SENIORS' GUIDE TO STAYING CYBER SAFE DURING COVID-19

During the COVID-19 pandemic, Canadians are spending more time online than ever before. That's why it's never been more important to stay cyber secure.

Instances of cyber criminals masquerading as healthcare organizations or Government of Canada representatives have been increasing – and in many cases, they're targeting seniors.

COVID-19 has showed us how quickly the world can change, but the need to stay cyber safe hasn't. If you know how to spot a scam and keep your account secure, you can prepare yourself for what's out there.

PROTECT YOURSELF WITH SIMPLE STEPS

PRACTICE SAFE PASSWORDS

Use a **passphrase**, a series of at least four words and 15 characters in length.

Or use **complex passwords** with:

- At least 12 characters
- Upper and lower case letters, numbers and symbols
- No personal information

USE A DIFFERENT PASSWORD FOR EVERY ACCOUNT

NEVER, EVER SHARE YOUR PASSWORDS WITH ANYONE

Too many passwords to remember? Try storing them in a password manager: software that creates, stores and securely encrypts your passwords so only you can access them when you need to.

ENABLE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) uses two or more different ways of verifying that you are who you say you are to add an extra layer of protection for your accounts and devices. We call these **authentication factors**.

Some different types of authentication factors include:

- Proof of **who you are**, like fingerprint scanners or facial recognition
- Proof of **what you know**, like a security question or password
- Proof of **what you own**, like an app or text notiftication on your phone

DON'T TAKE THE BAIT

Phishing scams are messages or phone calls made to look and sound like they're from people or companies you're familiar with. In some cases, a cybercriminal may already know something about you to make the message or phone call sound more legitimate.

IF YOU RECEIVE A SUSPICIOUS EMAIL, PHONE CALL OR TEXT (EVEN IF IT SEEMS LIKE IT'S FROM A FAMILIAR COMPANY OR A FRIEND) HERE'S WHAT TO DO:

BREATHE. Phishing messages often pressure or threaten you to respond quickly. If an email needs you to "act now", it's probably a scam.

DON'T OPEN ANY LINKS OR ATTACHMENTS you're unsure of. Reach out to the sender in a different way, like by phone, to confirm.

CONSIDER YOUR INTERNET HISTORY. Unless you requested it, any message asking you to reset your password or update your account info is likely fake.

DELETE ANY MESSAGES THAT SEEM TOO GOOD TO BE TRUE, like winning a contest you didn't enter.

GET MORE TIPS TO PROTECT YOURSELF AND YOUR DEVICES AT **GETCYBERSAFE.CA**

FOLLOW US ON SOCIAL MEDIA **@GETCYBERSAFE**

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada