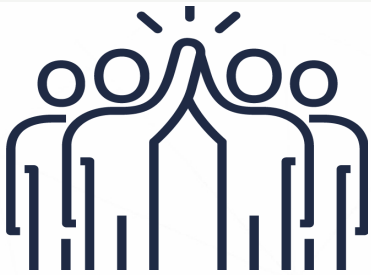
CANADIAN CENTRE FOR CYBER SECURITY

Common employee IT security challenges

May 2024

ITSAP.00.005



As an employee, you're not only privy to your organization's important and sensitive information, you're also responsible for protecting this information. Inadequate security practices leave your device vulnerable to threat actors who may want to bring down your organization's network and access your sensitive information. To prevent these vulnerabilities, it's critical that you recognize these common cyber security challenges and take measures to reduce the associated risks.

Falling for phishing attempts

Phishing is form of social engineering and scam where cyber threat actors attempt to trick you into opening malicious emails that contain attachments or links that will download malware onto your device. Phishing attempts can result in compromises to your organization and its sensitive information. Be vigilant and assess your emails before you open them.

Phishing is the most common way for attackers to compromise a computer system

Choosing poor Wi-Fi security

Wi-Fi hotspots are nearly everywhere, making them very convenient to use. However, accessing these networks gives threat actors opportunities to carry out attacks on devices and access information. A hotspot perceived as friendly, like at a coffee shop or restaurant, could be compromised and used for malicious attacks. To minimize this risk, avoid using unknown, unsecured, or public Wi-Fi hotspots when possible. Ensure that you have security measures in place to protect your networks, systems, and information when you must connect to public Wi-fi.

Mishandling sensitive information

A lost device like a USB drive, laptop, or tablet can lead to financial, legal, or public relations problems for your organization. It can also leave an embarrassing mark on your professional reputation. Follow the proper procedures if you need to take information out of the office. Contact your IT department to see if your files need to be encrypted. Keep in mind that removing the protective markings from a document does not change the sensitivity of the information.

Failing to use your mobile device securely

A lost, stolen, or compromised mobile device, such as a phone, laptop, or tablet, can allow unauthorized access to your organization's network. This puts not only your own information at risk but also that of your organization. Be sure to keep track of your devices, and maintain situational awareness. If your device is missing, contact your IT department immediately.

There have been over 150,000 reports of fraud in Canada with **over $600 million** stolen since January 2021.

According to a 2023 Canadian Anti-Fraud Centre report

AWARENESS SERIES

Cat. No. D97-1/00-005-2023E-PDF
ISBN 978-0-660-68429-1

Having poor password practices

Passwords and passphrases are simple forms of security and your first line of defence. Passwords and passphrases verify your identity and protect sensitive information from unauthorized access. Threat actors can easily hack into devices or accounts if you use easy-to-guess passwords or use the same password for different accounts.

When possible, we recommend that you use passphrases instead of passwords. Passphrases are longer and easier for you to remember, but more difficult for a threat actor to guess. Aim to create passphrases made up of **at least 4 words and 15 characters in length**. If you cannot use a passphrase (some websites have character limits) use a password with a **minimum of 12 characters**. Make sure it has both lowercase and uppercase letters, as well as numbers and special characters.

Here are some tips on password management:

- Use a complex password or passphrase that cannot be easily guessed
- Use a unique password or passphrase for each account
- Change passwords or passphrases when compromised,
  or if you suspect they have been compromised
- Keep your passwords or passphrases secret
- Enable multi-factor authentication on your accounts
- Consider using a password manager to help you create, protect, store and remember your login credentials
- Avoid typing your passwords on public computers
- Shield your keyboard or keypad when entering your password, passphrase or PIN

Downloading unauthorized applications

With the variety of workflow-enhancing applications that are available, you may be tempted to download applications to your work device to increase productivity. However, doing so can endanger your device and network by introducing vulnerabilities that threat actors could exploit.

Be sure to consult with your IT department whether you are authorized to download applications onto your device, and if there is an existing list of approved applications. If you are authorized to download applications, we recommend researching different vendors to make an informed choice about which is right for you and only downloading from a reputable vendor to minimize risks.

You should also keep your applications up to date by routinely running updates and patches.

Learn more

- Don't Take the Bait: Recognize and Avoid Phishing Attacks (ITSAP.00.101)
- Protecting your organization while using Wi-fi (ITSAP.80.009)
- Protecting high-value information: Tips for small and medium organizations (ITSAP.40.001)
- Using your Mobile Device Securely (ITSAP.00.001)
- Best Practices for Passphrases and Passwords (ITSAP.30.032)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
- Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Password Managers Security (ITSAP.30.025)
- How Updates Secure Your Devices (ITSAP.10.096)

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**.