

Phishing (email) and Smishing (texts)

Phishing (emails) and smishing (texts) are fake messages that appear to come from a legit, trusted individual / organization. Scammers prompt you to give up personal info – *username, password, credit card number, bank account info* – or click on a link that downloads malware or spyware to your device.

Phishing on social media is the use of fake profiles and malicious links used to steal personal information or gain control of accounts.

Scammers use the data to take over an account, send unauthorized payments, open fake accounts, and create fake identities.

A scammer contacts Jane and claims to be from her bank. There's an issue with her account or credit card, and they need to fix it right away. They ask for her PIN.

A scammer contacts Frank and claims to be with the CRA. They ask for his SIN and other personal info. He owes back taxes and must pay right away to avoid a fine or arrest. Or he has a refund – that he can access when he clicks on the link.

A scammer poses as a medical organization such as Blue Cross or Canada Life. They send a fax, asking for medical and other documents, falsely claiming they are part of a health audit.

BE AWARE!

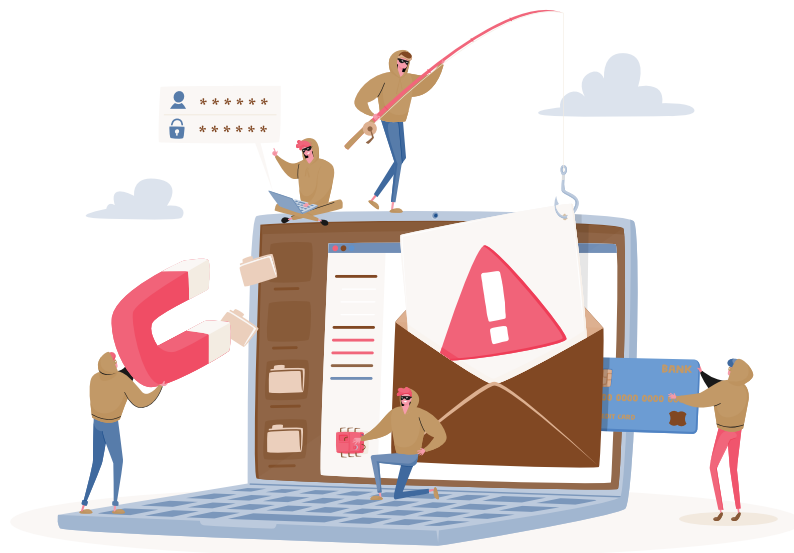
Banks and Governments will never ask for personal information, passwords or pin numbers by text or email. They will also never send links for you to click on to provide personal information.

WARNING SIGNS FOR PHISHING / SMISHING

- Threats and urgency – pressure to act quickly / right away.
- Unexpected sender – someone who would never contact you this way. For example, banks, the CRA, and all other federal or territorial departments would NEVER contact you this way.
- Unusual or unknown sender – someone you don't usually hear from, even if you know them.
- Unexpected or odd attachment.
- Too good to be true.
- Links to a suspicious URL (webpage address).
- Email or phone number that doesn't match the organization it's supposed to come from.

IF YOU SUSPECT A SCAM ...

- **PAUSE.** Take time to think. Do NOT reply or click on any links or provide any personal info.
- **VERIFY.** Contact the sender directly – call them. Tell them about the message that you suspect a scam.
- **Check the URL.** You can see it without clicking if you hover the cursor over it. Type it directly into your search engine.
- **Delete any suspicious messages and empty the ‘trash’ right away.**
- **Check your accounts if needed.**



Northwest Territories
Seniors' Society
ESTD. 1983
Seniors Helping Seniors