FRAUD IN 3D

Detect, Denounce, Deter

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.

BANQUE DU CANADA
BANK OF CANADA

BANK NOTE COUNTERFEITING

Checking bank notes: It's on the money!

Cash is a convenient and quick method of payment. Everyone uses it, which is why counterfeiters 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 only secure 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.

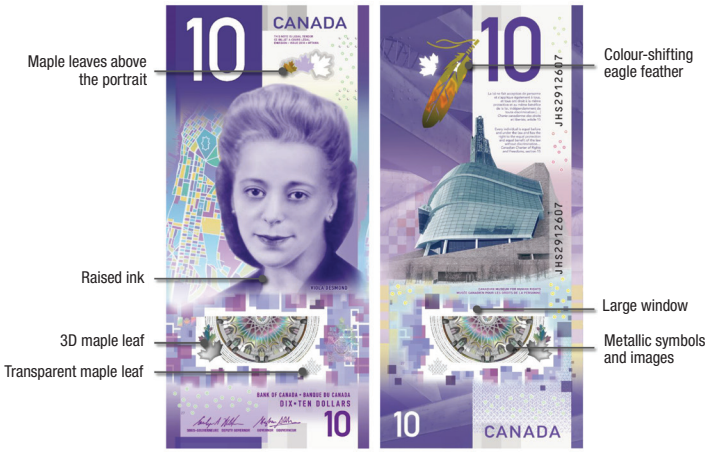
How to check polymer notes?

A New Direction for Canada's Bank Notes: the New $10 Note

The new $10 note has bold security features that are easy to check and difficult to counterfeit. Some are enhanced compared to those on the current polymer notes. The same checking method applies to all polymer bank notes.

Feel, look and flip

- Feel the smooth, unique texture of the note. It's made from a single piece of polymer with some transparent areas.
- Look for transparency in the large window.
- Look at the detailed metallic images and symbols in and around the large window.
- Look at the pattern in the colour-shifting eagle feather.
- Feel the raised ink on the portrait, the word "Canada" and the large number at the bottom.
- Flip the note to see these images in the large window, repeated in the same colours and detail on the other side.



Older series

To learn more about the security features of older bank note series, visit **www.bankofcanada.ca/banknotes/bank-note-series/**.

Did you know?

- **It is a criminal offence to knowingly pass counterfeit bank notes on to someone else.**
- **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.

TO GET HELP OR REPORT FRAUD

Report the incident or take the suspect note to local police.

For more information on bank notes, contact the Bank of Canada at **1-800-303-1282** or visit **www.bankofcanada.ca/banknotes**.

IDENTITY THEFT AND FRAUD

What is it?

Identity theft occurs when a person obtains 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 or credit cards, or open accounts (bank, client);
- sell your property without your knowledge;
- obtain passports or receive government benefits; or
- 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 to collect your personal information or create imitations of legitimate websites or applications (such as banking websites, business websites or social media websites).
- Trick you into giving them access to your electronic devices (computer, phone or tablet) in order to hack them.
- Tamper with automated banking machines and point-of-sale terminals.
- Make purchases without your knowledge.

Main personal information:

- **Full name**
- **Date of birth**
- **Home 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 downloading applications, registering on a website or sharing personal information on social media. Consider everything you post to be public information.
- Deactivate the automatic geolocation feature on your telephone. Carefully review usage and privacy policies before activating a location service.
- 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 (e.g., in a café).
- Never keep a photo of your driver's licence, passport or health card on your cell phone.

Antivirus software and passwords

- Install antivirus software, a spam filter, a firewall and a spyware blocker on your electronic devices. Activate the spam filter in your inbox. These measures will help reduce your vulnerability to hacking.
- Protect your home's Wi-Fi network with a complex password that contains at least 10 characters. Avoid dictionary words. Insert special characters in the middle of the word (avoid using upper-case letters at the beginning and numbers or special characters at the end of the word). Avoid replacing letters with special characters (e.g., a = @).
- Memorize your passwords and change them regularly (including your router password). Never use the same password for more than one site. Never allow a website to "remember your password."

