Connecting Generations
Cyber-Seniors™

Staying Safe While Online Banking

Online Banking provides convenience but also presents risks such as fraud, phishing, and identity theft. This guide outlines key threats and best practices to protect your financial information.

Common Online Banking Threats

- **Phishing Attacks** – Fraudulent emails, texts, or calls impersonating banks to steal login credentials.
- **Cyberattacks & Data Breaches** – Hackers target banks and payment processors to gain access to sensitive information.
- **Social Engineering Scams** – Scammers manipulate individuals or bank employees to access accounts.
- **Skimming & Shimming Devices** – Hidden card readers on ATMs steal card details.
- **Mail Theft** – Criminals steal financial statements from mailboxes.

Consequences of Bank Fraud

- Unauthorized transactions and drained accounts.
- Identity theft leading to fraudulent loans and accounts.
- Stolen bank details used for money laundering.
- Compromised financial records and credit scores.

Who Is at Risk?

- Less experienced online users.
- Young people unfamiliar with banking security.
- Elderly individuals who may be more trusting.
- Anyone who does not actively monitor their accounts.

Common Banking Scams

1. **Overpayment Scams** – Fraudulent payments with fake refunds.
2. **Automatic Debit Scams** – Unauthorized recurring charges.
3. **Fake Check Scams** – Scammers send fake checks and demand refunds.
4. **Government Imposter Scams** – Fake government representatives requesting payment.

5. **Phishing Scams** – Emails or texts impersonating banks.
6. **Charity & Lending Scams** – Fraudulent organizations requesting donations or loans.
7. **Sweepstakes & Lottery Scams** – Fake winnings that require payment upfront.

Warning Signs of Bank Fraud

- **Unsolicited banking alerts** claiming your account is locked or compromised.
- **Unexpected transactions** in your bank statements.
- **Requests for sensitive information** via phone, email, or text.
- **Fake password reset notifications** urging immediate action.

Safe Banking Practices

- **Use Strong Passwords** – At least 10 characters with numbers, symbols, and mixed case.
- **Enable Two-Factor Authentication (2FA)** – Adds an extra layer of security.
- **Monitor Bank Statements Regularly** – Detect fraudulent transactions early.
- **Use Encrypted Websites Only** – Ensure the URL starts with 'https://'.
- **Avoid Public Wi-Fi for Banking** – Use a secure network or mobile data.

What to Do if You Are a Victim

- **Notify Your Bank Immediately** – Banks must investigate fraud reports within 10 business days.
- **Freeze Your Account** – Prevent further unauthorized transactions.
- **Change Banking Passwords** – Secure your account with a new, strong password.
- **Report Fraud to Authorities:**
    - **U.S.:** Report to the Federal Trade Commission (FTC) at reportfraud.ftc.gov.
    - **Canada:** Contact the Anti-Fraud Centre at antifraudcentre-centreantifraude.ca.
    - **Local Law Enforcement:** File a report for further investigation.

Who Can You Safely Share Banking Information With?

- **Trusted financial institutions** (banks, credit card providers).
- **Employer** for direct deposit purposes.
- **Tax filing services** (for tax credits and refunds).
- **Reputable online payment platforms** (PayPal, Zelle).

Need More Help?

For more information, contact Cyber-Seniors at **844-217-3057** or visit **www.cyberseniors.org**.

*This lesson guide was made possible by a **CIRA Net Good Grant**. Learn more at **cira.ca**.*