

Fraud prevention starts with you.

Tips to help protect your business.



Ready
for you



Recognizing and Preventing Fraud

How secure is your company?

No matter what type of business you're in, the risk of fraud is present and always evolving.

Fraud Facts

- Weaknesses in internal controls are responsible for nearly half of all employee thefts/frauds¹
- Over 80% of businesses reported being targets of payment fraud in 2018²
- While cheques remain the most frequent source of payment fraud, Business Email Compromise (BEC) scams are on the rise. The percentage of organizations being targeted by such scams has increased from 64% in 2014 to 80% in 2018².

¹2018 Report to the Nations. Association of Certified Fraud Examiners.

²2019 AFP Payments Fraud and Control Survey, Association for Financial Professionals.

Stay vigilant and guard your information.

TD Bank will not ask you to provide personal information or login information such as Connect IDs, passwords, authentication token codes or account numbers either by phone or by email.

Common Electronic Fraud Schemes:

■ Phishing/Smishing/Vishing:

An authentic looking email/text message/ phone call that appears to come from a legitimate company and asks the recipient to: validate their account, confirm suspicious activity, prevent their account from being suspended etc. Typically, a link or document is included in the email/text that directs recipients to a fake website where they are asked to provide their login credentials or other confidential information. Do not open attachments or click on links in emails from unknown senders.

■ **Business email compromise:** An email that impersonates a source known to the recipient (CEO, Finance Director, supplier etc.). Such emails will often request that a wire or EFT payment be made or may provide new instructions/account numbers for an existing payment. As email impersonation is relatively easy, you should always confirm payment instructions in person or by phone via existing phone numbers you have on file.

■ **Malware:** Malicious software used to disrupt computer operations, gather sensitive information or access computer systems. Malware may be hidden in an attachment or macro in an email that a user has opened and clicked on.

■ **Ransomware:** Type of malware that infects computers, encrypting files and data until the victim pays a ransom.

While you can't predict when or why your organization may become a target, there is a lot you can do to reduce the opportunity for fraud.

Fraud Prevention Best Practices

There are several best practices designed to protect your financial transactions and reduce the risks associated with fraud. Review these tips and implement them as part of your everyday fraud prevention plan. **Remove the opportunity for fraud and you have gone a long way towards preventing it.**

Online Safety Checklist



Banking

Ensuring the security of our customers' information is paramount for TD. Do not share your confidential login credentials for any online banking platform with anyone. **TD Bank Group will not ask you to provide personal, login or account information through emails or phone calls.**



- Review and implement the security features available for TD's products and services, including those that enable the separation of duties, dual authentication, and enhance administration and control.
- Always enter the address of any banking website. Do not use links embedded in emails, pop-up windows or search engines.
- Set individual user limits for your payments that are appropriate for each user.
- Make sure your browser is securely connecting to all online banking sites using HTTPS protocols (i.e., "https://") must be in the address). This encrypts information passed between your computer and the banking website.
- Never access banking websites using public or shared computers as they may contain unauthorized software.
- Do not use public Wi-Fi networks when accessing online banking as public Wi-Fi connections are unsecure.
- Pay attention to the appearance of online banking screens. If they are not consistent with what you are familiar with, this could mean your browser has been compromised. Stop your transaction immediately and report your concerns to TD.
- Log off when you've finished your banking or if leaving your computer unattended. Use a stand-alone, locked down computer system reserved exclusively for your online banking, where email and web browsing are not possible.
- Use caution when visiting other websites from the same computer as you conduct your banking because malware can be downloaded without your knowledge from unsafe websites.

Computers

- Install a firewall to protect your computer from hackers.
- Use only legally licensed software and keep it current with the latest updates.
- Use the most up-to-date commercially available antivirus software. Free software may not protect against the latest threats.
- Choose unique passwords that include a combination of letters, numbers and symbols.
- Do not use the same passwords for personal and work applications.
- Ensure that autocomplete password functions on your browser are disabled.
- Never save passwords on your computer, the internet or on any software.



Email

- Do not include banking information in an email to TD or anyone else unless it is encrypted.
- Do not open file attachments in emails from unknown senders.
- Do not use links in an email to go to any web page. If you suspect the message might not be authentic, call to verify it or type in the web address directly in your browser.
- Be suspicious of emails that appear to be from a trusted sender (such as a bank or government agency) that instruct you to provide account information or verification, or banking access credentials such as Connect ID, password and authentication token codes via a hyperlink. Report any suspicious emails immediately to TD at phishing@TD.com.
- If you believe you've responded to a suspicious email and have shared your online banking login credentials, please report the incident immediately:
 - For Web Business Banking call the CMS Support Desk at 1-800-668-7328
 - For EasyWeb call EasyLine at 1-866-222-3456
- Always verify payment instructions by phone or in person even if they appear to be from a known source. Do not act on email instructions as the email could have been fraudulently created.



