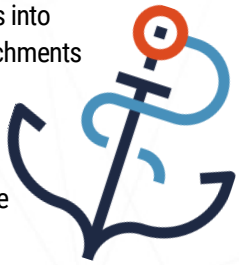
COMMON EMPLOYEE CYBER SECURITY CHALLENGES

OCTOBER 2020 **ITSAP.00.005**

INFORMATION TECHNOLOGY SECURITY IS EVERYONE'S RESPONSIBILITY

As an employee, you're not only privy to your organization's important and sensitive information, but you're also responsible for protecting this information. Inadequate security practices provide cyber threat actors with an easy way to bring down your organization's network and access your sensitive information. To prevent cyber attacks, there are some common cyber security challenges you can avoid.

FALLING FOR PHISHING ATTEMPTS



Cyber threat actors try to trick employees into opening emails that have malicious attachments or links to malicious websites. These **phishing** attempts can result in compromises to your organization. Be vigilant and assess your emails before you open them.

To learn more, read *Don't Take the Bait: Recognize and Avoid Phishing Attacks*.

PHISHING ATTACKS ARE STILL THE NUMBER ONE WAY FOR ATTACKERS TO COMPROMISE A COMPUTER SYSTEM

CHOOSING POOR WI-FI SECURITY

Wi-Fi hotspots are are just about everywhere these days, giving threat actors opportunities to carry out attacks on devices and information. A hotspot perceived as friendly (e.g. at a coffee shop or restaurant) may be compromised or malicious.

To minimize your risk of compromise, avoid using unknown, unsecured, or public Wi-Fi hotspots. To learn more, visit the Cyber Centre website to see our *Cyber Security and Wireless Technologies* interactive application.

MISHANDLING SENSITIVE INFORMATION

One lost USB drive, laptop, or tablet can lead to financial, legal, or public relations problems for your organization and leave an embarrassing mark on your professional reputation. If you need to take information out of the office, make sure you follow the proper procedures and 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

USING YOUR MOBILE DEVICE SECURITY

A lost, stolen, or compromised mobile device (e.g. phone, laptop, or tablet) can allow unauthorized access to your organization's network, which puts not only your own information at risk but also that of your organization. Follow the advice in *ITSAP.00.001 Using your Mobile Device Securely* to reduce this risk.

Over 28 Million Canadians have been affected by a data breach

According to The Office of the Privacy Commissioner of Canada's mandatory data breach reporting — October 2019

AWARENESS SERIES

DOWNLOADING UNAUTHORIZED APPLICATIONS

With the variety of workflow-enhancing applications that are available, you may be tempted to download unapproved applications to your work device. However, do you really know what the application is doing, or which data the application has access to? If you are authorized to download applications, only download them from a reputable vendor to minimize risks.

You should also keep your applications up to date by running updates and patches. See *ITSAP.10.096 How Updates Secure Your Devices* for more information.

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.

Your passphrase should be **at least 4 words and 15 characters in length**. For example, you might create a passphrase by scanning a room in your home and creating a passphrase that uses words to describe what you see (e.g. "ClosetlampBathroomMug").

- Use a complex password or passphrase or 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.

For more details on passwords and passphrases, refer to *ITSAP.30.032 Best Practices for Passphrases and Passwords*.

THE ART OF STRONG PASSWORDS AND PASSPHRASES

STRIVE FOR COMPLEXITY

If you cannot use a passphrase (e.g. on a website that only allows your password to be less than 15 characters), use a password that is as complex as possible. We recommend that you use a minimum of 12 characters. A password made up of lowercase and uppercase letters, as well as numbers and special characters, is more complex than a password of only lowercase letters. Keep in mind that websites and applications have different password creation rules that you have to follow (i.e. the letters, numbers, punctuation marks, and special characters that a password must and cannot contain).

****

We also recommend that you use two-factor authentication (e.g. a password **and** a biometric) for any application that allows it. Two-factor authentication increases your level of security.

BE AWARE

Shoulder surfing can happen anywhere, especially in public locations. Be wary of your surroundings, don't use public computers, and shield your keyboard or keypad when entering your password, passphrase, or PIN.

USE VARIETY

Using the same password or passphrase for multiple accounts makes it easier for unauthorized users to gain access to them. Use a unique password or passphrase for all your accounts.

PROTECT THEM

Do not keep your passwords, passphrases, or PINs on a piece of paper under a keyboard, on sticky notes next to a computer, or saved on the device itself. Consider using a password manager to help you create, protect, store, and remember your login credentials.

ACT QUICKLY

If you suspect that your password, passphrase, or PIN has been compromised, act quickly. Change it and consult your IT department for further advice.

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**.