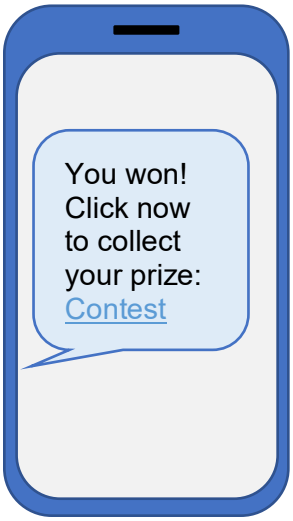
Grassroots Digital Hub

Phone safety tips



Watch out for…

- Calls and SMS/texts from phone numbers you don't know
- A message that makes you really happy or frightened
- A caller or SMS/text that pressure you to act quickly
- An SMS/text that tells you to click a link
- If there is a delay before a caller begins to speak
- If a caller is abusive and threatening
- Any request for money or personal/confidential information

Don't do it!

- Don't give any confidential information, like your social insurance number (SIN), banking information, or username and password.
- Don't send money.
- Don't click links provided.
- Don't respond to the SMS/text.
- Don't call a number that's given to you, or use the call back feature on your phone.

What to do

- It's ok to hang up, or let an unknown caller go to voicemail.
- Block the number.
- If you are worried about a loved one, find their number and call them.

Remember

- Fraudsters can be very tricky and will try everything to manipulate you, including impersonating loved ones.
- Government and banks do not ask for personal information over the phone if they call you. If you call them, they may ask for this information to verify your identity.
- A company that pressures you, doesn't deserve your business.

What you might see or hear

- **A plea for help:** It seems like it's someone you know. They really need your help. Usually they need money. You are told that if you don't help, something bad will happen to them.
    - The caller or SMS/text builds your trust by:
        - Sharing personal information about you and your family (they found it on social media)
        - Sounding just like someone you care about (this may be AI)

- **The threat:** The caller or SMS/text is aggressive and demanding. You may be told:
    - It's the government or a legal service contacting you.
    - Something very bad will happen if you don't take action right away.
    - You must visit a website, or share confidential information, like your SIN or banking information.

- **Great news!** The caller or SMS/text may say that they have a great offer just for you, or that you won a contest, or that you have money coming. You are told to:
    - Act quickly
    - Click a link, or provide person information

  If you ask questions or delay, the text or caller may become abusive.

- **An offer of help:** The caller or SMS/text says that:
    - Your device or account has been hacked ("compromised")
    - To get help, you must click a link or provide confidential information
    - If you delay, you'll lose your funds or services

  You may be told it's your bank or computer service.

If it happens to you

- If you share your username and password, try to change them right away.
- If you share banking or credit card information, call your bank right away.
- Make a report to the police and the Canadian Anti-Fraud Centre's online reporting system or by phone at 1-888-495-8501.
- Tell friends and family what happened to you so that it's less likely to happen to them.

SSHRC CRSH
Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada
NSERC CRSNG
We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council.