CYBER TIPS

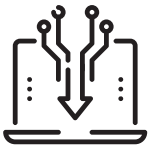
Message to Members

Cyber threats are happening more frequently than ever before with so many of us working remotely.

Here are some practical tips to allow you to stay cyber safe and protect Scouts Canada data and your digital identity from being stolen or compromised.

1 PROTECT DEVICES

Software updates matter.



Our computers, tablets and phones are great devices to have. But for all the benefit they bring us, they can also leave us exposed to cyber threats.

If you protect your devices, you protect yourself. And one of the best—and easiest—ways to protect your device is to regularly update its operating systems and applications and install security patches. Updates and patches do not just fix bugs or improve usability or performance; they address known security vulnerabilities.

Update during off-hours.

If you find you are prompted to update your software at inconvenient times, try setting a reminder to turn on your device during off-hours, like right before bed. That way your device can update when you do not need to use it.

Install updates automatically.

Enable automatic updates for all software on your devices, especially your OS. If automatic updates are not available, make sure to install secure when you do.

Use password-enabled screensavers.

When a user is inactive after a defined period, their device locks.

Turn off Bluetooth or Wi-Fi in your personal device when not in use.

Turning off Bluetooth and Wi-Fi prevents threat actors from attempting to connect to access your device.

Use multi-factor authentication.

This will add an additional layer of protection and requires two or more authentication factors to unlock devices, such as a PIN or a fingerprint.

Create complex passwords.

A password made of lowercase and uppercase letters, as well as numbers and special characters, is more complex than a password of only lowercase letters. Change them regularly and do not reuse passwords. Use a different password for each device and account, especially for accounts with sensitive information. Do not share passwords and do not give them out over the phone. Log off and sign out of accounts and websites when you are done using them. Be aware of your surroundings when entering passwords in a public space.

2 SAFEGUARD PROTECTED INFORMATION

Apply the principle of least privilege: Ensure that you only have access to the information that you need for your role. Controlling access can prevent unauthorized access to data.

Be aware of Protected Data that you encounter and cognizant of its associated restrictions. Scouts Canada collects personal information for membership purposes, and we have an obligation to keep it safe. In general:

- Only view sensitive and Protected Data residing in myScouts, such as Date of birth, PRC, or health information and do not download to your computer, or mobile device.
- Use encryption software to protect the confidentiality of sensitive information. Only transmit sensitive information if needed for a business reason, and this data needs to be encrypted both in transit and at rest. **How to encrypt files in Windows**
- Securely remove sensitive data files from your system when they are no longer needed. (e.g., No need to save the information you downloaded from myScouts as it will be there when you require it again.) Think twice about downloading sensitive information. Is there another way to accomplish the task at hand? If not, be sure to delete when no longer needed.

3 SAFEGUARD SCOUTS CANADA FROM MALWARE

Scammers steal sensitive information by pretending to be someone they are not. They may even use information from your social media accounts to make it seem like they know you, a tactic called social engineering.

1. Be vigilant and take care when you receive message or calls from someone you do not know, and requests come out of nowhere.
2. Trust your gut and if a phone call or a message is threatening or too good to be true, it probably is.
3. Think twice before you click a link's URL by hovering your cursor over it and do not open unexpected attachments.
4. Err on the side of caution.

Some ways that you can protect your device from malware are:

- Back up your devices and information.
- Use anti-virus software and keep it updated.
- Verify that files and attachments are legitimate before downloading them.
- Avoid using public Wi-Fi.
- Do not share personal information on social media sites that could help threat actors hack into your other accounts.
- Scan and verify removable media (e.g., USB, hard drives, CD, DVD before using it).
- Download media and software through trusted vendors.

Phishing is the act of sending mass emails that appear to be from a legitimate source but contain infected attachments or malicious links. The emails are written to trick receivers into opening attachments or clicking on links that permit threat actors to obtain personal credentials or gain access to a computer system and its information.

Spear phishing is a tactic used to send socially engineered emails to specifically target individuals or groups based on their personal characteristics, interests or lines of work. The messages appear to be sent by a credible source or subject that are relevant to the recipient and is the reason that they are so effective. They appear to be genuine. Before opening attachments or links embedded within an email, please take the following steps:

- Make sure that you know the sender of an email and that its tone is consistent with the sender. You can also call the individual on the phone to discuss.
- Make sure that the Web address or attachment is relevant to the content of the email.
- Make sure that the sender's email address has a valid username and domain name.

If you receive suspicious email or suspect malicious activity block the user, delete the message and do not click on any links.

Cyber Links for Reference:

Canadian Centre for Cyber Security | Centre canadien pour la cybersécurité

Get Cyber Safe