NSPW Presentation - Sep 19, 2007

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

Mohammad Mannan and P. C. van Oorschot

Carleton University

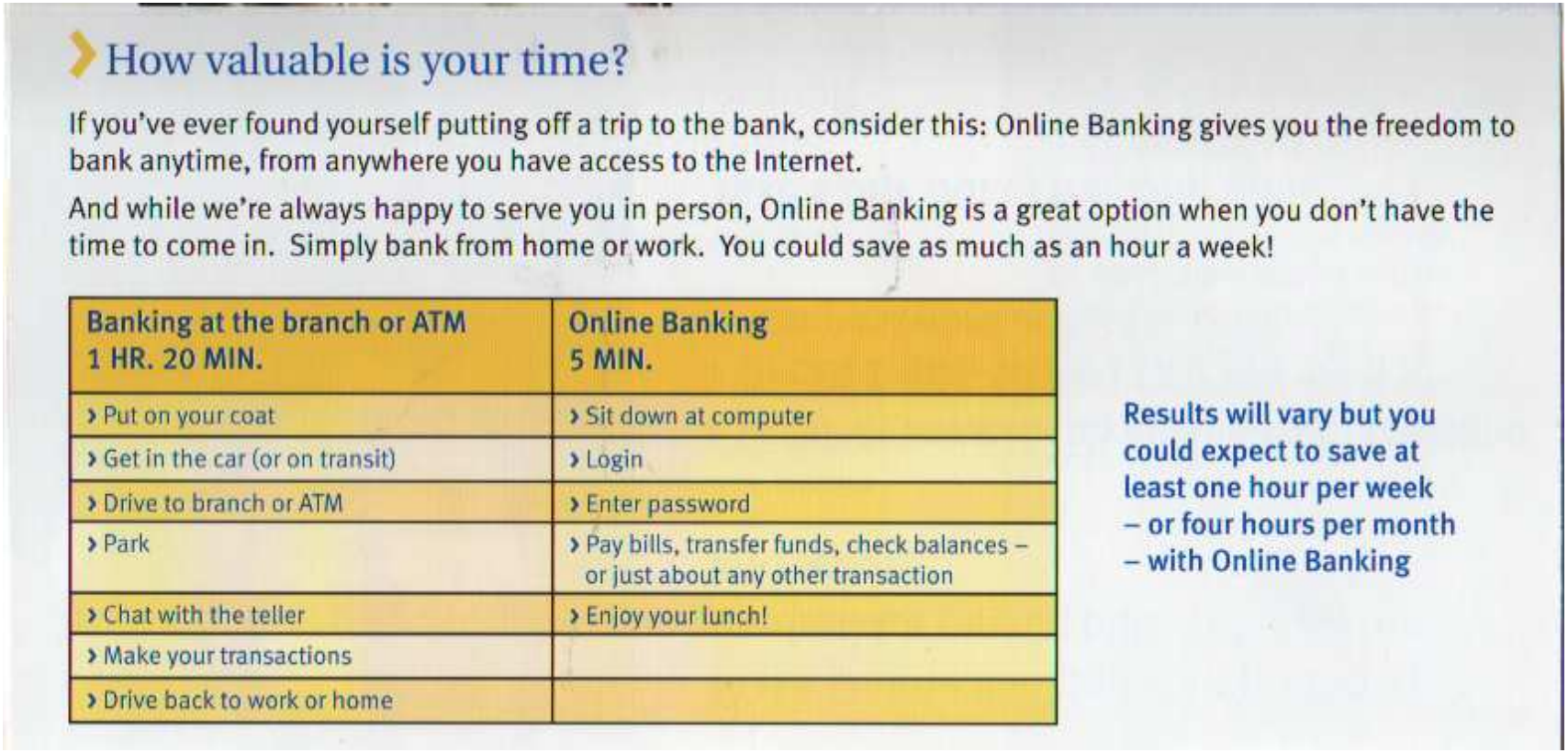
Large Canadian banks

- 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

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

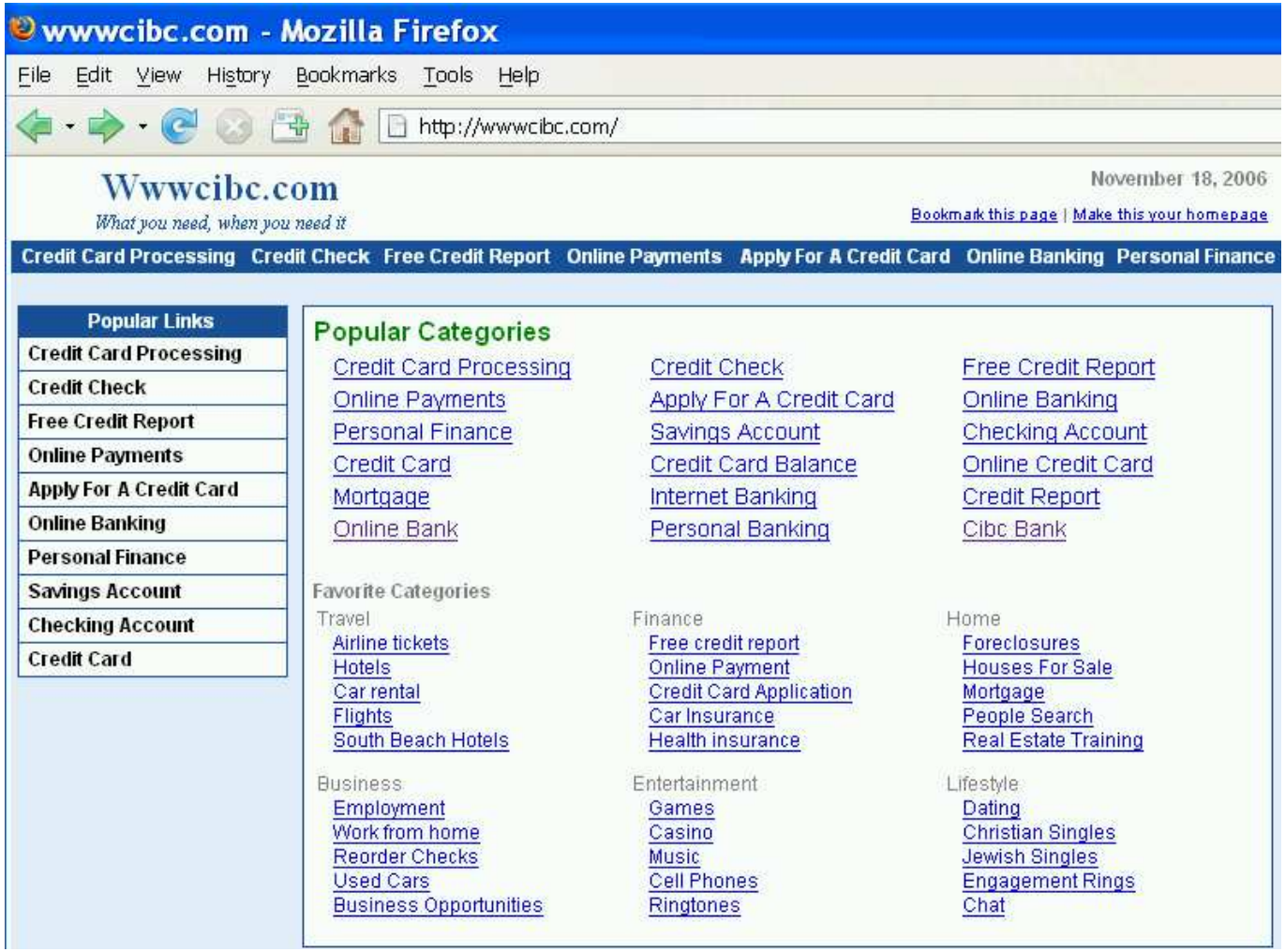
Anti-malware user study

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.pcfinancial.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
Credit Card Processing
Credit Check
Free Credit Report
Online Payments
Apply For A Credit Card
Online Banking
Personal Finance
Savings Account
Checking Account
Credit Card
Popular Categories
Credit Card Processing
Credit Check
Free Credit Report
Online Payments
Apply For A Credit Card
Online Banking
Personal Finance
Savings Account
Checking Account
Credit Card
Credit Card Balance
Online Credit Card
Mortgage
Internet Banking
Credit Report
Online Bank
Personal Banking
Cibc Bank
Favorite Categories
Travel
Airline tickets
Hotels
Car rental
Flights
South Beach Hotels
Finance
Free credit report
Online Payment
Credit Card Application
Car Insurance
Health insurance
Home
Foreclosures
Houses For Sale
Mortgage
People Search
Real Estate Training
Business
Employment
Work from home
Reorder Checks
Used Cars
Business Opportunities
Entertainment
Games
Casino
Music
Cell Phones
Ringtones
Lifestyle
Dating
Christian Singles
Jewish Singles
Engagement Rings
Chat

