Protect yourself from Identity Theft

How to identify it, protect yourself, and what to do when it happens

Recognizing identity theft and scams

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 you.

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
- Advance payments for a job application
- Requests to send payments via wire transfers, gift cards, prepaid cards, Bitcoin and other cryptocurrency

Common 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)

How to spot: 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

SIM jacking and porting fraud

What: A form of identity theft where a fraudster can obtain a duplicate of your SIM card 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)

How to spot: Unauthorized password changes or logins to your bank, email and social media accounts, or 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 to disrupt, damage, or gain unauthorized access to a computer system

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

Protecting yourself from identity theft

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 "SecurLock alerts" to inform you of any unauthorized transactions
- ✓ **DO:** Install up-to-date antivirus software on your PC to detect and remove malware
- ✓ **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 or one-time verification codes to anyone
- ✗ **DO NOT:** Respond to unsolicited emails or text messages, and ignore requests to click on embedded links
- ✗ **DO NOT:** Use your personal or banking information when creating unique passwords
- ✗ **DO NOT:** Respond to any online pop-up windows requesting personal or banking information
- ✗ **DO NOT:** Save login credentials on any of your electronic devices

What can I do if I'm a victim?

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

1. **Report fraud to us immediately** so we can replace your debit card. We urge you to change your banking password and PIN.
2. **Review all of your products** (e.g. Checking and savings accounts, debit cards, etc.) to identify any unauthorized activity.
3. **Protect compromised accounts quickly** by calling the Client Support Center at 877-448-6500.
4. **Validate personal information** (e.g. address, email, and phone numbers) for accuracy at any CIBC Banking Center or by calling the Client Support Center at 877-448-6500.

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 us.cibc.com/fraudprevention