Offer tailored cyber security training to your employees

CANADIAN CENTRE FOR CYBER SECURITY

September 2024 | ITSAP.10.093

One of the top 10 IT security actions from the Cyber Centre is to provide cyber security training that is tailored to your organization's business needs and security requirements. By providing tailored training to all personnel, including employees, contractors, managers and executives, you can increase awareness of the cyber security issues that your organization faces. When your employees have a greater awareness of cyber security, your organization can reduce its risks. Training creates a positive cyber security culture where personnel feel supported and equipped with the right tools to carry out their job functions.

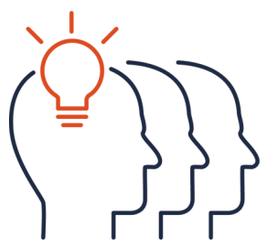
Types of training to offer

Cyber security training should cover various topics and can be delivered in different formats. For example:

- **basic cyber security training** for new and existing personnel to review policies, procedures, and current threats
- **computer-based training** that personnel can take from their desks to refresh their understanding of key cyber security topics
- **role-based training** for specific job functions, such as system administrators or developers

For all types of training, consider incorporating practical exercises, such as learning to spot phishing emails or reviewing your incident response process

Training topics



At a minimum, training should include the following topics:

- identifying and handling phishing attempts
- strengthening passwords
- updating and patching systems
- securing IT assets and sensitive information
- reporting incidents

Including case studies or examples of publicly known cyber security incidents in training material can help demonstrate vulnerabilities, threat actor techniques and mitigation measures.

Depending on the nature of your organization, specific job requirements and industry standards, you may need to provide more specialized training. For example, critical infrastructure sectors will need to provide specific training related to the cyber security elements of operational technology and industrial control systems.

Your organization may also want to provide awareness training on topics such as misinformation, disinformation and artificial intelligence technologies.

Related readings

- Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)
- Best practices for passphrases and passwords (ITSAP.30.032)
- How updates secure your device (ITSAP.10.096)
- Developing your incident response plan (ITSAP.40.003)
- Social engineering (ITSAP.00.166)
- How to identify misinformation, disinformation, and malinformation (ITSAP.00.300)
- Generative artificial intelligence (AI) (ITSAP.00.041)

In-house training

If you have the resources and expertise, make in-house training opportunities available to all personnel. Coordinate training activities with your IT and security teams to ensure topics are covered appropriately.

External training

You may need to look at third-party training providers if you don't have the resources to provide in-house training. The Cyber Centre Learning Hub offers in-class and online learning programs for various audiences, as well as customized programs. These activities and programs are offered primarily to the Government of Canada (GC) and our domestic partners. However, other government organizations and industry partners who work with GC departments may also participate. Our Certification in the field of cyber security publication outlines globally recognized certification training bodies that offer a variety of training options at different levels.

Learn more:

- Top 10 IT security actions: #6 provide tailored cyber security training (ITSM.10.093)
- Cyber security hygiene best practices for your organization (ITSAP.10.102)
- An introduction to the cyber threat environment
- Cyber security resources for small and medium organizations (ITSAP.00.137)

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Cat. No. D97-1/10-093-2024E-PDF
ISBN 978-0-660-73503-0

Canada