Anyone can be the victim of a scam, regardless of age, education or place of residence. Most incidents of fraud can be avoided. To protect yourself effectively, stay vigilant and learn to recognize fraud.
BANK NOTE COUNTERFEITING
Checking bank notes: It’s on the money!

Cash is a convenient and quick payment method. Everyone uses it, which is why counterfeitors are interested in it. Each time you accept a bank note without checking it, you are at risk of becoming a victim of counterfeiting.

Whether you’re the clerk or the customer, you can help stop counterfeit notes from entering the cash flow. When businesses lose money to fraud, the cost is often passed on to you, the consumer.

Canadian bank notes have security features that are easy to check and hard to counterfeit. However, bank notes are secure only if you check them. If you know your notes, you’ll be able to detect a counterfeit at a glance.

To identify a counterfeit note, you need to know the bank note security features. It’s your best defence against counterfeiting. Here are some tips:

• Compare a suspicious note to one you know is genuine.
• Check two or more security features.
• Look for differences, not similarities.
• If you do not know how to check a paper note, ask for a polymer note instead.

How to check polymer notes

Feel, look and flip

• Feel the smooth, unique texture. It is made from a single piece of polymer with some transparent areas.
• Feel the raised ink on the large number, the shoulders of the large portrait, and the words “Bank of Canada” and “Banque du Canada.”
• Look at the large window containing a metallic portrait and building, the word “Canada” which is transparent and feels slightly raised, and small numbers that match the note’s value.
• Flip the note to see these images in the large window repeated in the same colours and detail on the back.
Be aware that you are not legally required to accept a bank note if you doubt its authenticity.

If, **DURING** a transaction, you suspect that you have been given a counterfeit note:

- Politely refuse the note and explain that you suspect it might be counterfeit.
- Ask for another note (and check it too).
- Advise the person to check the suspicious note with local police.
- Inform your local police of a possible attempt to pass counterfeit money.

If, **AFTER** a transaction, you notice that you have accidentally accepted a note that may be counterfeit, give it to your local police for examination. If it turns out to be genuine, you’ll get your money back.
**Older series**
To learn more about the security features of older bank note series, visit www.bankofcanada.ca/banknotes/bank-note-series/.

**Canada 150 commemorative bank note**
In 2017, the Bank of Canada issued a commemorative $10 note to mark the 150th anniversary of Confederation. To learn more about this note and its security features, visit www.bankofcanada.ca/banknotes/banknote150/.

**A new $10 bank note in 2018**
Issued at the end of 2018, a new regularly circulating $10 bank note features the portrait of Viola Desmond, a champion for social justice. For the first time, an iconic Canadian woman is portrayed on a regularly circulating Bank of Canada bank note. To learn more about this note and its enhanced security features, visit http://www.bankofcanada.ca/banknotes.
IDENTITY THEFT AND FRAUD

What is it?

Identity theft occurs when a person obtains and uses your personal information for criminal activity without your knowledge or consent. Identity fraud is the fraudulent use of this information to

• gain access to your bank accounts
• apply for loans, credit cards or bank accounts
• obtain passports or receive government benefits
• obtain medical services

What do fraudsters do?

• Steal your wallet, purse or residential mail
• Search your garbage or recycling for bills, bank statements or other documents
• Complete a change of address form to redirect your mail
• Call you, pretending to be your creditor, your landlord, your employer, a government agent or an investigator
• Send unsolicited emails that appear legitimate
• Hack your electronic devices (computer, phone or tablet) or trick you into giving them access to your devices
• Create websites that mimic legitimate ones (such as banking websites, business websites or social media websites) to collect your personal information
• Tamper with automated banking machines and point-of-sale terminals

Main personal information:

• Full name
• Date of birth
• Address
• Email address
• Telephone number
• Passwords
• Social Insurance Number (SIN)
• Signature (manuscript or digital)
• Passport number
• Driver’s licence number
• Health insurance number
• Payment card information
How can you protect yourself?

Communication of personal information

• Stay alert: provide your personal information only when strictly necessary. Before giving your information, make sure that you know the people or organizations you are doing business with and that it was you who made contact with them.

Security and privacy settings

• Check your privacy and security settings before sharing personal information on social media. Consider everything you post to be public information.

