

*NSPW Presentation - Sep 19, 2007*

# **Security and Usability: The Gap in Real-World Online Banking**

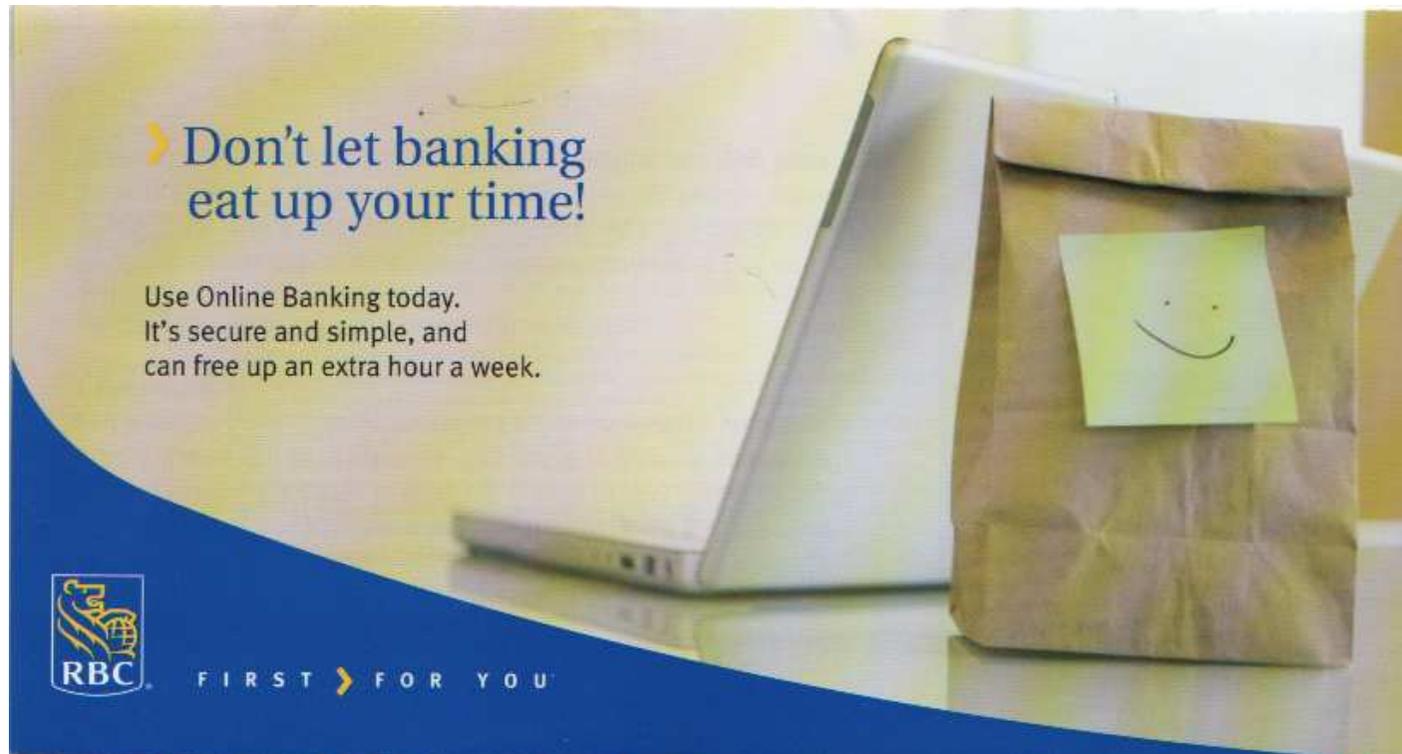
Mohammad Mannan and P. C. van Oorschot

Carleton University

## **Large Canadian banks**

- ▣▶ RBC Royal Bank
- ▣▶ Canadian Imperial Bank of Commerce (CIBC)
- ▣▶ TD Canada Trust
- ▣▶ Scotiabank
- ▣▶ Bank of Montreal (BMO)
- ▣▶ President's Choice (PC) Financial

## Why bank online?



58% of Internet-connected Canadians used online banking in 2005  
(Statcan, 2006)

## › How valuable is your time?

If you've ever found yourself putting off a trip to the bank, consider this: Online Banking gives you the freedom to bank anytime, from anywhere you have access to the Internet.

