Help protect yourself from financial fraud

At Scotiabank, we're committed to helping you keep your accounts and financial information safe and secure. As part of this commitment, we use a number of security measures to help ensure the integrity of your transactions and your account information remains secure. By helping you recognize, reject, and report the most common types of scams, together we can help prevent financial fraud.

Here are three principles to help you be more aware and protect yourself from fraud. We also encourage you to visit scotiabank.com/security for more information and tips.

1 Recognize Fraud by knowing the most common scams

Phishing

- Fraudsters send text messages luring a victim into providing personal or financial information
- Fraudsters often impersonate government agencies, banks, communication providers or other companies
- Messages often ask victims to provide usernames, passwords, credit/debit card numbers, PINs and other sensitive information that can be used to commit financial crimes

Service

- Scammers call and claim to be a representative from a well-known tech company such as Microsoft or Windows
- Scammers claim that the victim's computer has been hacked and must be serviced
- Scammer remotely access victim's computer and may run programs, alter settings or access personal information
- Scammer advises that a fee is required for this service and request payment by credit card or money transfer

Extortion

- Fraudsters call impersonating the Canada Revenue Agency (CRA) claiming there are discrepancies from past filed taxes and repayment is required immediately
- Fraudsters threaten that failure to pay will result in additional fees and/or jail time
- Fraudsters request payment by a money service business or pre-paid cards or gift cards (e.g. iTunes)

Personal information

- Any solicitation where an individual is asked to disclose or verify private personal information via email, text, telephone etc.

Cryptocurrency

- Victims receive mass marketing offers requesting that payments be sent through a cryptocurrency service, such as Bitcoin
- Cryptocurrencies operate independently of a central bank and are currently unregulated in Canada
- Bitcoin is the most common, however, there are many other cryptocurrencies

Bank Investigator

- Fraudsters contact consumers by phone asking for assistance to catch a bank employee who has been stealing money
- Victim is instructed to attend their bank branch and make a cash withdrawal from their account without disclosing the reason for their action as the teller may be involved in the scam
- The victim is instructed to place the cash in an envelope and meet the "investigator" or send money through a wire service such as Western Union

Mail Scams

- Victims receive unsolicited mail advising that they are either the beneficiary of an inheritance from a distant relative or have won a lottery
- Before any funds can be released, the victim is asked to pay one or more upfront fees

Romance

- Scammers use dating or social networking sites to seek out potential victims
- Scammers gain trust of the victim and communicate via phone, skype, social media and email for months to build trust
- Scammers often claim to be working abroad, usually in a lucrative business venture
- Scammers eventually ask to meet the victim, but ask for assistance in paying travel costs or for money to cover an emergency

Loan

- Offers are found through advertising or websites designed to look like legitimate lending institutions
- Victims applying are required to provide personal information, which can lead to ID fraud
- Since all victims are approved, fraudsters demand victims pay an upfront fee to secure the loan
- Victims are told that the loan will be deposited to their account within 24 hours of sending the fee
- Once the money is sent, the fraudster stops communication and no loan money is received

Visit the Canadian Anti-Fraud Centre website (www.antifraudcentre-centreantifraude.ca) for scam updates and to learn more about protecting yourself from fraud.

2 Reject Fraud by being aware of preventative tips

Dos

- Shred and dispose of all personal and financial documents; receipts, credit card offers, bills etc.
- Keep personal and financial documents, wallets and purses locked safely
- Sign up for Scotiabank *InfoAlerts* through *Scotia OnLine* or *Scotia Mobile Banking*
- Always review your banking and other statements for irregularities. Go paperless by signing up for online statements

Don'ts

- Never provide personal or banking or other account information unless you initiated the call
- Never click on any links received from suspicious senders
- Never respond to any request offering a % of a fortune or fees to claim prizes
- Never respond to companies offering guaranteed loans or pay upfront fees

Keep your financial and personal information secure

Scotiabank will not ask you to validate or restore your account access through email or text messages. We do not send text messages or emails that ask you for your:

- Password for *Scotia OnLine* and *Scotia Mobile Banking*
- Personal Identification Number (PIN) for either your ScotiaCard or credit cards
- Account numbers, for any type of account

Please do not respond to any message that asks you for any of these details, and do not provide your information. If you suspect suspicious activities, please report it to us.

Call 1-800-4SCOTIA (1-800-472-6842)

3 Report Fraud by immediately notifying Scotiabank

Report any suspicious activity to Scotiabank immediately either by:

- **Emailing phishing@scotiabank.com**
- **Calling the Scotiabank Contact Centre at 1-800-4SCOTIA**

Online Security Guarantee

SECURITY GUARANTEE

We will fully reimburse you in the unlikely event that you suffer direct financial losses due to unauthorized activity[1] in your accounts through *Scotia OnLine* Financial Services[2] or through Mobile Banking, provided you have met your security responsibilities.

Visit www.scotiabank.com/security for more information.