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, including the clerk.

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.

Email

- Check the sender's email address on every message you receive. Always think twice before you click on a link or open a file of unknown origin. Delete the email if you do not know the sender. Never confirm or validate personal information by email.

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-centreantifraude.ca**.

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

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 or sell it on the Darknet.
- Obtain the personal identification number (PIN) of your debit card to make withdrawals, make purchases and rob you of your savings.
- Obtain information from the magnetic stripe on the back of a payment card to clone it.

How can you protect yourself?

- Keep only the cards you need with you and make sure the rest are in a safe place.
- Report your card as lost or stolen as soon as you notice it's missing.
- Make transactions at a terminal when and where you feel most secure. If you notice anything unusual, report it to the merchant, your financial institution or the police.
- Never lend your payment card to anyone and never share your PIN. Swipe your card yourself when you make a transaction and never let it out of your sight.
- 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, including the clerk.
- 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.

Been offered an "easy way" to make money? Resist the temptation—it's a scam!

What is it? You will be asked to lend out your bank account, including your debit card, for a transaction in exchange for a financial reward.

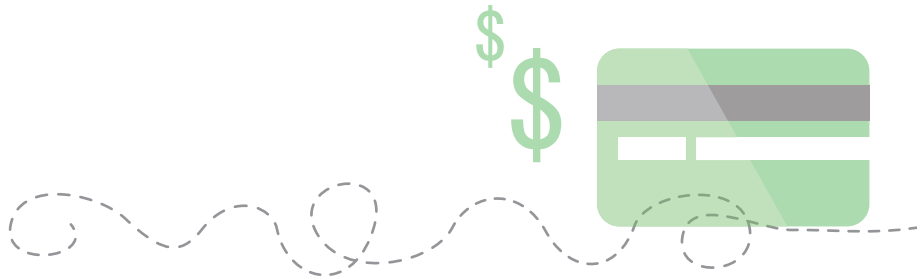
How can you protect yourself? Never let anyone borrow your payment card and never share your banking information (PIN).

Anyone who participates in this type of fraud will have their record with the financial institution marked for fraudulent bank account use.

Criminal charges for fraud may also be laid against you for involvement.

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**.



"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 (revenue or immigration), peace officers or head office employees. The scammers try to get you to pay them an amount or disclose information 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.
- Pretend to be a head office employee and ask you to purchase prepaid cards and share the activation codes on the back of the card.
- Ask you to purchase cryptocurrencies or pre-paid vouchers (such as Flexepin).
- 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.
- Never assume that the telephone number on your call display is right. Scammers use software programs and applications to trick their victims.
- Be aware that government agencies never:
  - use a threatening tone or exercise undue pressure when making requests for payment;
  - accept payments for reimbursements using prepaid cards.
- 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**.

CRYPTOCURRENCY SCAMS

What is it?

Cryptocurrency scams use digital or virtual currencies, presented as cryptographic (encrypted) codes. Scammers take advantage of the fact that it is difficult to trace cryptocurrencies to:

- Impersonate someone (e.g., government employee) to extract money from a victim in the form of cryptocurrency (e.g., bitcoin);
- create false cryptocurrency trading platforms to steal from victims;
- create fake digital wallets that facilitate the use of ransomware or that imitate popular sites to steal from victims;
- require a payment using a cryptocurrency for a fake online purchase (product will never be delivered); or
- encourage investors to participate in fake investments in cryptocurrency or token offerings, commonly known as an initial coin offerings (ICOs), related to so-called startup technology projects.

In Canada, only the Canadian dollar has legal tender status.

What do fraudsters do?

- Promise incredible rates of return and outstanding customer service to convince their victims that their trading platform or initial coin offering is superior.
- Contact victims directly by telephone, text or email and threaten them (e.g., unpaid taxes) by requiring an immediate payment in cryptocurrency.
- Imitate certain trading sites to trick victims.

How can you protect yourself?