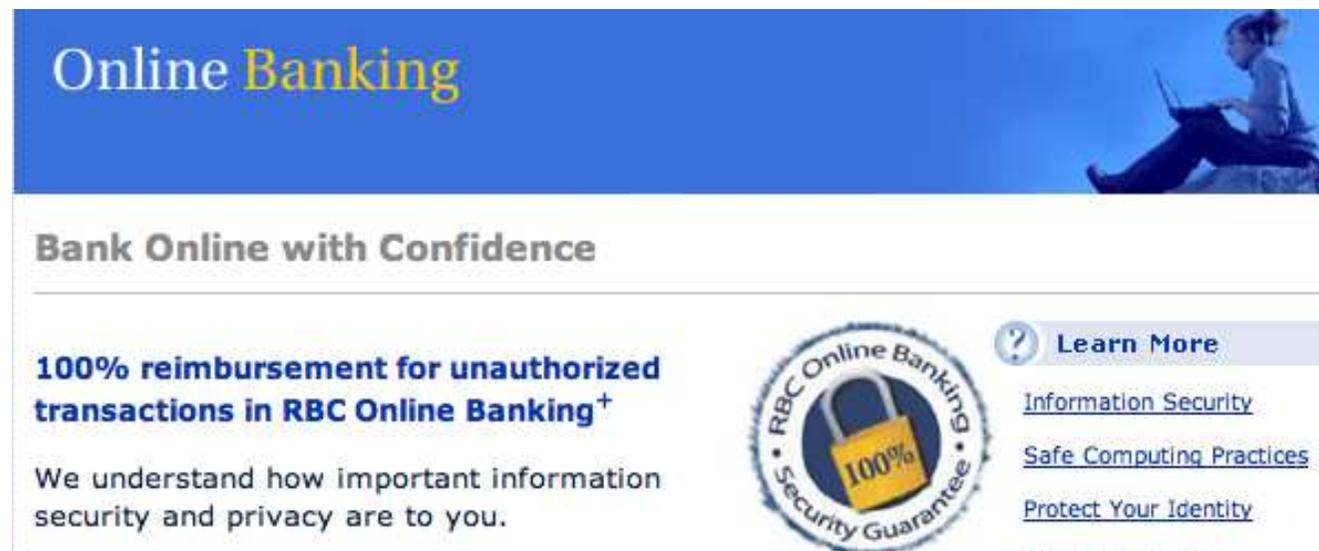
And while we're always happy to serve you in person, Online Banking is a great option when you don't have the time to come in. Simply bank from home or work. You could save as much as an hour a week!

Banking at the branch or ATM 1 HR. 20 MIN.	Online Banking 5 MIN.
› Put on your coat	› Sit down at computer
› Get in the car (or on transit)	› Login
› Drive to branch or ATM	› Enter password
› Park	› Pay bills, transfer funds, check balances – or just about any other transaction
› Chat with the teller	› Enjoy your lunch!
› Make your transactions	
› Drive back to work or home	

Results will vary but you could expect to save at least one hour per week – or four hours per month – with Online Banking

## 100% reimbursement guarantee

- ▣▶ There are risks – but most banks give a 100% reimbursement guarantee on any money lost due to online banking



The screenshot shows the RBC Online Banking website. At the top, it says "Online Banking" in a blue header. Below that, it says "Bank Online with Confidence". The main content area features a large blue box with the text "100% reimbursement for unauthorized transactions in RBC Online Banking<sup>+</sup>". To the right of this text is a circular logo with a padlock and the text "RBC Online Banking Security Guarantee 100%". Below the logo is a "Learn More" button with a question mark icon. Underneath the button are three links: "Information Security", "Safe Computing Practices", and "Protect Your Identity".

Online Banking

Bank Online with Confidence

**100% reimbursement for unauthorized transactions in RBC Online Banking<sup>+</sup>**

We understand how important information security and privacy are to you.

**RBC Online Banking Security Guarantee 100%**

[? Learn More](#)

- [Information Security](#)
- [Safe Computing Practices](#)
- [Protect Your Identity](#)

## So, why worry?

+ For a definition of an unauthorized transaction and for full details regarding the protections and limitations of the RBC Online Banking Security Guarantee, please see your [Electronic Access Agreement](#). This guarantee is given by Royal Bank of Canada in connection with its Online Banking service.

