



Protect yourself from Identity Theft



Your guide to Identity Theft: how to identify it, protect yourself, and what to do if it happens





Recognizing identity theft and scams

Bank with confidence, no matter where you are. We're committed to keeping you and your banking information safe. Discover how you can keep your information safe and protect yourself from being a victim of identity theft and scams.

What is identity theft?

Identity theft is the deliberate use of someone else's identity and personal information illegally for financial gain.

How can criminals steal my identity?

-  Calls from people impersonating financial institutions, government agencies and other legitimate companies, requesting personal/banking information
-  Fake emails that appear to be from a legitimate enterprise, requesting personal or banking information
-  Text messages prompting you to open a link requesting personal or banking information
-  Smartphone and computer device risks (malware)

What is a scam?

Scams are schemes perpetrated by individuals to illegally obtain money or information, often by tricking the victim into giving them up.

Know the signs of a scam

- ! Unusual prize offers that sound too good to be true
- ! Suspicious and unexpected messages or calls asking you to conduct financial transactions
- ! Receiving a payment in advance for a job application you recently applied for
- ! Requests to send payments via wire transfers, gift cards, prepaid cards, Bitcoin and other cryptocurrency

Common types of scams

Phishing, smishing, and vishing scams

What: An attempt by fraudsters to trick you into revealing personal or banking information through unsolicited contact via emails (phishing), text messages (smishing), or telephone/voicemail calls (vishing)

Example: An email or text message that states you won a contest or prize and prompts you to click on the attached link; a call from someone claiming to be from a government agency or financial institution demanding immediate payment or personal information with extreme consequences for non-compliance

Detection: Urgent requests to send money to a third party, misspelled messages and email addresses, requests for personal information, suspicious links with an unusual combination of letters and numbers

Subscriber Identification Module jacking and porting fraud

What: A form of identity theft where a fraudster can obtain a duplicate of your SIM card and be able to receive all of your calls and text messages, (SIM jacking), or obtain your personal information to transfer your phone number from one service provider to another (number porting)

Example: A fraudster contacts your wireless carrier and convinces them to switch the SIM card linked to your phone number with a SIM card in the fraudster's possession, using your personal data

Detection: Unauthorized password changes or logins to your bank, email and social media accounts, a notification from your cell phone provider that your SIM card or number has been activated on another device

Malware scams

What: Malicious software secretly installed onto a computer that is designed to disrupt, damage, or gain unauthorized access to a computer system

Example: Malicious software installed on your computer with the threat to publish your personal data or restrict access to it indefinitely unless a ransom is paid (ransomware)

Detection: Requests to install software, divulge personal information or click on a link

Protecting yourself from identity theft

We would like to remind you that you must immediately report any actual or suspected fraud and unauthorized activity on your accounts and debit and credit cards, the loss or theft of cards, and if your card details or PINs are compromised. You must immediately replace your debit card or credit card and change your PINs and banking passwords.

Follow the safeguards below to protect your personal and banking information from being compromised.

How can I protect myself?

- ✓ **DO:** Create difficult and unique passwords for each of your accounts (i.e. email, banking, social media)
- ✓ **DO:** Set up “My Alerts” on CIBC Online and Mobile Banking to inform you of any unauthorized transactions
- ✓ **DO:** Install up-to-date antivirus software on your PC to detect and remove malware
- ✓ **DO:** Enroll in Interac e-Transfer® Autodeposit to have funds automatically deposited in your account
- ✓ **DO:** Contact your mobile service provider to learn more about port protection to avoid having your mobile device and SIM compromised

- ✗ **DO NOT:** Give out your personal passwords
- ✗ **DO NOT:** Respond to unsolicited emails or SMS messages, and ignore requests to click on embedded links
- ✗ **DO NOT:** Use your personal or banking information when creating unique passwords or e-transfer security question answers (i.e. SIN, date of birth, home address, card numbers, etc.)
- ✗ **DO NOT:** Respond to any online pop-up windows requesting personal or banking information
- ✗ **DO NOT:** Reuse the same security question answer for multiple e-transfer recipients, or share that answer through social media/email
- ✗ **DO NOT:** Save login credentials on any of your electronic devices

Interac e-Transfer® is a registered trademark of Interac Corp., used under license.

What can I do if I'm a victim?

Follow the steps below immediately to avoid further losses and being a repeat victim:

- 1 Review all of your products** (e.g. Chequing and savings accounts, credit cards, etc.) to identify any unauthorized activity.
- 2 Replace compromised accounts quickly** at a CIBC Banking Centre or by calling the number on the back of your card.
- 3 Validate personal information** (e.g. address, email, and phone numbers) for accuracy at any CIBC Banking Centre (two pieces of government issued ID required) or by calling our Telephone Banking service.
- 4 Reset/set up a verbal password** with Telephone Banking on your new credit card(s), and a 3-digit PIN on your debit card by calling the number on the back of your card.

Additional steps

- 5 Contact credit reporting agencies** to request a fraud alert be placed on your file. This will notify companies not to issue credit to anyone applying under your name without verification.
- 6 Install reputable antivirus software** on your computer and run full scans regularly to remove any viruses.
- 7 Change passwords**, including your online banking password and email address passwords on a **clean** device (i.e. a device free of malicious software).
- 8 Check email and telephone** message forwarding and redirection settings to ensure there are no rules set that were not made by you.
- 9 Contact your mobile service provider immediately** if you cannot place calls or texts, or if you've been notified that your phone number has been activated on another device.

Don't let cybercriminals get away with it

More questions?

For more information on how to protect yourself, visit www.cibc.com/fraud

If you believe there is suspicious activity on your account(s) please visit your nearest CIBC Banking Centre immediately, or contact us at:

| | | | |
|-----------------------|----------------|------------------------------|----------------|
| CIBC Everyday Banking | 1 888 872-2422 | CIBC Investor's Edge and IIS | 1 800 567-3343 |
| CIBC Credit Cards | 1 800 465-4653 | CIBC Wood Gundy | 1 800 563-3193 |

