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!

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

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?

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
Security and Usability Gap in Online Banking

www.cibc.com
wwwcibc.com with a twist
Check the lock?

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

- **Microsoft Windows:**
  - Microsoft Internet Explorer
  - Netscape Navigator
  - Firefox

- **Apple MacOS:**
  - Apple Safari
  - Firefox

Secure

Not Secure
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: iwthych or iw2hych (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 (3rd, 4th year) and grad students, post-docs, profs, net admins, security researcher and professionals

– gives us a best-case scenario
Result summary

[Bar chart showing percent of compliance for various requirements such as statement check, sign-out, software update, firewall, unique password, unique PVQ, anti-virus, close browser, no file-sharing, anti-spyware, clear cache, password change, read agreement, and state 3 conditions.]
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”