1. The guarantee is conditional
2. Security is a 'shared responsibility'

Can users realistically meet online banking requirements?

## Overview

- ▣▶ Example requirements
- ▣▶ Bank site authentication
- ▣▶ Misleading information
- ▣▶ User survey
- ▣▶ Concluding remarks

## Example requirements: RBC

1. Electronic Access Agreement
  - (a) Sign out, log off, disconnect, close browser
  - (b) Use up-to-date anti-virus, firewall
  
2. “How you can protect yourself”
  - (a) Install all security updates
  - (b) Test your computer for security vulnerabilities
  - (c) Stay aware of the latest security-related issues

## **Anti-malware**

1. Cost: 71.45 USD, per computer, per year for CIBC customers
2. Proper installation and maintenance is difficult
3. Effectiveness is questionable
  - (a) may give a false sense of security
  - (b) targeted by malware

## Anti-malware user study

1. 95% users knew the term 'spyware'
2. 70% use online banking
3. Some believed spyware was 'protecting' their computers

## Check the URL?

1. `https://www.txn.banking.pcfincanial.ca/a/authentication/preSignOn.ams?referid=loginBox_banking_go`

2. One user study reports

▣▣▣▣ 45% users did not look at URLs

▣▣▣▣ 35% noticed `https`, but many didn't know its significance

# wwwcibc.com

**wwwcibc.com - Mozilla Firefox**

File Edit View History Bookmarks Tools Help

http://wwwcibc.com/

**Wwwcibc.com**  
*What you need, when you need it*

November 18, 2006  
[Bookmark this page](#) | [Make this your homepage](#)

**Credit Card Processing** **Credit Check** **Free Credit Report** **Online Payments** **Apply For A Credit Card** **Online Banking** **Personal Finance**

Popular Links
<a href="#">Credit Card Processing</a>
<a href="#">Credit Check</a>
<a href="#">Free Credit Report</a>
<a href="#">Online Payments</a>
<a href="#">Apply For A Credit Card</a>
<a href="#">Online Banking</a>
<a href="#">Personal Finance</a>
<a href="#">Savings Account</a>
<a href="#">Checking Account</a>
<a href="#">Credit Card</a>

Popular Categories		
<a href="#">Credit Card Processing</a>	<a href="#">Credit Check</a>	<a href="#">Free Credit Report</a>
<a href="#">Online Payments</a>	<a href="#">Apply For A Credit Card</a>	<a href="#">Online Banking</a>
<a href="#">Personal Finance</a>	<a href="#">Savings Account</a>	<a href="#">Checking Account</a>
<a href="#">Credit Card</a>	<a href="#">Credit Card Balance</a>	<a href="#">Online Credit Card</a>
<a href="#">Mortgage</a>	<a href="#">Internet Banking</a>	<a href="#">Credit Report</a>
<a href="#">Online Bank</a>	<a href="#">Personal Banking</a>	<a href="#">Cibc Bank</a>

Favorite Categories		
<b>Travel</b> <a href="#">Airline tickets</a> <a href="#">Hotels</a> <a href="#">Car rental</a> <a href="#">Flights</a> <a href="#">South Beach Hotels</a>	<b>Finance</b> <a href="#">Free credit report</a> <a href="#">Online Payment</a> <a href="#">Credit Card Application</a> <a href="#">Car Insurance</a> <a href="#">Health insurance</a>	<b>Home</b> <a href="#">Foreclosures</a> <a href="#">Houses For Sale</a> <a href="#">Mortgage</a> <a href="#">People Search</a> <a href="#">Real Estate Training</a>
<b>Business</b> <a href="#">Employment</a> <a href="#">Work from home</a> <a href="#">Reorder Checks</a> <a href="#">Used Cars</a> <a href="#">Business Opportunities</a>	<b>Entertainment</b> <a href="#">Games</a> <a href="#">Casino</a> <a href="#">Music</a> <a href="#">Cell Phones</a> <a href="#">Ringtones</a>	<b>Lifestyle</b> <a href="#">Dating</a> <a href="#">Christian Singles</a> <a href="#">Jewish Singles</a> <a href="#">Engagement Rings</a> <a href="#">Chat</a>

