5 CONSEILS DE SÉCURITÉ INFORMATIQUE
POUR LES PROFESSIONNELS DE LA PAIE

Par Kevin Sokolowski

Les données confidentielles sur la paie et les employés doivent être parmi les renseignements les mieux protégés que l'organisation possède. Comme les technologies s'améliorent et deviennent omniprésentes dans tous les aspects des opérations, l'organisation doit constamment améliorer ses pratiques de sécurité. Les gestionnaires, surtout ceux qui gèrent des renseignements personnels des employés, doivent montrer l'exemple et fixer des normes d'acceptabilité pour encadrer les pratiques de sécurité.

Voici des lignes de conduite simples, mais efficaces, pour incorporer les pratiques de sécurité des renseignements dans votre lieu de travail.

1) FORMATION EN SÉCURITÉ INFORMATIQUE

Le sujet de la sécurité informatique surgit inévitablement lorsque je discute avec des gestionnaires. Il existe une idée fausse largement répandue à propos des meilleurs moyens de défendre l'organisation contre une fuite de données : la sécurité informatique et la cybersécurité évoquent souvent l'image mentale d'un groupe de pirates informatiques qui s'efforcent de forcer la porte de votre infrastructure technologique à partir d'ici ou d'un pays étranger. Bien que ce type d'attaque se produise réellement, ce n'est pas aussi courant qu'on pourrait le croire. À cause de certaines brèches de sécurité qui ont fait les manchettes dernièrement, plusieurs organisations se sont mises à dégager des fonds en continu afin d'ériger un meilleur périmètre de défense. C'est bien d'avoir de bonnes défenses, mais l'organisation ne peut pas se fier uniquement sur elles pour assurer une pleine protection. Même les murs les plus hauts et les plus épais sont inutiles lorsqu'on invite l'ennemi à entrer par la grande porte – parlez-en aux citoyens de Troie.

Voilà pourquoi je suis convaincu que faire suivre une formation en sécurité informatique à tous les employés est l'une des pratiques les plus utiles pour améliorer la sécurité globale de l'organisation. Plusieurs ressources sont disponibles pour vous aider à créer une politique globale sur la sécurité et pour éduquer votre personnel. La formation en sécurité informatique est la plus efficace lorsque les employés comprennent son importance et comment l'appliquer à l'organisation. Lorsque les employés sont formés et à l'affût, les risques de brèche de sécurité technologique et/ou physique diminuent d'autant.

2) GESTION DES MOTS DE PASSE

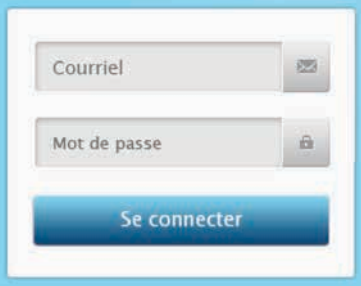
Le mot de passe est l'un des outils les plus connus en sécurité informatique. Même avec les progrès sur le plan des méthodes d'authentification, vous aurez toujours besoin de mots de passe à plusieurs endroits – votre courriel, votre connexion au site de l'Association canadienne de la paie, et ainsi de suite. Mais parce que les mots de passe sont si courants, les gens deviennent négligents. Ne pas se conformer à des normes efficaces en matière de mot de passe pourrait bien mettre en danger les systèmes et les ressources de l'organisation – et les vôtres.

Gardez vos mots de passe confidentiels en tout temps et évitez d'utiliser la fonction « Retenir le mot de passe ». Changez-les souvent et assurez-vous qu'ils soient entièrement nouveaux. N'utilisez pas le même pour plusieurs applications et, à moins qu'elle ne soit chiffrée, n'entreposez pas la liste de vos mots de passe dans votre ordinateur ou votre appareil mobile.

À FAIRE ET À NE PAS FAIRE POUR CRÉER DES MOTS DE PASSE SÉCURITAIRES

[À FAIRE]

+ Utiliser 15 caractères ou plus. Plus il y en a, plus c'est dur à craquer ou à deviner.
+ Utiliser des mots et des chiffres au hasard.
+ Utiliser des majuscules et des minuscules.
+ Utiliser des symboles et des caractères spéciaux.



