OFFRIR AUX EMPLOYÉS UNE FORMATION SUR MESURE EN CYBERSÉCURITÉ

OCTOBRE 2020 **ITSAP.10.093**

Le Centre canadien pour la cybersécurité vous propose d'adopter dix mesures de sécurité des TI, dont l'une d'elles est d'offrir de la formation en cybersécurité adaptée à vos besoins opérationnels et à vos exigences de sécurité. Si tous les membres du personnel (c'est-à-dire les employés, les entrepreneurs, les gestionnaires et les cadres) suivent une formation adéquate, ils seront davantage sensibilisés aux enjeux de cybersécurité, ce qui fera diminuer les risques qui pèsent sur votre organisme. La formation favorise l'adoption d'une saine culture de cybersécurité dans laquelle les employés se sentent soutenus et outillés pour s'acquitter de leurs fonctions.

PRÉPARER DE LA FORMATION À L'INTERNE

Si vous disposez des ressources et du savoir-faire nécessaires, offrez de la formation à l'interne à tous les membres du personnel. Coordonnez la formation avec vos équipes de TI et de sécurité pour vous assurer de toucher à tous les sujets importants.

TYPES DE FORMATION À OFFRIR

- Une **formation de base en cybersécurité** offerte à tous les membres du personnel (nouveaux ou déjà en poste) qui porte sur les politiques, les procédures et les menaces.
- Une **formation assistée par ordinateur** que les employés suivent à partir de leur bureau pour se mettre à jour sur les principales notions de cybersécurité.
- Une **formation axée sur les rôles** propre à certaines fonctions (p. ex., administrateurs de système ou développeurs).

Songez à intégrer des exercices pratiques à toutes les formations, comme la détection des courriels d'hameçonnage ou l'examen du processus d'intervention en cas d'incident.

SUJETS À ABORDER

Offrir une formation adéquate aux membres du personnel est un des premiers moyens de défense contre les cybermenaces, car ils peuvent ainsi se familiariser avec leurs rôles et leurs responsabilités et savoir pourquoi ils doivent mettre en œuvre les pratiques exemplaires. Voici quelques sujets à aborder :

- repérer et contrer les tentatives d'hameçonnage;
- choisir des mots de passe robustes;
- mettre les systèmes à jour et appliquer les correctifs;
- protéger les biens informatiques et l'information sensible;
- signaler les incidents.

Les études de cas et les exemples d'incidents de cybersécurité connus du public permettent d'illustrer plus facilement les vulnérabilités, les techniques employées par les auteurs de menaces et les mesures d'atténuation.

FORMATION EXTERNE

Si vous ne disposez pas des ressources nécessaires pour offrir de la formation à l'interne, tournez-vous vers la formation externe.

Le Carrefour de l'apprentissage du Centre canadien pour la cybersécurité offre des programmes de formation en classe et en ligne s'adressant à un public varié ainsi que des programmes sur mesure. Les activités et les programmes sont surtout destinés aux ministères et aux organismes du gouvernement du Canada (GC) et à leurs partenaires nationaux, mais les autres ordres de gouvernement et les intervenants de l'industrie qui collaborent avec le GC peuvent aussi s'en prévaloir.

INFORMATION SUPPLÉMENTAIRE

En panne d'inspiration? Consultez les publications du Centre canadien pour la cybersécurité (cyber.gc.ca) pour connaître les conseils et les pratiques exemplaires en matière de cybersécurité :

- *ITSM.10.093 Les 10 mesures de sécurité des TI : N° 6, Miser sur une formation sur mesure en matière de cybersécurité*
- *ITSAP.00.101 Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*
- *ITSAP.30.032 Pratiques exemplaires de création de phrases de passe et de mots de passe*
- *ITSAP.10.096 Application des mises à jour sur les dispositifs*

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.

SÉRIE SENSIBILISATION