# wwwcibc.com with a twist

wwwcibc.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://wwwcibc.com/

Contact Us Find Us Français 中文 Site Map Sign On CIBC Website

**CIBC** CIBC. For what matters.

Personal Banking Business Services About CIBC Search Go

**Everyday Banking**  
Chequing & Savings  
VISA Cards  
How to Bank with CIBC  
Kids & Students

**Borrowing**  
Mortgages  
Loans & Lines of Credit

**Investing**  
Mutual Funds  
GICs  
Principal Protected Notes  
Portfolio Programs  
Retirement – RRSPs, RRIFFs  
Education – RESPs  
Self-Directed Brokerage

**Wealth Services**  
CIBC Imperial Service  
CIBC Wood Gundy

The advice you want.  
The solutions you need.™  
Time-limited bonus offer plus new investment solutions.  
[Find out more](#)

**Introducing CIBC CreditSmart™**  
A smart new way to manage your credit card.  
Exclusively from CIBC.  
[Learn more](#)

**Sign On**  
CIBC Online Banking & Investing  
**Sign On** View demo Register now

**Privacy & Security**  
Online Banking Security Guarantee  
How you can protect yourself  
⚠ E-mail fraud alert: November 20

**CIBC Brokerage Sites**  
Select

**Customer Service**  
Apply Online  
How to Bank with CIBC  
Branch hours & ABMs  
Rates

## Check the lock?

Look for the SSL lock icon on the lower-right corner

	Secure	Not Secure
<b>Microsoft Windows:</b>		
Microsoft Internet Explorer		
Netscape Navigator		
Firefox		
<b>Apple MacOS:</b>		
Apple Safari		
Firefox		

## IE7 – where is the lock?



## Embedded SSL lock



The image shows a login form for CIBC Online Banking. At the top left, there is a yellow padlock icon next to the text "Online Banking". To the right of this, there is a link that says "Read our Security Guarantee". Below this, there are two input fields: "Card Number:" followed by a text box, and "Password:" followed by a text box. Under the "Card Number:" field, there is a checkbox and the text "Remember my card number". Under the "Password:" field, there is the text "Case-sensitive" and a link "Forgot your password?". At the bottom of the form, there is a "Note" section with the text: "Note: We've changed the agreement that governs CIBC Online Banking. By signing on, you agree to the new version. Please review the Electronic Access Agreement (2006)". At the bottom right of the form, there is a blue button with the text "Sign On".

# Not big enough?

The screenshot shows the President's Choice Financial website's security page. At the top left is the logo with the tagline "fresh financial thinking". The main navigation bar includes "accounts & products", "PC points", "ways to bank", "helpful stuff", "about us", and "home". A "sign in" section offers "online banking" and "go" buttons, with a link for "Select a password to register" for new users. On the right, there are links for "about security", "forgotten password?", and "sign in help", along with a "now serving Quebec" badge. The page title is "security". A sidebar on the left lists "daily banking", "PC MasterCard", and "PC points", with "quick links" for "legal stuff", "privacy", "cdic deposit insurance information", and "about tied selling". The main content area features a "security" heading, a "peace of mind" icon, and a large image of a padlock. Text on the page states: "With President's Choice Financial® services, your online security is the most important concern. Please select an area below to read more about the security policies for specific products and services." Below this is a list of links: "daily banking", "PC MasterCard", and "PC points". On the right side, there are three orange call-to-action boxes: "why join? what's in it for you", "your guided tour it's easy to bank online apply now sign up and start saving", and "today's great rates the latest and greatest".

## Summarizing SSL certs

1. “This certificate has failed to verify for all of its intended purposes”
  - known bug, the site is actually ‘secure’
2. SSL comments
  - (a) users: a ‘formality’ like an ‘elevator certificate’
  - (b) researchers: ‘indistinguishable from placebo’
  - (c) banks: ‘electronic passport’

“People being too dumb/lazy, though, is the hard problem. Fortunately this is evolution at work.”