wwwcibc.com with a twist

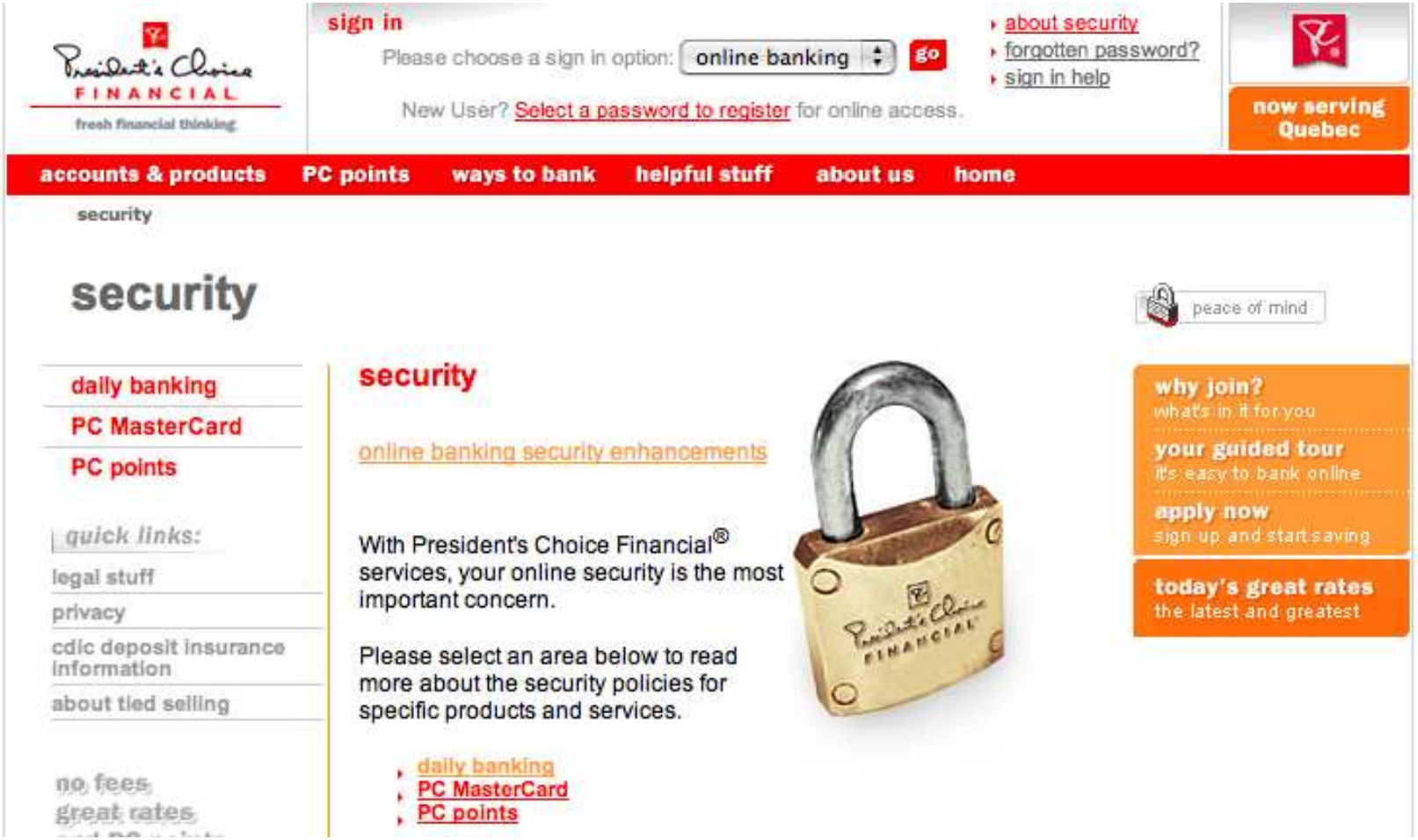
Check the lock?

