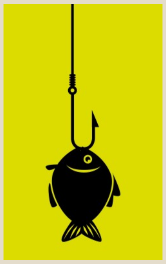
Communications Security Establishment
Centre de la sécurité des télécommunications

COMMON GC EMPLOYEE IT SECURITY CHALLENGES

OCTOBER 2017 AWARENESS SERIES ITSAP.00.005

INFORMATION TECHNOLOGY SECURITY IS EVERYONE'S RESPONSIBILITY

As employees, you are not only privy to important and sensitive information, but you are also responsible for safeguarding this information. Inadequate Information Technology Security (ITS) practices by employees can provide cyber threat actors with an easy way to bring down your organization's network, or give them access to sensitive information. To keep threat actors out, make sure to avoid these common IT Security challenges.



FALLING FOR PHISHING OR SPEAR PHISHING ATTEMPTS

Cyber threat actors will try to trick employees into opening e-mails and clicking on links to malicious websites or opening attachments that contain malicious software. These phishing attempts can result in cyber compromises to your organization. Be vigilant.
To learn more, read *Spotting Malicious E-mail Messages*.

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

CHOOSING POOR WI-FI SECURITY

Wi-Fi hotspots are just about everywhere these days making it easy for threat actors to snoop on others. A hotspot perceived as friendly (e.g., at a coffee shop or restaurant) may have been compromised, or the hotspot itself could be malicious. To minimize your risk of compromise, limit your use of unknown Wi-Fi hotspots. To learn more, watch CSE's *Cyber Security and Wireless Technologies* video.

25%

of data breaches are due to employee mistakes.

The Ponemon Institute's 2016 Cost of Data Breach Study

MISHANDLING SENSITIVE INFORMATION

A single 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. Removing the protection markings from a document does not change the sensitivity of the information.

BASIC MOBILE SECURITY

A lost, stolen, or compromised mobile device, phone, laptop, or tablet has the potential of allowing unauthorized access to your organization's network, placing not only your own information at risk, but also that of your organization. Follow the advice in CSE's *Using your Mobile Device Securely* which lists simple actions that can drastically reduce this risk.

Canada

DOWNLOADING UNAUTHORIZED APPLICATIONS

With the variety of available workflow-enhancing applications, it may be tempting to download unapproved applications to the device provided by your organization. However, do you really know what the application is doing, or what data the application has access to? If you are authorized to download applications, only download from a reputable vendor (e.g., iTunes, Google Play or Microsoft) to minimize risks.

HAVING BAD PASSWORD PRACTICES

Passwords are the simplest form of security, and they are the first line of defense. They verify your identity and safeguard access to sensitive information—be it a database at work or an on-line banking account at home. Access control is everyone's business and password security is a topic that we should all pay attention to. Make sure to use a complex password that cannot be easily guessed. Use a separate password for each account, and change them when they have been or are suspected of having been compromised. Most importantly, keep your passwords secret! Being IT security savvy isn't difficult, but in today's cyber world, it is important. By avoiding these common pitfalls, you will increase your organization's security posture and frustrate cyber threat actors.

The Art of Strong Passwords

Strive for Complexity

Weak passwords are easy to crack. Try using a memorable phrase with a mix of characters to create a stronger password: Ou8Tr&yc2 (Oh, you ate the red and yellow candy too).

Be Aware

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

Use Variety

Remember that using the same password for multiple accounts increases your security risk if your password is revealed. Use different passwords for work and home accounts.

Protect Them

Do not keep your passwords on a piece of paper under a keyboard, on sticky notes next to a computer, or save them on the device itself. Your passwords should never be written down.

Act Quickly

If at any time you suspect that your password may have been compromised, act quickly. Change it and consult your IT department for further advice.