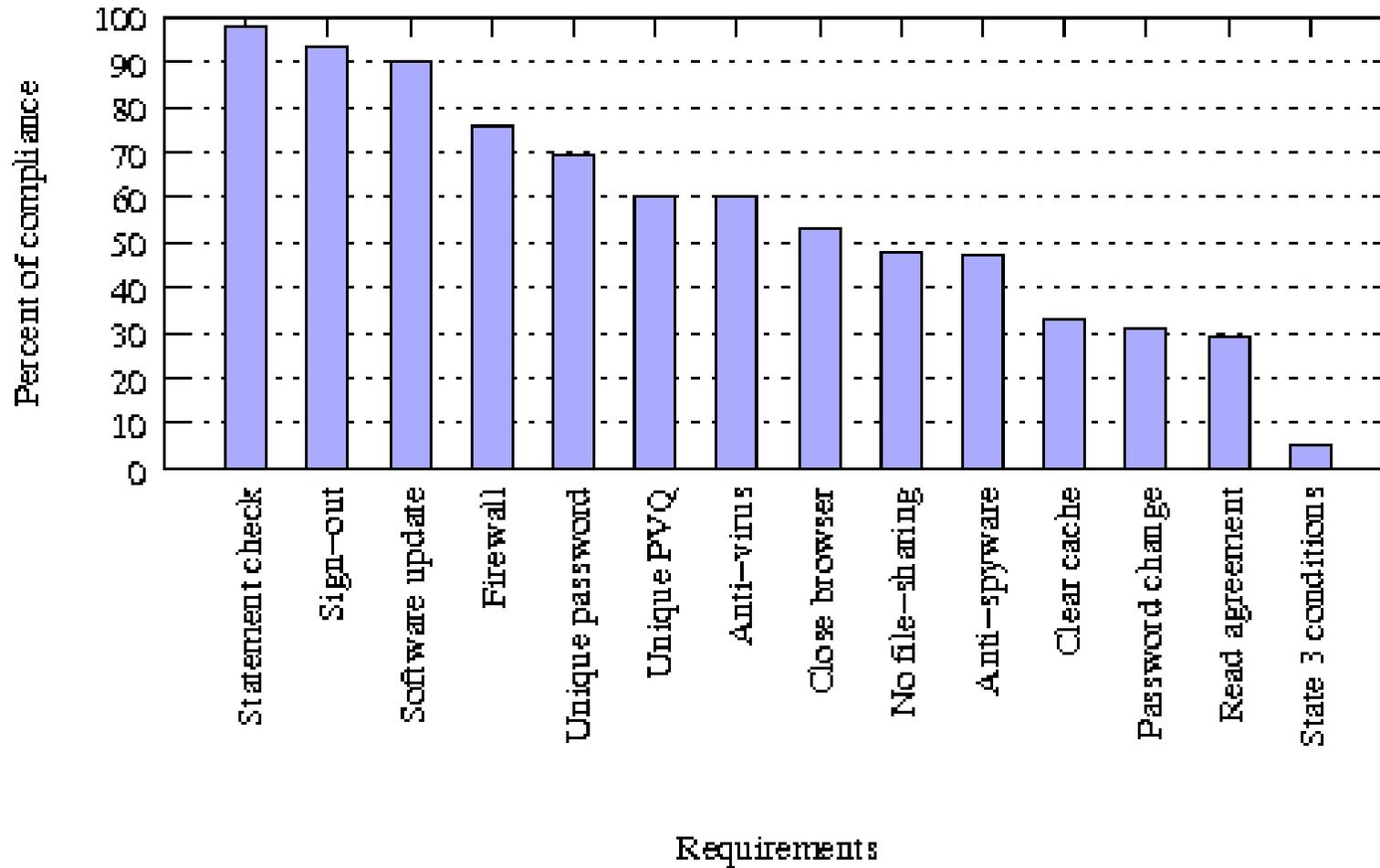
## Misleading information

1. Password advice
  - (a) 'Rock solid' password examples: iwthyh or iw2hyh (Beatles' "I want to hold your hand")
  - (b) '111111', '123456' are not disallowed
2. Safe as in-branch banking?
3. Firewalls "will only allow in the connections that are known and trusted"
4. "... will not undertake to provide a service that compromises the security and confidentiality of customer information"

## User survey

- ▶ 123 users: CS undergrad (3<sup>rd</sup>, 4<sup>th</sup> year) and grad students, post-docs, profs, net admins, security researcher and professionals
  - gives us a best-case scenario

## Result summary



## **Concluding remarks/questions**

1. Apparently users can hardly meet their 'shared' responsibilities
2. What can users do in the face of 'session hijacking' attacks?
3. Who bears the responsibility for security?

“To err is human, to forgive is not bank policy”