• Deactivate the automatic geolocation feature on your phone before taking photos or videos you plan to share online. This will prevent people from finding out where you live or work.

• Protect your information. Lock your computer and mobile devices whenever you are not using them.

• Use secure websites (beginning with “https://”) whenever you have to communicate personal or financial information.

• Avoid making financial transactions or purchases on public wireless (Wi-Fi) networks.

Antivirus software and passwords

• Install antivirus software, a spam filter, a firewall and a spyware blocker on your electronic devices to reduce the risk of hacking.

• Protect your home's Wi-Fi network with a complex password.

• Use passwords that are difficult to crack. Your passwords should contain at least eight characters (the longer the better, including upper case letters, lower case letters, numbers, special characters or the first letters of each word in a phrase). Memorize your passwords and change them regularly.

Personal identification number (PIN)

• Memorize your PINs so that you do not have to keep a written record of them. When entering your PIN, make sure that no one around you can see it.
Social Insurance Number (SIN)

• Never share your SIN. By law, only government agencies, your employer (at the time of your hiring) and your financial institution can require you to provide it.

Official statements

• Check your bank and credit card statements regularly. Immediately dispute any purchase you do not recognize.

• Shred all documents containing personal information before you discard them.

Free software and applications

• Before you install free software or applications, read the licence agreement and privacy policy to avoid giving virtually unlimited access to your personal information.

• Check the sender’s email address on all the messages you receive. Always think twice before you click on a link or open a file of unknown origin. If you do not know who the sender of an email is, delete it. Never reply to email messages that ask you to verify your personal information or confirm your user ID or password.

Each year, request a copy of your credit report from TransUnion or Equifax and make sure there are no errors.

TO GET HELP OR REPORT FRAUD

• Immediately contact your financial institution and credit card company.

• Report the incident to local police.

• Contact both national credit rating agencies and request that a fraud alert be added to your credit report.
  • Equifax Canada: 1-800-465-7166
  • TransUnion Canada: 1-877-713-3393

• Contact the Canadian Anti-Fraud Centre to report the fraud at 1-888-495-8501 or visit www.antifraudcentre-centreatifraude.ca.
PAYMENT CARD FRAUD (CREDIT OR DEBIT)

What is it?

Payment card fraud refers to fraud committed using credit or debit cards, or the information from these cards, to obtain funds or acquire goods.

What do fraudsters do?

• Obtain your credit card number, its expiry date and security number (CVV number) and use this information to make telephone or online purchases.
• Obtain the personal identification number (PIN) of your debit card to make withdrawals and rob you of your savings.
• Obtain information from the magnetic strip on the back of a payment card in order to clone it.

How can you protect yourself?

• Keep only the cards you truly need on you, and make sure the rest are in a safe place.
• If your card is lost or stolen, report it as soon as you notice.
• Make transactions at a terminal when and where you feel most secure. If you notice anything unusual, report it to the police, the merchant or your financial institution.
• Never let anyone borrow your payment card and never share your PIN.
• Protect your PIN: it is your electronic signature.
  • Memorize your PIN and make sure that it is not recorded on any documents.
  • Choose a PIN that cannot be easily guessed. Do not use your date of birth, telephone number or address.
  • Change your PIN regularly.
  • Take care to shield your PIN from prying eyes when making transactions.
• Check your bank and credit card statements regularly. Immediately dispute any purchases you do not recognize.
• Beware of emails or text messages that claim to be from your financial institution or a government agency. These institutions never request personal or banking information from their clients by email or text messages.
TO GET HELP OR REPORT FRAUD

• Contact your financial institution or credit card company immediately.
• Report the incident to local police.
• Contact both national credit rating agencies and request that a fraud alert be added to your credit report.
  • Equifax Canada: 1-800-465-7166
  • TransUnion Canada: 1-877-713-3393
• Contact the Canadian Anti-Fraud Centre to report the fraud at 1-888-495-8501 or visit www.antifraudcentre-centreantifraude.ca.
“OVERPAYMENT” SCAMS

What is it?

“Overpayment” scams are various strategies that are generally used in conjunction with fraudulent (falsified, counterfeit or stolen) cheques or fake notices of transfer.

