simplii FINANCIAL

Protect yourself from *Interac* e-Transfer® fraud

E-transfer interception fraud occurs when money is being sent via *Interac* e-Transfer® from one's bank account to another's through the use of an email address or phone number. Fraudsters will intercept the online transaction and divert the money to a different bank account.

How to protect yourself

Fraudsters are able to intercept *Interac* e-Transfers by gaining access to the recipient's email account and guessing or obtaining the security question answer. Whether you are the sender or recipient of an *Interac* e-Transfer, everyone is responsible for playing their part in preventing fraud.

As the sender:

- ✓ **DO:** Create difficult and unique security questions that only you and the recipient will know
- ✓ **DO:** If necessary, only share the security question answer with the recipient over a secure method of communication (phone)

- ✗ **DO NOT:** Include the security answer in your question
- ✗ **DO NOT:** Share your security question answer over email, text or social media
- ✗ **DO NOT:** Reuse the same security question answer for multiple recipients

As the recipient:

- ✓ **DO:** Enroll in *Interac* e-Transfer Autodeposit to have funds automatically deposited without answering a security question
- ✓ **DO:** Create difficult and unique passwords to protect your accounts (email, social media)

- ✗ **DO NOT:** Create account passwords that are easy to guess by anyone
- ✗ **DO NOT:** Share your passwords with anyone
- ✗ **DO NOT:** Suggest multiple senders use the same security question answer

ⓘ Want to learn more? Visit **simplii.com/stoppingfraud**