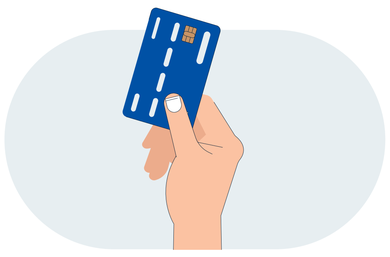
Bank Impersonation Scams

A bank impersonation scam involves you being contacted by a scammer pretending to be a legitimate bank employee.

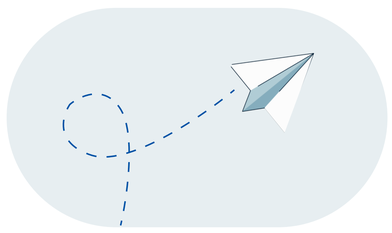
Scammers will try to trick you in various ways to obtain account information or complete unauthorized transactions.

Read more to learn how to spot red flags, understand what RBC will NEVER ask, and how to protect your information.

Beware of Red Flags



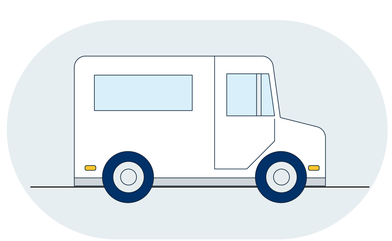
You receive a call, email or text message asking for your card information, password(s), one-time passcode, e-transfer reference number or other sensitive details.



You are asked to complete actions to 'secure your profile', such as:

- Send a transfer to 'RBC'
- Send yourself funds
- And/or initiate any other type of transaction

When a caller prolongs conversations, utilize misdirection, and create a false sense of urgency to pressure you in completing their request and releasing sensitive information.



You receive a call asking you to place your debit or credit card in an envelope with your PIN and/or password details and are told to place it somewhere or give it to a 'courier' company representative that will come to your location to pick it up.

You have received a call from RBC regarding unauthorized transactions, but when you call the number on the back of your card, you are advised there are no notes or indicators in our systems to support this.

What RBC will <u>never</u> ask you to:

- ✕ Initiate any type of transaction on RBC's behalf.
- ✕ Provide one-time codes sent through SMS, emails, or voicemail to identify yourself over the phone or in person.
- ✕ Download a remote access application.
- ✕ Disclose your PIN.
- ✕ e-Transfer money for any reason.
- ✕ Perform any digital two-step authentication for outbound calls, including One Time Passcode, ID verification or PIN verification.
- ✕ Create a new online banking password with the Advisor or ask to share your password with anyone.

Ways to keep yourself safe

- ☐ If you receive a suspicious call, hang up immediately and contact RBC at the number on the back of your card.
- ☐ Do not click on any link or provide any information if you cannot confirm with certitude who is contacting you.
- ☐ Report suspicious texts to your telecommunications company by forwarding the message to 7726 on your mobile device.
- ☐ Utilize the self-serve locking feature via Mobile Banking and Online Banking to secure your card(s) until you reach RBC.
- ☐ Treat unsolicited communication by phone, email, or social media with caution. It is likely not legitimate.
- ☐ Take time to research any offers or what you're being told. Never let someone rush you into making a decision or into releasing information or acting immediately.
- ☐ Regularly review RBC's Scam Alerts at www.rbc.com/cyber/alerts.

RBC Be Cyber Aware
rbc.com/cyber