RBC Commercial Banking

Bank Impersonation Scams

How to protect your business

What is an impersonation scam?

Impersonation scams often begin with a call, text or email where a scammer poses as a trusted individual or organization. Scammers may impersonate figures of authority, such as police officers, lawyers, government employees, or a legitimate company or business, by posing as a representative of that organization. Regardless of the scheme, scammers have a specific goal in mind, which is to gain business, confidential and sensitive information, all with the purpose of ultimately stealing funds.

Bank impersonation scams continue to be one of the most prevalent types of impersonation scams. Scammers often pose as bank employees by initiating a request or conversation with the goal of obtaining your company's banking details, and access to your account(s) and/or money.

Common bank impersonation scenarios

Businesses should familiarize themselves with common bank impersonation scam scenarios to recognize how scammers may attempt to steal your business's confidential and financial information, and ultimately funds.

Desktop Sharing App

Scammers will call and request that the staff member (victim) download a desktop sharing app. The victim may then be redirected to a fraudulent website or asked to initiate a chat through a fake support mechanism. After sign-in, the scammer will prevent the victim from viewing the screen while they complete fraudulent transactions in the active session. The scammer will often request token values from the victim, falsely advising that token information is required to resolve a fraud occurrence on the account. Sharing the token with the scammer allows fraudulent transactions to be processed.

Fraud or Security Department Impersonation

Scammers may refer to themselves as RBC's fraud or security department. They will advise that the account or profile has been compromised, and steps must be taken in order to secure it. As a result, they may ask staff to complete transactions or ask them to forward a notification email or text message, which is then used to intercept a legitimate transfer and steal funds.

RBC Ideas Happen Here™

(05/2026)

Red flags

- A call, email or text message asking for card information, password(s), e-Transfer reference number or other sensitive information.
- A request to provide a one-time passcode in order to identify the staff member.
- A request to complete actions to “secure your profile”, including sending a transfer to “RBC” or a business account, and/or initiating another type of transaction.
- A request to download a remote access application.
- A call, email, or text message with minor differences in email addresses, spelling errors within the communication, or phone calls from an unfamiliar phone number.
- A caller prolongs the conversation, utilizes misdirection, and creates a false sense of urgency to pressure staff into completing their request and sharing sensitive information.

Ways businesses can protect themselves

- If your staff receive a suspicious call, they should hang up immediately and contact RBC at the number on the back of their card or contact their relationship manager.
- Do not share token information or other sensitive details.
- Do not click on links or provide any information if you cannot confirm with certainty who is contacting you.
- Implement strong verification procedures – verify requests before taking any action, especially those involving confidential or sensitive information.
- Regularly issue and install updates on every device on your network to eliminate vulnerabilities that may be known to criminals.
- Report suspicious texts to telecommunications companies by forwarding suspicious messages to 7726 from the mobile devices on which they were received.
- Report suspicious emails that appear to be from RBC to phishing@rbc.com.

Stop

Scammers try to gain trust and pressure staff into taking action by pretending to be the business’s bank. Stay alert for any unusual requests.

Check

Staff should hang up and call the number on the back of the credit card or log into the business’s online banking to verify if the bank tried to reach out.

Talk

Share the experience with other staff members. The more people become aware of schemes scammers are using, the less likely they are to fall victim.

For more information on cyber security best practices, visit rbc.com/cyber

Ideas Happen Here™

(03/2026)