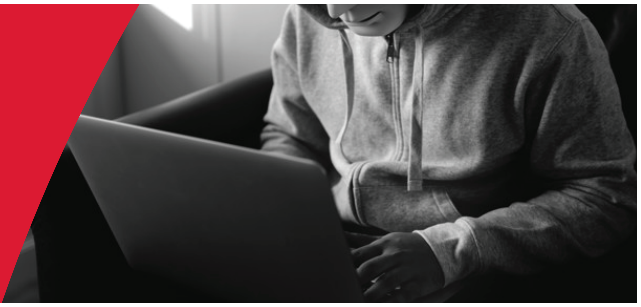
Preventing Fraud



BE PROACTIVE: TOP TIPS TO HELP PREVENT FRAUD

Every day fraudsters use all kinds of strategies, technologies and techniques to try and steal from businesses of all sizes. These four simple tips can help keep your business safe.

RECOGNIZE FRAUD

1

Notice the unusual

If you receive a suspicious request or unexpected email from an employee, vendor or business partner – **be very cautious**. The sender may not be who you think. They may be impersonating, or *spoofing*, someone else. Before you act on an unusual request, take the time to look for potential red flags such as, urgent demands and emails with unexpected links or attachments.

2

Know who you're talking to

Sometimes fraudsters pretend they are your CEO or a trusted supplier and will request funds or confidential information. Before you send a wire transfer, change account information or divulge confidential details, ensure the receiver is **someone you actually know and trust**. Always contact the sender directly by phone, using contact information from your records.

3

Educate your employees

Ensure your employees know how to keep the business safe from fraud:

- Teach your employees how to recognize, reject and report fraud.
- Develop security policies which employees can understand and follow.
- Ensure employees use passwords that are complex, hard-to-guess and unique. They **should never re-use passwords**.

4

Protect your systems

Securing your systems can help your business stay safe. Be sure to:

- Scan your systems for viruses and malware, and remove any malicious software.
- Keep anti-virus and firewall software up to date.
- Use two-factor authentication whenever possible.

REJECT FRAUD

Use these simple actions to help keep your company safe from fraudsters.

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.

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.

WANT TO LEARN MORE?

Stay Safe From Fraud

Learn more about email and phone 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.

Fend Off Fraud

Discover how to prevent cheque and credit card fraud.

REPORT FRAUD

- **Contact Scotiabank immediately:** Don’t wait until the next business day. Call us right away at 1 (800) 265-5613. The sooner we know, the more effective we can be in helping you reduce the damage.
- **Forward suspicious emails that appear to be from Scotiabank** to phishing@scotiabank.com.
- **Tell the authorities:** Contact your local police and the Canadian Anti-Fraud Centre to report the crime.

Scotiabank®