Communications Security Establishment | Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

# OFFER TAILORED CYBER SECURITY TRAINING TO YOUR EMPLOYEES

OCTOBER 2020 ITSAP.10.093

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

## DEVELOP IN-HOUSE TRAINING

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

### TYPES OF TRAINING TO OFFER

- **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 (e.g. 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.

### TOPICS TO COVER

Proper training is one of your first lines of defence against cyber threats. Training ensures that employees know what their specific roles and responsibilities are and why they are being asked to follow best practices. So what topics should you cover? Some examples include:

- 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 can help demonstrate vulnerabilities, threat actor techniques, and mitigation measures.

## LOOK FOR EXTERNAL TRAINING

If you don't have the resources to provide in-house training, you can look outside of your organization for 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.

## LEARN MORE

If you are looking for inspiration on cyber security tips and best practices, refer to the publications on the Cyber Centre website (cyber.gc.ca), such as:

- *ITSM.10.093 Top IT Security Actions: Provide Tailored Cyber Security Training*
- *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*
- *ITSAP.10.096 How Updates Secure Your Device*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**

**AWARENESS SERIES**