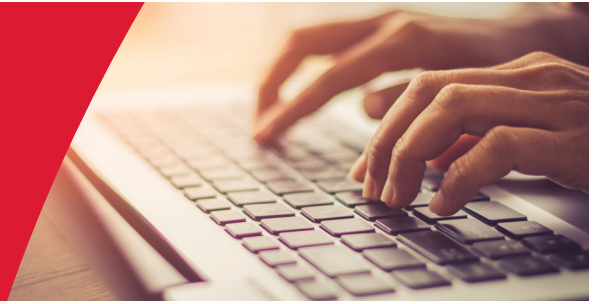


# *Interac e-Transfer*<sup>†</sup> for Business Fraud Guide



## *INTERAC E-TRANSFER*<sup>†</sup> FOR BUSINESS CAN HELP PROTECT YOU FROM FRAUD

These days, it's more important than ever to protect your business from fraud. *Interac e-Transfer*<sup>†</sup> for Business can help - it's one of the safest ways to send and receive funds.

### ***Interac e-Transfer*<sup>†</sup> Security Messaging**

When you send a payment\*, the recipient gets a notification delivered to their email address. Money never actually travels by email - only notifications and deposit instructions do. To protect your funds *Interac* and Scotiabank use multiple layers of security:

- Your data is encrypted for added protection.
- Added security with multi-factor authentication and multiple levels of risk control.
- Unusual transactions and payments are monitored, preventing potential fraud losses before they happen.

### **Accept payments and stay protected**

With a unique security feature *Interac e-Transfer*<sup>†</sup> allows you to accept funds and safeguard your account:

**Autodeposit:** For easy, fast and more secure transactions, payments are automatically delivered to the account associated with the email address reducing the risk of having a criminal guess your password and access your funds.

## RECEIVE PAYMENTS SAFELY WITH THESE SIMPLE TIPS

### RECOGNIZE FRAUD

- 1 **Stop**  
Take a moment to stop, think and follow your instincts. Whether it's a transfer you weren't expecting, or an email asking for your personal information, use caution. You should never feel rushed to respond when working with a trusted organization.
- 2 **Scrutinize**  
Assess the situation before you click. Phishing emails often contain a sender's email address that does not match the website of the organization. Be suspicious of unknown links and always hover over links with your cursor to see the final destination.

### REJECT FRAUD

- 3 **Speak up**  
Confirm the validity of the email and report any concerns. If you suspect fraud, contact the sender of the communication through a different channel.

### REPORT FRAUD

- 4 **Contact Scotiabank immediately**  
If you've accidentally provided personal information or clicked a suspicious link, call us right away at 1 (800) 265-5613. Don't wait until the next business day. The sooner we know, the more effective we can be in helping you reduce the damage. Forward the fraudulent email to [phishing@scotiabank.com](mailto:phishing@scotiabank.com). Do not change or retype the subject line.
- 5 **Tell the authorities**  
Contact your local police and the [Canadian Anti-Fraud Centre](#) to report the fraud or call 1-888-495-8501.

### WANT TO LEARN MORE?

#### [Canadian Anti-Fraud Centre](#)

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

#### [Interac e-Transfer<sup>†</sup> Security](#)

Discover why *Interac e-Transfer<sup>†</sup>* is the secure way to send and receive funds.

#### [Payment Fraud](#)

Protect Your Business from COVID-19 payment fraud.