Keeping your PIN and passwords secure is key to keeping your money safe.

Your Personal Identification Number (PIN), passwords or access codes you use to access your accounts at Automated Banking Machines (ABMs), Direct Payment terminals, *Scotia OnLine*® Financial Services, Scotiabank® Mobile Banking and *TeleScotia*® Automated Telephone Banking constitute your electronic signature. Keeping your PIN, access codes and passwords secure is essential to keeping your money safe. While Scotiabank takes strong measures to ensure the security of your financial transactions and the confidentiality of your information, you play the most important role. Selecting secure PINs, passwords and access codes for your *ScotiaCard* bank card or credit card and keeping them confidential is the first step.

Keeping your PIN and passwords secure is key to keeping your money safe.

To report a lost or stolen card, fraudulent activity, internet or mobile security concerns, immediately call one of these numbers:

Service in English:
1-800-4SCOTIA (1-800-472-6842)
In the Toronto Area (416) 701-7200

Service en français:
1 800 575-2424
(416) 701-7222 (Région de Toronto)

Customer Service for TTY/TTD:
1-800-645-0288

You're richer than you think.®

10052936 9221018 (05/15) R

DIRECT PAYMENT • ABM
ONLINE • MOBILE • *TELESCOTIA*

Protect your PIN & Password

Scotiabank®

How to select and protect your PIN and passwords:

- Select 4 unique digits (numbers, letters or a combination) that you can remember. DO NOT select your birth date, telephone number, license plate, address or other easy to guess combinations.
- Memorize your PIN and passwords, DO NOT write them down, note them on your phone, or in an app, on your computer, or tell anyone what they are.
- Remember to shield the keypad when entering your PIN at an ABM or when making an *Interac*† Debit or credit card purchase.
- Contact us immediately if you suspect your card and/or PIN have been compromised.

Tips for fraud prevention:

- Check your monthly statements: contact us immediately if you detect unusual activity, e.g. purchases you did not make or missing charges.
- Keep your card in sight at all times during a transaction.
- Report a lost or stolen card immediately.
- Never lend your card to anyone, even someone close to you.
- Contact your wireless carrier to have your mobile service suspended if you lose your cellphone.

You can get a new or replacement *ScotiaCard*®, and change your *ScotiaCard* or credit card PIN at any Scotiabank branch in Canada. *ScotiaCard* and credit card PINs can also be changed at any Scotiabank ABM. For further details, please refer to your banking card agreement (copies are available at any Scotiabank branch).

Interac and VISA* Zero Liability Policy

The *Interac* and VISA Zero Liability policies protect you when using your *ScotiaCard*. You will not be liable for losses resulting from unauthorized transactions. Refer to the *ScotiaCard*® Cardholder Agreement Liability section for more details.**

How to protect yourself when banking online or using a mobile device:

- Never send confidential information (such as account numbers, ***ScotiaCard*** number, password, etc.) via email. Scotiabank will never send you emails or text messages requesting personal or any other confidential information.
- Avoid using software that records your passwords.
- Use required browsers with 128-bit encryption.
- Install and frequently update proven anti-virus and personal firewall products.
- Never download software or accept files or attachments when accessing websites, newsgroups and chat rooms unless you are confident in their authenticity.
- Disable file sharing on your personal computer.
- If you use mobile banking, use our Save this ***ScotiaCard*** feature. We use a secure method that does not keep your information on your phone.

Security tips for online and mobile banking:

- Memorize and protect your ***Scotia OnLine*** and mobile banking password, as well as your Verified by Visa* Access Code. Do not reveal them to anyone.
- On a computer, always type the website address or use your bookmarks to access ***Scotia OnLine*** (www.scotiaonline.scotiabank.com). This address will always be present in the first part of the address line for a valid ***Scotia OnLine*** web page.
- Do not leave your computer or mobile phone unattended while signed-on to either ***Scotia OnLine*** or Scotiabank Mobile Banking.
- Always sign-out of ***Scotia OnLine*** using the link located on the top right hand corner of your screen.
- When you finish a mobile banking session, use the Logout function.
- Clear your browser's cache after each ***Scotia OnLine*** session.

Our Security Guarantee

At Scotiabank, we're committed to keeping your accounts and financial information safe and secure. With ***Scotia OnLine*** Financial Services and Scotiabank® Mobile Banking you are protected from unauthorized transactions and will be fully reimbursed provided you have met your security responsibilities.

For more information on our guarantees:

Online Security Guarantee:
scotiabank.com/guarantee

Mobile Security Guarantee:
scotiabank.com/mobilebanking/security