

The Banking Industry Perspective on Cybersecurity

Presented to: Public Policy Forum Conference
“Cybersecurity – Developing a Canadian Strategy”

March 27, 2008



CANADIAN BANKERS ASSOCIATION
ASSOCIATION DES BANQUIERS CANADIENS

What is Cybercrime?

- Any criminal activity performed over on-line channels.
- From a banking industry perspective, it is criminal activity performed against the bank or its customers through on-line channels that is intended to steal funds, steal information, or disrupt service.
 - Phishing attacks
 - Malware (e.g. “Silentbanker” virus)
 - Hacking attempts
 - Denial-of-service attacks



Cybersecurity is a Shared Responsibility

- Responsibility for ensuring cybersecurity and combating on-line fraud is shared among:
 - business
 - government
 - the General Public




The Role of the Banking Industry

- The banking industry takes cybersecurity very seriously.
- Cybersecurity in banking happens at three levels:
 - customer level
 - industry level
 - firm level



The Role of the Banking Industry


CIBC. For what matters.

Personal Banking | Business Services | About CIBC

How CIBC Protects You
 Online Banking Guarantee
 Browser Security
 Online Banking Security
 Using Your Information
 CIBC Cookies
 CIBC Privacy Policy

How You Can Protect Yourself
 What You Can Do
 Safe Computing Practices
 Clear Your Browser's Cache

Be Aware of
 Debit Card Skim
 Cheque Fraud
 Identity Fraud
 E-mail Fraud (Phishing)
 Credit Card Fraud
 Accounts Payable
 Moving Money
 Internet Stock
 Spyware

Home > Privacy and Security > Safe Computing Practices

Safe Computing Practices

With CIBC Online Banking, you can manage almost all of your everyday banking, anywhere you have Internet access, using your laptop or a trusted computer terminal. Consider these safe computing practices when conducting your online banking at home or on vacation.

Important tips:

- When you're traveling, use a trusted computer whenever possible
- Never leave your computer unattended once you have signed in to Online Banking
- After completing your transactions, ensure that you sign out of Online Banking and close your browser

TD Canada Trust | Apply | Search | Contact Us | Login to: EasyWeb | Now

My Accounts | Customer Service | Products & Services | Markets & Research | Planning

Overview > Contact Us > Today's Rates > Security > Accessibility

Security

Online Safety & Security

At TD Canada Trust, we're committed to protecting the security of your account information when you bank online. We have extensive security features to ensure that you can conduct your banking in a safe and private online environment.

While we are doing all we can to safeguard your information, there are also important measures you can take to protect yourself when you bank online. Please take the time to read over this valuable security information, and be sure to share it with any friends or family members who also bank online.

How TD Canada Trust protects you

- [Protect your Information](#)
- [Monitor our Computer Systems](#)
- [Use Secure Firewalls and Cookies](#)
- [Offer the EasyWeb Security Guarantee](#)
- [Offer EasyWeb IdentificationPlus](#)
- [Offer you Additional Tools to Protect Yourself](#)

How you can protect yourself

- [Protect yourself from Online Fraud](#)
- [Protect your Password](#)
- [Use a Firewall](#)
- [Use Anti-Virus and Anti-Spyware Software](#)
- [Ensure your Browser and Operating System](#)

RBC.com | Search | Site Map | Contact Us | Legal Terms | Français

Other RBC Sites: Banking | Investments | Insurance | Capital Markets

Security

Safe Computing Practices

We have taken strong measures to ensure the security of your financial transactions and the confidentiality of your information. It is also important that you take precautions as well to help keep your information safe and secured.

The following safe computing practices are some steps you can take to maximize the security of your online activities:

- ▶ [Anti-Virus Software](#)
- ▶ [Firewalls](#)
- ▶ [Encryption](#)
- ▶ [Passwords](#)
- ▶ [Software Updates](#)
- ▶ [Log-Off](#)

[Learn ways to help you recognize fake websites and e-mail scams](#)

[See our Tips >>](#)

[Learn More](#)
[Safe Computing Practices \(pdf\)](#)



The Role of the Government

- The legal and law enforcement framework needs to treat cybercrime seriously.
 - Legislation to combat identity theft and malicious spam.
 - Resources for law enforcement to go after cyber-criminals.
 - A renewed focus to use these new tools to stop cybercrime.



The Role of the General Public

- The general public is the “soft target” for cyber-criminals.
- Raising awareness among the general public on how to spot and stop cyber-crime is a key to enhancing cybersecurity.
- Both industry and governments have a role to play.



What we Need – A Plan

- Government needs to make cybersecurity a priority, and resource it accordingly.
- Law enforcement needs to take those legislative tools and, using additional resources from governments, pursue cyber-criminals with renewed vigour.
- Industry needs to redouble its efforts to make customers aware of safe computing practices and work together to keep a step ahead of the cybercriminals.





Thank You