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

IE7 – where is the lock?

Embedded SSL lock

Not big enough?



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."

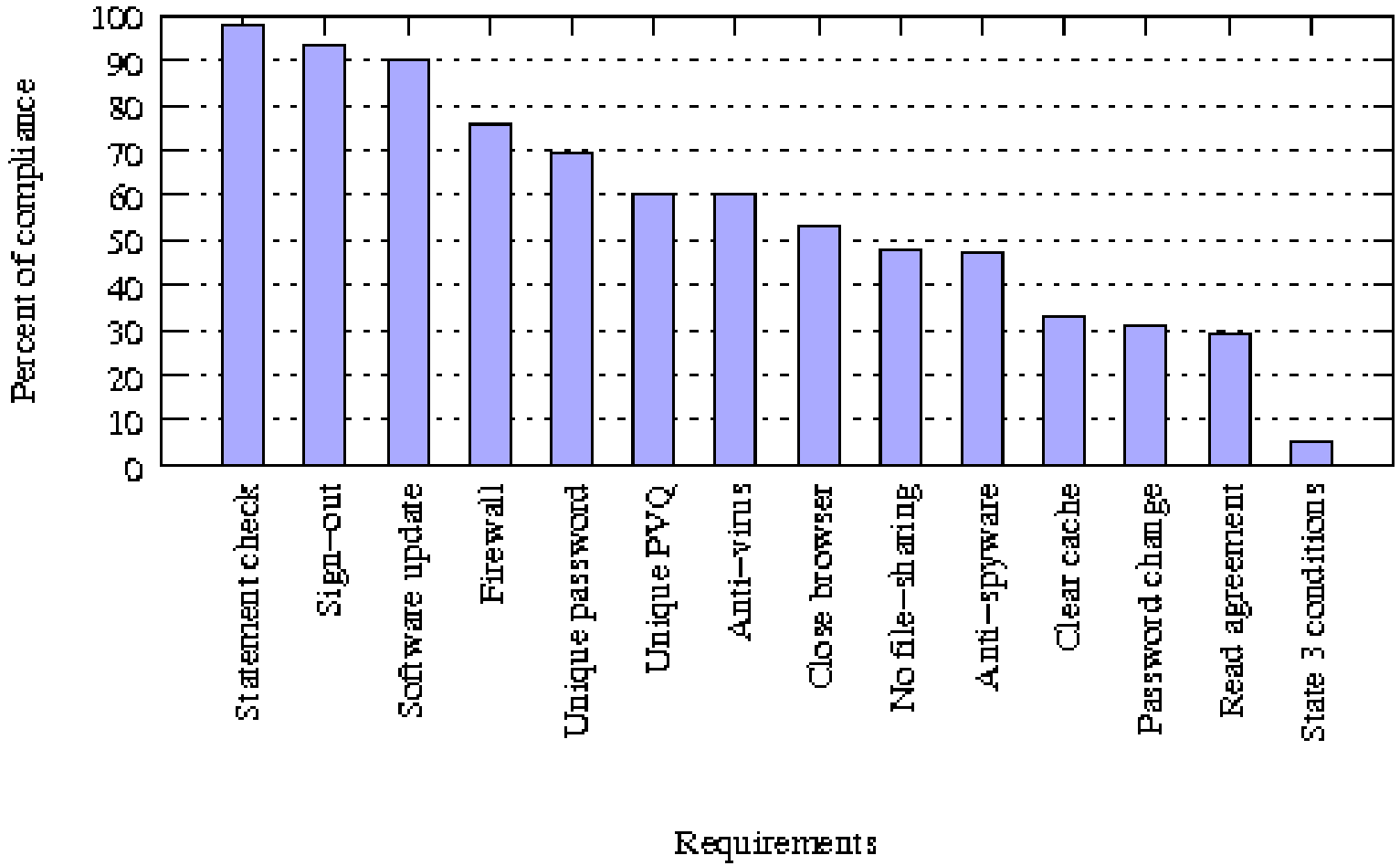
Misleading information

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^{rd}, 4^{th} 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”