PROTECTING YOURSELF FROM CYBERTHREATS

PHISHING AND SCAMS

Scam emails and texts are designed to **create urgency** through emotional manipulation so you're tempted to click or share your personal information.

Phishing and Scam Red Flags:

In emails or texts, look out for:

- Requests to log-in and/or share banking information.
- Unexpected links or attachments, or coming from unexpected contacts/sources ie why would X be contacting me this way?
- Requests for personal information (address, phone number, email, passwords, MFA codes).

Over the phone or on social media, look out for:

- Voice calls from loved ones from unknown numbers - hang up and call them back to their actual phone number.
- Messages asking you to verify accounts or click links.

Best Practices:

- Enable Multifactor Authentication (MFA).
- Use trusted software.
- Use public Wi-Fi for low-risk activities only.
- Review privacy settings to limit data sharing.
- Use secure websites that start with https://

STOP.THINK.VERIFY.

Ask yourself:

- Does this make sense?
- Are they rushing or pressuring me?
- Am I feeling strong emotional responses? (Fear, excitement, anger)
- Is this really who they're saying they are? Can I confirm their identity?
- **Be suspicious - trust as much as you are comfortable, but make sure you verify legitimacy when there is a high risk to your information.**

SOCIAL ENGINEERING

Social engineering is when cybercriminals use information about you, taken from social media or phishing, to make scams look more legitimate or to access accounts.

Where are they getting information?

- Phishing scams where you share personal information by completing a form, sharing passwords, log-ins, credit card information, cell phone numbers etc.
- Social media oversharing - photos, names, birthdays, locations.

Protect yourself:

- Limit what you share publicly.
- Think before you post - how could someone use this information?

I'VE BEEN SCAMMED

You're not at fault:

- Act quickly - gather documents, screenshots and other evidence.
- Contact your bank immediately. Lock cards, lower limits, enable protection services.
- Change passwords and check your security settings. Enable any MFA that is not enabled.
- Report the incident:
  - Call your local police at their non-emergency line
  - RCMP: (519) 645-4329
  - Canadian Anti-Fraud Centre: https://reportcyberandfraud.canada.ca/

Western UNIVERSITY · CANADA



cybersmart.uwo.ca