CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Offrir aux employées et employés une formation sur mesure en cybersécurité

Septembre 2024 | ITSAP.10.093

Une des dix mesures de sécurité des TI que propose le Centre pour la cybersécurité est d'offrir de la formation en cybersécurité adaptée à vos besoins opérationnels et à vos exigences de sécurité. En offrant de la formation sur mesure à tout votre personnel, y compris les employées et employés, les entrepreneures et entrepreneurs, les gestionnaires et les cadres, vous le sensibilisez davantage aux enjeux de cybersécurité qui touchent votre organisation. Si votre personnel est mieux informé sur ces questions, votre organisation court moins de risques. La formation favorise l'adoption d'une saine culture de cybersécurité dans laquelle les employées et employés se sentent soutenus et outillés pour s'acquitter de leurs fonctions.

Types de formations

La formation relative à la cybersécurité doit aborder divers sujets et être offerte dans différents formats. Par exemple :

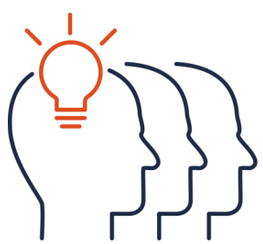
- Une **formation de base en cybersécurité** offerte à l'ensemble des membres du personnel (nouvelles, nouveaux ou déjà en poste) qui porte sur les politiques, les procédures et les menaces.
- Une **formation assistée par ordinateur** que les membres du personnel suivent à partir de leur bureau pour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

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

Sujets des formations

La formation devrait au minimum comprendre les sujets suivants :

- 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 dans les formations permettent d'illustrer plus facilement les vulnérabilités, les techniques employées par les auteures et auteurs de menaces et les mesures d'atténuation.

Selon la nature de votre organisation, les exigences précises des rôles et les normes de l'industrie, vous pourriez devoir offrir de la formation spécialisée. Par exemple, les secteurs des infrastructures essentielles devront offrir de la formation abordant les aspects de cybersécurité liés à la technologie opérationnelle et aux systèmes de contrôle industriel. Vous pourriez également souhaiter offrir de la formation de sensibilisation sur des sujets comme la mésinformation, la désinformation et les technologies d'intelligence artificielle.

Lectures connexes

- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)
- Piratage psychologique (ITSAP.00.166)
- Repérer les cas de mésinformation, désinformation et malinformation (ITSAP.00.300)
- L'intelligence artificielle générative (ITSAP.00.041)

Formation interne

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

Formation externe

Vous pourriez devoir avoir recours à des fournisseurs tiers pour offrir des formations si vous ne disposez pas des ressources à l'interne. Le Carrefour de l'apprentissage du Centre 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. Ces activités et programmes sont surtout offerts au gouvernement du Canada (GC) et aux partenaires nationaux du Centre pour la cybersécurité. Cependant, les autres organismes gouvernementaux et partenaires de l'industrie qui travaillent avec des ministères du GC peuvent également participer. La publication intitulée Certifications dans le domaine de la cybersécurité liste les organismes de certification reconnus dans le monde qui offrent des options de formation à différents niveaux.

Pour en savoir plus

- Les 10 mesures de sécurité des TI : n° 6, misé sur une formation sur mesure en matière de cybersécurité (ITSM.10.093)
- Pratiques exemplaires en matière de cybersécurité à intégrer dans votre organisation (ITSAP.10.102)
- Introduction à l'environnement de cybermenaces
- Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)
- Ressources de cybersécurité pour les petites et moyennes organisations (ITSAP.00.137)

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

No de cat. D97-1/10-093-2024F-PDF
ISBN 978-0-660-73504-7

Canada