



Cellphone Service Provider Fraud

The Canadian Anti-Fraud Centre (CAFC) is receiving reports of criminals pretending to be cellphone service providers. They may claim to work for a victim's current provider and offer a discount, upgraded plan or new device. The threat actors may guide victims to log in to their real cellphone account while they remain on the phone. They may then ask for account details, security codes or other personal information.

In other cases, criminals may convince victims to open an account with a different service provider and obtain a new cellphone or tablet. They may ask victims to provide identification, such as a driver's licence or Social Insurance Number (SIN), to complete the order. Once the device is delivered, the fraudster may claim that the wrong item was sent and instruct the victim to ship it to another address. The device and personal information may then be used to commit fraud or identity theft.

Warning signs

- You receive an unexpected call, text message or email offering a discount, upgraded plan or new device.
- The person pressures you to act quickly or says the offer is only available for a limited time.
- You are asked to log in to your cellphone account while the caller stays on the line.
- You are asked for your account password, security code, PIN or multi-factor authentication code.
- You are asked to provide a driver's licence, Social Insurance Number or other identification.
- You are told to open an account with a different service provider.
- You receive a cellphone or tablet and are told to send it to an address provided by the caller.
- The return address is different from the verified address of the service provider.

How to protect yourself

- If someone contacts you claiming to be from your service provider, end the call and contact the company directly.
- Use the telephone number on your bill, account or the company's official website.
- Do not use contact information provided by the caller.
- Never share passwords, PINs, security codes or multi-factor authentication codes.
- Do not provide personal or financial information during an unexpected call, text message or email.
- Do not log in to your account while an unknown caller is guiding you.
- Before opening a new account or accepting a device, confirm the offer directly with the service provider.
- If you receive a device you did not order, contact the service provider directly and confirm the correct return process.
- Never ship a cellphone or tablet to an address provided by an unknown caller.

What to do if you've been the target of a fraud

If you believe you have been a target of fraud, contact your financial institution immediately and report the incident to your local police and the [Canadian Anti-Fraud Centre](#).