- Constantly check the legitimacy of the person contacting you during transactions (in person, by phone, by email, on the Internet, etc.). Locate the official telephone number of the organization that contacted you and check the validity of what is being asked of you. Use secure websites (beginning with "https://").
- Check the sender's email address on all the messages you receive. Always think twice before clicking on a link or opening a file of unknown origin. Never reply to email messages that ask you to verify your personal information or confirm your user ID or password.
- Be careful of all online transactions involving cryptocurrencies. Beware of platforms that store private keys when purchases are made; it's a scam.
- Replace your digital wallet with one or more hardware wallets to store your cryptocurrency.
- Carefully check the wallet download source to keep viruses out of your computer systems.
- Protect your personal information and never share your private keys with third parties.
- Keep all documents related to cryptocurrency transactions.

TO GET HELP OR REPORT FRAUD

If you suspect or know that you have been a victim of a cryptocurrency scam:

- Report the incident to local police.
- Contact the Canadian Anti-Fraud Centre to report the fraud at **1-888-495-8501** or visit **www.antifraudcentre-centreantifraude.ca**.

RANSOMWARE

What is it?

- Ransomware is a type of malicious software that locks access to files or systems when it infects a computer.
- A ransom, payable by a crytpocurrency (such as bitcoin), appears on the screen in exchange for the decryption key.
- The infected computer remains functional overall, but work documents are inaccessible.
- The user is unable to open them with the usual software. Victims may also be asked to contact a fake technician.

How can you protect yourself?

- Do not click on a link or open a file of unknown origin in an email or text message. Request assistance from a dedicated technician (if required) and avoid contacting "online technicians."
- Regularly install updates of your computer's operating system: most ransomware takes advantage of flaws that can be avoided.
- Use a complete security solution offering protection against ransomware, spam and Web navigation.
- Secure your remote desktop services: use secure remote access services such as a virtual private network (VPN), which requires double authentication and strong passwords (fees apply).
- Limit the use of administrator accounts on your operating system.
- Implement a backup procedure: the backup frequency depends on the nature and value of the data. Also, ensure backups are stored outside the shared network.
- Raise awareness of other users of the network if it is shared (e.g., family using the same Wi-Fi at home).

What should you do if you are a victim or ransomware?

- Do not pay the ransom. Paying the ransom does not guarantee that you will recover your data and encourages the attacker to strike again.
- Contact local police.

ROMANCE SCAM

What is it?

In a romance scam, the scammer contacts his or her victim through social media or dating sites. Using seduction techniques (flattery, compliments), the scammer builds trust with the victim and reveals romantic feelings for them. Once the virtual relationship is established, the scammer fakes financial problems to get the victim to send him or her money.

What do fraudsters do?

- Create fake profiles on social media or online dating sites and show an interest in developing a "serious" relationship.
- Patiently build the "relationship."
- Pretend to need money for reasons such as a trip to visit you or to visit a sick or dying parent or child, various fees related to hospital fees, customs issues, further to a job loss or financial difficulties.
- Contact their victim again to ask forgiveness (following a fraudulent transaction), reiterate their feelings and try to get more money from their victim using a new strategy.

How can you protect yourself?

- Be careful and skeptical on dating sites and social media.
- Do not accept friend requests from people who you do not know.
- Never send money to someone you only know virtually. Refuse any transaction for a third party.
- Never share your banking information.
- Do not share explicit photos or videos.
- Keep fraudulent identities on file to report them, if necessary.

When in doubt, talk to someone you trust.

TO GET HELP OR REPORT FRAUD

If you suspect or know that you have been a victim of a romance scam, report the incident to:

- your financial institution
- your local police
- the Canadian Anti-Fraud Centre at **1-888-495-8501**.

NOTES

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: **911**
For municipalities without 911 service: **310-4141** or ***4141** (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**.

To download a copy of *Fraud in 3D*:
http://www.bankofcanada.ca/wp-content/uploads/2019/01/fraud-3d.pdf

March 2019