[À NE PAS FAIRE]

- Utiliser un même caractère pour tout le mot de passe ou moins de cinq caractères uniques.
- Utiliser une variation de votre code d'accès.
- Utiliser des mots, des chiffres ou des renseignements connus et associés à sa personne (p. ex., nom de famille, nom d'un animal domestique, date de naissance, numéro de téléphone ou adresse).
- Utiliser un simple mot (p. ex., motdepasse). Ces mêmes mots dans d'autres langues sont tout aussi risqués.
- Utiliser une suite de lettres ou de chiffres connue (p. ex., 123456 ou qwerty).
- Utiliser des substituts à des mots communs (p. ex., 3=E, 4=A, 1=I, 0=O, m0td3p4553).

[DANS LE CONTEXTE ACTUEL, EN PARTICULIER DANS LA PROFESSION DE LA PAIE, NOUS SOMMES TOUS RESPONSABLES DE BIEN PROTÉGER LES RENSEIGNEMENTS.]

3) OUTILS CONTRE LES MALICIELS

Il existe toute une panoplie de programmes malveillants et de virus, chacun ayant une cible différente. Le meilleur moyen de s'en défendre est d'installer un logiciel anti-maliciels sur votre ordinateur. Étant donné qu'il est largement accepté qu'aucune technologie à elle seule n'assure une protection adéquate contre la totalité des attaques sophistiquées d'aujourd'hui, les experts en sécurité informatique recommandent d'utiliser une approche multiple impliquant plusieurs outils pour protéger vos renseignements, notamment un pare-feu, une solution de sécurité des courriels, un antivirus et un anti-maliciels.

4) MOINS DE PAPERASSE

Il peut être difficile et parfois inefficace d'éliminer tout le papier des processus d'affaires, mais dans toute la mesure du possible, vous devriez cesser d'imprimer, à moins que cela ne soit essentiel à votre travail. La plupart des fournisseurs offrent des fonctions libre-service qui permettent aux employés d'accéder à leurs bulletins de paie et à leurs feuillets d'impôt en ligne et de façon sécurisée. Non seulement cette solution sans papier est-elle plus sûre, mais elle est aussi écologique et moins coûteuse que d'imprimer. Si vous n'avez pas le choix d'imprimer, assurez-vous de tout passer à la déchiqueteuse aussitôt que possible après utilisation. Les documents que l'on laisse traîner sur le bureau ou dans la poubelle sont des cibles de choix pour les voleurs de données.

5) ÉVALUATION DE L'ESPACE DE TRAVAIL

Cette dernière étape concerne le plan personnel. Demandez-vous si vous laissez votre travail à la vue ou des documents sur votre bureau. Votre ordinateur se verrouille-t-il lorsqu'il tombe en veille? Qui a accès à vos dossiers et à votre pupitre lorsque vous n'êtes pas là? Avez-vous des documents qui devraient être gardés sous clé? Créez votre propre stratégie de protection des renseignements et appliquez-la.

Dans le contexte actuel, en particulier dans la profession de la paie, nous sommes tous responsables de bien protéger les renseignements. Les attaques sont de plus en plus sophistiquées et il faut s'en défendre non seulement avec les technologies, mais aussi en adaptant les processus et en formant les gens. Les voleurs de données ont compris qu'essayer d'obtenir l'information de vos employés est beaucoup plus efficace que de simplement craquer la technologie. C'est pour cela qu'une main-d'œuvre à l'affût est la clé de la protection des données. Avec une politique détaillée et une formation en profondeur sur la sécurité des renseignements, vous et vos employés serez équipés pour protéger toutes les données confidentielles sur la paie et tous les renseignements personnels. ■

Kevin Sokolowski est vice-président, Technologies de l'information chez Payworks, un leader national du secteur de la gestion globale de la main-d'œuvre, qui offre en ligne des solutions de paie, de ressources humaines et de gestion du temps des employés à plus de 13 000 entreprises au Canada. Pour en savoir plus, visitez payworks.ca.