HOW TO SPOT A TECH SUPPORT SCAM

It often starts with a **POP-UP**…

"CALL NOW or Else…"

THEN, YOU CALL A **TOLL-FREE NUMBER**
OR CLICK A **WEBSITE LINK**.

THE SCAMMER MIGHT:

Ask you to give them **REMOTE ACCESS** to your computer

Pretend to run a **DIAGNOSTIC TEST**

Tell you they've "discovered" a **VIRUS** or other **SECURITY** issue

Try to sell you **REPAIR SERVICES** or a **SECURITY SUBSCRIPTION**

THEN, YOU'RE ASKED TO **PAY A FEE**.

THE SCAMMER CLAIMS IT CAN PROVIDE "SERVICES" THAT RANGE FROM:

"Fixing" a problem that doesn't exist

Subscriptions that don't do anything

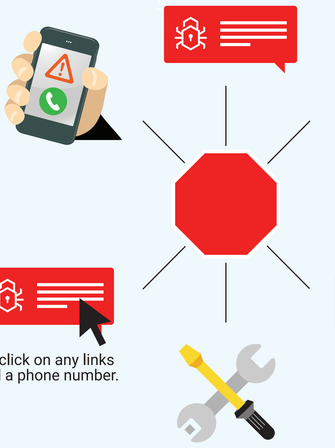
Installing fake antivirus software

Leading the scammer to STEALING PERSONAL INFORMATION **or** INSTALLING MALICIOUS MALWARE

Legitimate companies **do not display pop-up warnings and ask you to call a toll-free number** about viruses or security problems.

WHAT YOU CAN DO:

If you get a **POP-UP**, **CALL**, **SPAM EMAIL** or any other urgent message about a virus on your computer, **STOP**.



Don't click on any links or call a phone number.

Don't send any money.

Don't give anyone control of your computer.

TIPS

Keep your **ANTI-VIRUS** and security software up to date. Know how to spot a scam.

Tell **friends** and **family** about this **SCAM**. You might help them **SPOT IT!**

REPORT THE SCAM

to **fightspam.gc.ca** and **antifraudcentre.ca**