);
- ✓ Accès non autorisé à de l'information sensible;
- ✓ Perte financière.

Précautions

- ✓ Garder le portable sous surveillance;
- ✓ Attacher le portable, si possible, avec un câble de sécurité;
- ✓ Transporter le portable dans un sac atypique;
- ✓ Éviter les logos et étiquettes trop voyants;
- ✓ Éviter de se connecter aux points d'accès sans fil non sécurisés;
- ✓ Éviter de transmettre de l'information critique dans un réseau public;
- ✓ Verrouiller le portable avec un mot de passe et chiffrer les données;
- ✓ Toujours verrouiller le portable lorsqu'il n'est pas sous surveillance;
- ✓ Désactiver les fonctionnalités de communication sans fil (Wi-Fi ou Bluetooth) lorsqu'elles ne sont pas utilisées;
- ✓ Prendre régulièrement des copies de sécurité.

Autres sujets de discussion proposés

- ✓ Procurez-vous des câbles de sécurité à vos employés qui utilisent des ordinateurs portables?
- ✓ Chiffrez-vous la partie du disque qui contient de l'information sensible?

- ✓ Quelles mesures mettez-vous en place pour le personnel qui fait du télétravail (p. ex. : environnement sécuritaire, protection de la visualisation d'information confidentielle, pare-feu, antivirus, accès à distance sécurisé, etc.)?
- ✓ Avez-vous un exemple concret d'un vol d'ordinateur portable dans votre organisation?

ANNEXE IV Questionnaire sur la séance de sensibilisation

Afin de nous permettre d'améliorer le programme de sensibilisation à la sécurité de l'information, nous vous invitons à prendre quelques minutes pour remplir le questionnaire ci-dessous. Vos commentaires et suggestions sont très importants, car ils nous permettront de mieux répondre à vos besoins et à vos attentes.
Merci d'avance !

Titre de l'activité : _____ Date : _____

Votre nom[21] : _____ Organisation[22] : _____

No	L'activité de sensibilisation	Totalement en désacord	Plutôt en désacord	Plutôt d'accord	Totalement d'accord
1	Le contenu de l'activité correspond à ce qui est annoncé.				
2	Les objectifs de l'activité ont été clairement expliqués au début de la séance.				
3	L'activité de sensibilisation est bien structurée et met en évidence les notions importantes.				
4	Le contenu de cette activité a suscité et maintenu votre intérêt tout au long de la séance.				
5	Le niveau de difficulté de la matière traitée est adéquat. (Sinon, spécifiez : ❒ Trop simple ou ❒ Trop compliquée)				
6	Le présentateur a bien situé le contenu de cette activité par rapport aux autres activités complémentaires.				
7	Les explications du présentateur sont claires.				
8	Les réponses du présentateur aux questions des participants sont				

21. Information facultative
22. Information facultative

	pertinentes et précises.				
9	Le présentateur utilise adéquatement les outils pédagogiques mis à sa disposition (vidéos, présentation, tableau, projecteur, etc.).				
10	Le présentateur sait faire appel à son expérience personnelle par des exemples, exercices ou démonstrations afin de mieux faire comprendre la matière présentée.				
11	Le temps alloué à l'apprentissage des notions présentées est suffisant.				
12	Je suis satisfait de l'activité.				

Donnez brièvement vos commentaires sur l'activité.

Aspects positifs :

Aspects à améliorer :

Autres commentaires :

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique