General security practices

Here are some general security best practices that can help you keep your personal and financial information secure.

Do

Education:

- Stay informed and follow any new security practices that emerge over time
- Educate children and seniors on the importance of information security practices

Password:

- Protect your PIN and passwords and never write them down
- Choose unique PINs and passwords that others can't guess and memorize them; don't use the same password for multiple websites or mobile apps
- Develop passphrases to help you remember your passwords

Communication:

- Find out why your information is needed and how it will be used, and then determine if it's appropriate to provide it
- Unless you've initiated the contact or are certain of who you are talking to, don't give out personal information over the phone, through the mail, or online

Elimination:

- Destroy old/expired bank cards, pre-approved credit card offers and carbons and receipts that contain account numbers and/or signatures
- Shred documents that contain personal and financial information

Physical documentation:

- Protect your tax identification number and those of your children and other family members by not carrying them in your wallet
- Minimize the amount of IDs that you carry (for example, SIN, password or birth certificate)
- Report lost or stolen cheques, credit cards, or debit cards immediately
- Notify your bank, branch, or the police of suspicious activity
- Store cancelled cheques, cheque books, and account statements in a safe place or sign up for eStatements
- Retrieve and review your mail promptly
- Sign the back of any new bank cards immediately and activate them

Scotiabank®

Review:

- Conduct a detailed review of your credit report at least once every year
- Review your bank account and credit card statements promptly
- Go paperless and sign up for InfoAlerts to monitor your account activity

---

Don't

Communication:

- Don't respond to unsolicited emails, text messages, or phone calls that request personal or financial information, such as your bank card number, ABM PIN, banking passwords, or credit card numbers

Bank cards:

- Don't leave your bank cards unattended or out of your sight when making a purchase (for example, a cashier or taxi driver)
- Don't write your PIN down anywhere (for example, the back of your bank card)

Personal information:

- Don't email confidential information, such as account numbers or tax identification numbers
- Don't leave personal information unattended, such as bank statements or tax returns
- Don't throw out documents before destroying or shredding all sensitive and identifiable information

Scotiabank®