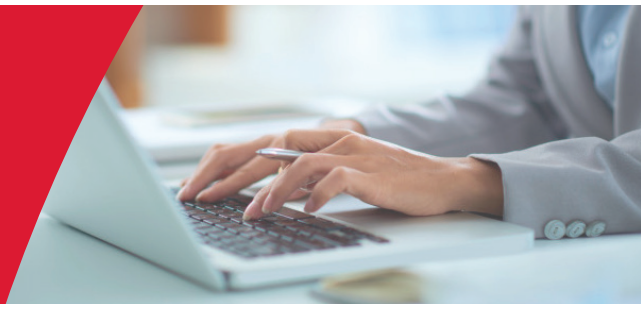
Staying Safe From Business Email Compromise Scams



One of the most common scams is Business Email Compromise (BEC). This sophisticated scam tricks employees at all levels into sending money, sharing data and granting access to fraudsters. Don't be a victim of fraud. Use this guide to learn how to stay safe.

BUSINESS EMAIL COMPROMISE SCAMS

Stay informed about BEC scams so you can avoid them.

1

CEO fraud

"It's urgent. Wire the funds right away"

Scammers contact you by email posing as the CEO or other senior-level executive. They claim to need money for a business opportunity, emergency or another urgent matter. They ask you to wire funds immediately to an unfamiliar account.

2

Vendor Email Compromise

"Here's your invoice for our recent work"

Fraudsters hack into a vendor's email system and send you an invoice. It looks legitimate but the account number is different. If you pay that invoice, that money will go straight to the scammer.

3

Beneficiary change

"Send payment to our new account"

You get an email that looks like it's from your supplier – but it's actually from a fraudster. They tell you their banking information has changed and ask you to send payments to a different account.

4

Data Theft

"Please send me my tax statements"

Cybercriminals often target businesses in order to get employee tax statements or other Personally Identifiable Information (PII). Fraudsters use PII data in future attacks like phishing attempts, CEO impersonations or to create fake invoices and accounts.

RED FLAGS

If you notice any of these warning signs, be on guard. You may be dealing with a scammer.

Something doesn't look right

- **Minor changes** in the email address or domain name.
- **Differences** in the invoice, letterhead, fax or email template.
- **Unfamiliar supplier** or vendor.
- **Altered beneficiary** and transaction information.
- **Poor grammar** or spelling.

Something doesn't sound right

- Strong sense of urgency, ***"You must act immediately."***
- Demand for secrecy, ***"Keep the payment details confidential."***
- Communication challenges, ***"I can't talk, I can only email."***
- Contact information that's different from what you have on file.
- A desire to skip regular approval processes.

WANT TO LEARN MORE?

Fend Off Fraud

Discover how to prevent cheque and credit card fraud.

Get Cyber Safe

Find out about cyber safety at home and work.

Canadian Anti-Fraud Centre

Stay on top of the latest frauds so you can avoid them.

PREVENT IT

Don't become a victim. Use these simple actions to help keep your company safe from scammers.

1

Before you act on the request

- **Stop and think** about what you've been asked to do. Does it seem unusual in any way?
- **Pick up the phone and call someone** you know to verify an unusual request.
- **Talk to your manager** about your concerns.
- **Get in touch with a known contact** to confirm banking changes in writing.
- Remember, **Scotiabank will never ask you for passwords**, token values, or other confidential information.

2

Establish and follow policies and procedures

- **Have payments approved** by more than one person.
- Regularly **review and reconcile transactions logs** and payment reports.
- Keep an up-to-date and **detailed supplier/payee directory** and use it frequently.
- **Create a process** to recall a payment that may be fraudulent.

Scotiabank®