PROTECT YOURSELF FROM COVID-19 SCAMS

COVID-19-related scams are on the rise. In some cases, cybercriminals are using the Canada Emergency Response Benefit (CERB) or ads for protective gear to lure you into clicking links that could steal from you or lock your information.

Protect yourself by understanding how you could be targeted, and take some simple steps to shore up your defences. Here are five steps you can take right now on any device to protect yourself.

VISIT WWW.CYBER.GC.CA FOR MORE

BE ON GUARD FOR SCAMS

You are an attractive target for cyber criminals.

Know how to spot phishing and spear-phishing messages.

Be wary of suspicious links – don't click on them. The Government of Canada will not text you about refunds or send you e-transfers. When in doubt, visit official government websites by entering the URLs in your browser. Visit the Canada Revenue Agency for more about common scams.

SECURE YOUR SOCIAL MEDIA AND EMAIL ACCOUNTS

Review all privacy and security settings on your social media and email accounts and activate as many protections as possible.

Choose security questions for which the answers are not known by many people. For example, instead of "What is the name of your pet," choose "Who was your best friend in kindergarten?" Better yet, make up an answer that only you know. And never share that information on social media.

APPLY UPDATES TO YOUR MOBILE DEVICES, COMPUTERS, AND APPLICATIONS

Those updates are crucial to your security: they can contain what we call security "patches." Don't ignore them.

Be sure to apply updates to your mobile applications and your device operating systems and get them to automatically update.

STORE YOUR DATA SECURELY AND KNOW YOUR BACK-UP PROCEDURES

Use anti-virus or anti-malware software on computers.

Back up your vital personal information and important files. You may want to use cloud services to do that. Be sure to review the ransomware protections offered by your cloud service provider and turn on the available security features.

Practice recovering your data at least once. This way, you'll know what to do if you become a ransomware victim.

PRACTICE GOOD PASSWORD ETIQUETTE

Use unique passphrases or complex passwords, especially for sites that hold sensitive or personal information like your online banking or CRA accounts.

Don't share passwords. Don't use the same password for multiple accounts, websites, or devices.

Use two-factor authentication (2FA) when available.