Cheque Safety Checklist



- **Fraud Protection:** Enroll in a cheque fraud protection service that manages cheque clearing through your Canadian and U.S. dollar accounts.
- **Centralize Cheque Issuing:** Do not leave cheques available to unauthorized staff.
- **Secure Cheques:** Lock up any unissued cheques, cheques scanned for deposit, signature stamps and cheque reorder forms. Audit cheque stock frequently, and without notice.
- **Mail Security:** Avoid mailing cheques in window or see-through envelopes.
- **Use High Quality Cheque Stock:** Use quality cheque stock with MICR encoding and all the latest security features.
- **Bill Payments:** Complete routine bill payments electronically. If you use Web Business Banking, you can reduce risks further by opting for restricted access to bill payments so that payments can only be made to registered payees.
- **Pre-Authorized Payment:** Reduce the number of cheques you issue by allowing creditors to automatically debit your account for recurring payments.
- **Credit Cards:** Make credit card payments where possible to reduce the use of cheques.
- **Payroll Cheques:** Link your in-house computer payroll software to an Electronic Funds Transfer (EFT) service to provide direct deposit to employee accounts. Alternatively, ask us about payroll service providers that can handle the entire payroll and direct deposit function for your business.
- **Bank Drafts:** Replace bank drafts with wire payments.

Deposit Security Checklist



- **Lockboxes:** If you collect many payments by cheque, consider subscribing to a bank-operated lockbox to centralize and automate the collection of receivables.
- **Returned Items:** Use endorsement stamps that clearly direct returned items to the account of your choice. Cheques deposited through Remote Deposit Capture (RDC) include a virtual endorsement, imaged on the back of the cheque.
- **Payment Cards:** If you accept credit or debit cards from customers, train employees to recognize suspicious behaviour or transactions. Immediately report any suspicious activity to TD Merchant Solutions at 1-800-363-1163. Also, ensure you are compliant with the Payment Card Industry Data Security Standard (PCI DSS).

Secure Accounting Checklist



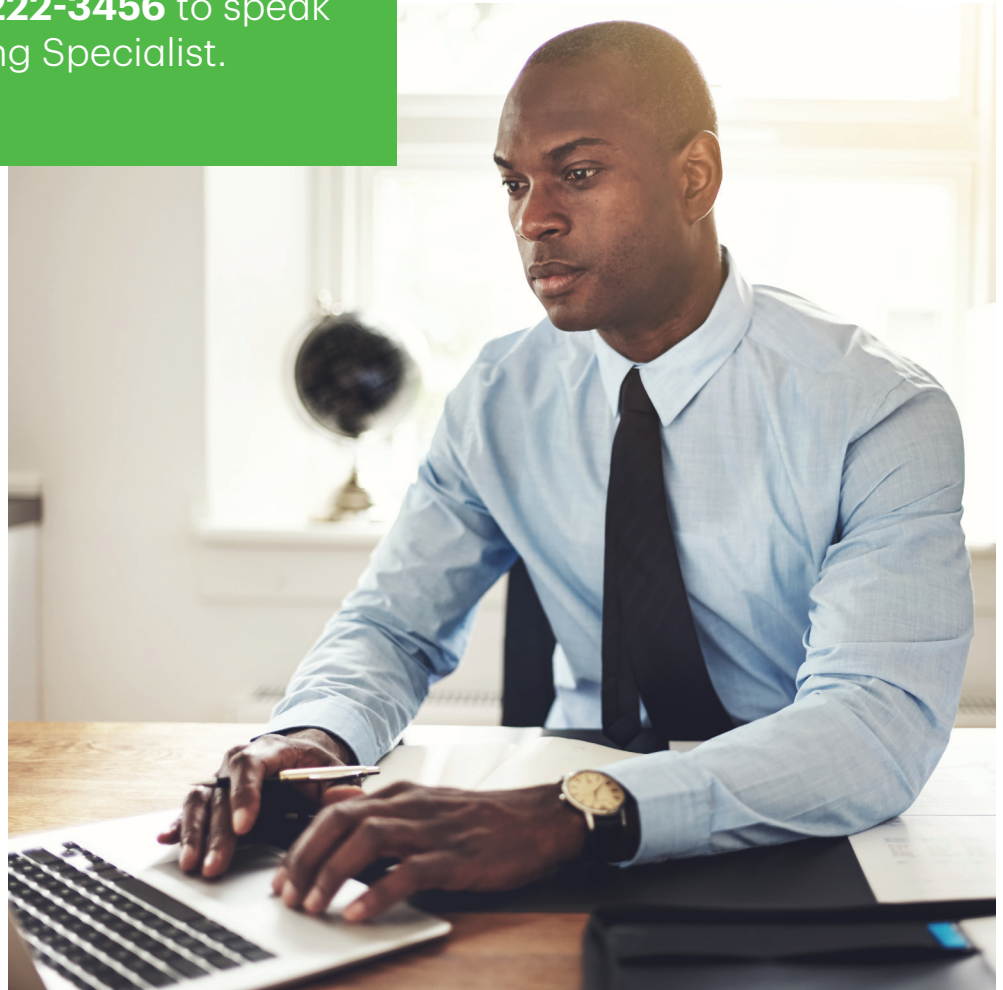
- **Daily Reconciliation:** Reconcile all of your business banking transactions daily and report any unusual transactions immediately.
- **Separate Functions:** Ensure different people are responsible for cheque issuing vs. reconciling the bank statement.
- **Separate Accounts:** Consider opening different accounts to separate such functions as incoming wire transfers and high-volume small-dollar cheques.
- **Security Audit:** Have an accounting professional execute a full audit that includes a complete review of your security procedures.

Need some fraud prevention advice?

We can provide information on our products and services that are available to assist in protecting your company against fraud.

If you are a Commercial Banking or Corporate customer, please contact your Relationship Manager for more information.

If you are a Small Business Banking customer, call **1-866-222-3456** to speak with a Business Banking Specialist.



Ready
for you

