Desjardins

Connected Canadians
Canadiens Branchés

Social Engineering Awareness Handout

Social Engineering

- Manipulating human psychology to gain access to sensitive information.

Common tactics

- **Phishing**: Scammers impersonate trusted sources to steal personal information.
    - **Pretexting** (fake scenarios to extract personal details).
    - **Baiting** (offering fake incentives like free software).
        - Example: The "Grandparent Scam" – fraudsters impersonate family members in distress to solicit money.
- **Smishing:** Text message scams that try to trick you into clicking bad links or sharing personal information
    - The word comes from combining **SMS (text messaging)** and **phishing (email scams)**.
- **Spear Phishing**: Highly targeted scams with personal details to increase credibility.
- **Pig Butchering:** Refers to scams where criminals build trust—often via social media or dating apps, before tricking victims into fake crypto or financial investments. The term comes from “fattening up a pig before slaughter.”

Warning signs

- Pressure to act quickly.
- Requests for secrecy.
- Unusual payment methods (gift cards, Bitcoin, prepaid credit cards).
- Emails with suspicious links, attachments, or requests for financial/personal data
- Malware & Ransomware

Malware

- Harmful software (viruses, Trojans, spyware) that steals data, damages systems, and enables unauthorized access.

(613) 699-7896
info@connectedcanadians.ca
www.connectedcanadians.ca
78 George St #204,
Ottawa, ON K1N 5W1

Desjardins

Connected Canadians
Canadiens Branchés

Signs of Malware infection:

- Sluggish device performance.
- Frequent crashes or pop-ups.
- Unauthorized file changes.
- Unusual network activity or disabled security software.

Ransomware:

- Encrypts or steals files and demands payment for access.

Real-Life Examples

- Phishing Scams: Impersonation of government agencies (e.g., CRA scam).
  - https://www.canada.ca/en/revenue-agency/corporate/scams-fraud/recognize-scam.html
- Romance Scam: Cybercriminal builds emotional trust to request money.
  - https://ottawacitizen.com/news/local-news/ottawa-woman-vicitimized-by-both-romance-scam-and-money-recovery-scheme
- Ransomware Attack: Ottawa health clinic disrupted by a cyberattack
  - https://ottawacitizen.com/news/local-news/rideau-valley-health-centre-service-disrupted-due-to-cyber-security-incident

Protecting Yourself

- Stay Vigilant: Question unexpected emails, texts, and calls.
- Verify Before Clicking: Never open suspicious links or attachments.
- Secure Your Devices: Use antivirus software, enable firewalls, and update your operating system.
- Avoid Public Wi-Fi for Sensitive Actions: Do not access banking or enter passwords on public networks.
- Check Suspicious Links: Use tools like VirusTotal to scan URLs.
- If in Doubt, Stop Communication: Contact organizations directly using official contact details.

(613) 699-7896
info@connectedcanadians.ca
www.connectedcanadians.ca
78 George St #204,
Ottawa, ON K1N 5W1

Desjardins

Connected Canadians
Canadiens Branchés

If you have questions or would like support with any of the topics discussed here, please reach out to Connected Canadians through our website: www.connectedcanadians.ca .
Our helpful volunteers are ready to assist you and ensure you feel confident and supported in your digital journey.

(613) 699-7896
info@connectedcanadians.ca
www.connectedcanadians.ca
78 George St #204,
Ottawa, ON K1N 5W1