For example, these strategies may involve

• offering you a non-existent job
• overpaying for an item you have put up for sale (e.g., on a classifieds site)
• offering to reimburse you an overpaid amount by asking you to click on the link of a service provider (telephone, Internet, etc.) or public body (municipality, government agency, etc.)

What do fraudsters do?

Employment-related scams

• The scammer will send a text message or email with an enticing money-making opportunity (e.g., to serve as a representative of a foreign-based company or as a mystery shopper or to display a logo on your vehicle).

• Once you have accepted the offer, the scammer will tell you to deposit a cheque, transfer a certain amount of money to another account and keep part of the money as payment or commission. When the cheque proves fraudulent, you absorb the loss.

• The scammer will transfer funds to your account, then ask you to transfer a certain amount to another account. When the initial transaction proves fraudulent, you absorb the loss.

Classifieds scam

• The scammer will offer you a higher price than the asking price and ask you to deposit a cheque, keep part of the amount as payment for the item and pay the balance to a third party. You then provide the item and the money to the scammer’s accomplice. When the deposited cheque proves fraudulent, you absorb the loss.
How can you protect yourself?

• Never answer an unsolicited email or text message.

• Beware of “companies” that use a simple Web-based email address to conduct their business. Confirm the company exists, look up its coordinates (company name, civic address, telephone number) and validate this information.

• Do not transfer any funds before confirming the authenticity of a cheque or electronic deposit.

• Never accept a cheque made out to another individual and then signed over to you.

If a job seems too good to be true, it is a scam.

When carrying out sales transactions

• Never accept a cheque for more than the amount of the sale.

• If in doubt, simply decline to carry out the transaction.

TO GET HELP OR REPORT FRAUD

• Report the incident to your local police.

• Contact the Canadian Anti-Fraud Centre to report the fraud at 1-888-495-8501 or visit www.antifraudcentre-centreantifraude.ca.
“URGENT PAYMENT” SCAM

What is it?
In this scam, the victim is solicited by telephone, text message or email by individuals posing as government agents (often revenue or immigration agents). The scammers will try to get you to pay them an amount by claiming you owe money for unpaid taxes or an unaddressed administrative matter.

What do fraudsters do?

• Create a feeling of panic or urgency by making threats (of fines, lawsuits, deportation, arrest warrants, etc.), using an aggressive tone, or strongly pressuring you to instill fear and demand immediate payment.

• Ask you to purchase prepaid cards and share the activation codes on the back of the card.

• Ask you to make a payment by telephone or using a specific website.

How can you protect yourself?

• Do not give in to pressure. Be careful and skeptical.

• Be aware that government agencies never
  • use a threatening tone or exercise undue pressure when communicating with people;
  • require immediate payment for taxes, services or the processing of an immigration application using a prepaid card or money transfer.

• Find the official telephone number of the agency that contacted you, and call to verify the authenticity of the request.

TO GET HELP OR REPORT FRAUD

• Report the incident to your local police.

• Contact the Canadian Anti-Fraud Centre to report the fraud at 1-888-495-8501 or visit www.antifraudcentre-centreantifraude.ca.
TO GET HELP OR REPORT FRAUD

If you suspect that you are a victim of fraud, contact your local police.

For information on currency counterfeiting prevention, contact the Bank of Canada at 1-800-303-1282 or visit www.bankofcanada.ca/banknotes.

To learn about the security features on American bank notes, visit www.uscurrency.gov.

To contact the Sûreté du Québec: 310-4141 or *4141 from your cell phone

To contact the Service de police de la Ville de Montréal: 514-280-2222 or contact your neighbourhood police station directly.

To contact the Service de police de l’agglomération de Longueuil: 450-463-7011

To contact the Service de police de Laval: 450-662-4242

To report fraud to the Canadian Anti-Fraud Centre: 1-888-495-8501 or visit www.antifraudcentre-centreantifraude.ca.

To report fraud or any other criminal activity anonymously and confidentially:

For the Montréal region, call Info-Crime at 514 393-1133 or visit www.infocrimemontreal.ca.

Outside the Montréal region, call Échec au crime at 1-800-711-1800 or visit www.echecaucrime.com.

March 2018