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

Mohammad Mannan, P.C. van Oorschot
School of Computer Science, Carleton University
Ottawa, Ontario, Canada
{mmannan, paulv}@scs.carleton.ca

ABSTRACT

Online banking is one of the most sensitive tasks performed by general Internet users. Most traditional banks now offer online banking services, and strongly encourage customers to do online banking with 'peace of mind.' Although banks heavily advertise an apparent '100% online security guarantee,' typically the fine print makes this conditional on users fulfilling certain security requirements. We examine some of these requirements as set by major Canadian banks, in terms of security and usability. We opened personal checking accounts at the five largest Canadian banks, and one online-only bank. We found that many security requirements are too difficult for regular users to follow, and believe that some marketing-related messages about safety and security actually *mislead* users. We are also interested in what kind of computer systems people really use for online banking, and whether users satisfy common online banking requirements. Our survey of 123 technically advanced users from a university environment strongly supports our view of an emerging gap between banks' expectations (or at least what their written customer policy agreements imply) and users' actions related to security requirements of online banking. Our participants, being more security-aware than the general population, arguably makes our results best-case regarding what can be expected from regular users. Yet most participants failed to satisfy common security requirements, implying most online banking customers do not (or cannot) follow banks' stated end-user security requirements and guidelines. The survey also sheds light on the security settings of systems used for sensitive online transactions. This work is intended to spur a discussion on real-world system security and user responsibilities, in a scenario where everyday users are heavily encouraged to perform critical tasks over the Internet, despite the continuing absence of appropriate tools to do so.

*Version: October 19, 2007.

New Security Paradigms Workshop (NSPW) 2007 New Hampshire, USA

Keywords

Online banking, Usability, Security requirements

1. INTRODUCTION

Applications with major security and usability issues, such as online banking, are being used by more and more people who are less and less technically savvy. Most major banks currently support online banking, as it enables them to serve far more customers than by traditional banking, at a fraction of the cost.[1] Exploiting the convenience and overhead savings possible through the Internet, some online-only banks have also arisen. Online access also reduces physical visits to the bank, which saves customers' an hour and fifteen minutes (as advertised by one bank). However, the popularity of online banking has attracted criminals exploiting (online) banking customers. Attacks have been launched against customers of big and small banks worldwide. Canadian banks – some of which are among the largest in the world – are no exceptions. There are five major traditional banks operating in Canada which are quite heavily regulated by the Canadian Bankers Association and the government of Canada. These banks provide comprehensive guidelines to their online customers as part of the campaign against Internet-based attacks. The 2005 Canadian Internet Use Survey [69] found that 58% of Canadian Internet users do online banking. However, it was not studied how many users actually fulfill their online banking 'responsibilities' as dictated by the banks. As a typical example, users are expected to install and maintain a firewall, anti-virus, and anti-spyware programs on their own. A user could be held responsible for financial losses if their PIN or password is 'easily' guessed, e.g., derived from their phone number, birth date, address or social insurance number (SIN).

Globally, banks are becoming increasingly reluctant to reimburse users who fall prey to online scams such as phishing. We are not aware of any such reported cases in Canada so far although numerous such incidents have made news in the recent past elsewhere. One report [28] indicates that U.S. victims of phishing attacks lost five times more money in 2006 than 2005. Although 80% of the victims in 2005 got their money back, in 2006 only 54% victims were refunded by their banks. In the U.K., bank card related frauds are on the decline over the first six months of 2006, but online banking fraud increased by 55% during this period. Online banking fraud victims of China must prove that the bank

[1]One study [40] estimates in-branch transactions cost about $1 to $4 while an online transaction costs less than five cents.

was at fault to get any money back. According to the 2007 Code of Banking Practice in New Zealand [51], banks may inspect a victim's computer in case of an Internet fraud to verify if the customer has met all the online banking security requirements (e.g. anti-spyware, operating system security updates). Netcraft news [48] reported that fraud victims of the Bank of Ireland were denied reimbursement when they lost about 160,000 euros through phishing attacks. When threatened by lawsuits, the bank finally refunded the victims. To avoid further losses banks worldwide are imposing increasingly more responsibility on online banking users. The fear of losses is also having an impact on users. A survey of 23,000 European Internet users reported [66] that security worries deter 40% of those surveyed from doing online banking. A Gartner survey [16] reported that online attacks influenced nearly 30% of online banking users; more than 75% of those users logged in less frequently, and about 14% stopped paying bills online.

In conjunction with this study, we opened personal checking accounts at the five largest Canadian banks: CIBC, RBC Royal Bank, TD Canada Trust, Scotiabank, and BMO Bank of Montreal.[2] We also opened an account at President's Choice Financial, which is primarily an online-only bank. We opened these accounts during October and November of 2006, and have been accessing them since then. Our study of online banking security and usability is mostly a *cognitive walk-through* [72]. We focus mainly on issues related to personal checking accounts (vs. business, trading, or credit card accounts). We critique privacy and security requirements[3] imposed by banks on regular home-based online banking users from a usability point of view (i.e. whether these requirements are reasonable and practical). Most of our reported findings were derived from our on-site bank account creation experiences, content of bank agreements (for regular and electronic use), security and privacy requirements and recommendations from bank websites, and our experience of using the online banking interfaces. Our findings lead us to believe that most users fail to meet the requirements enabling eligibility for the 100% reimbursement guarantee for online banking fraud losses. We also conducted a questionnaire-based survey among technically advanced users to understand whether even they satisfy online banking requirements. The survey indicated that indeed, most participants failed to fulfill their banks' online banking requirements.

Putting our work in perspective, user-centered security [81] was introduced by Zurko and Simon at NSPW 1996 (see also [80]). Several user non-acceptance paradigms were explored in an NSPW 2004 panel [29]. Online banking is no longer *new*, but still relatively young in its life, and increasingly new converts to online banking are less and less technically savvy. Security and usability is still a relatively *new* paradigm from an academic research perspective. Our work provides a reality check on usable security, using online banking as an example of widely used security-sensitive applications.

[2]Many of the 32 million Canadians have accounts at more than one of these.

[3]Requirements here include conditions from banks' customer agreements (hard-copy and/or electronic) and security recommendations/advice from bank websites. The legal implications of banks' recommendations and security guidelines are unclear.

Contributions/discussion points. We analyze banks' requirements for online banking from a usable security perspective, using Canadian banks as a case study. Our contributions and discussion points for NSPW include:

1. Specific Online Banking Security and Usability Issues. We provide an analysis of online banking requirements from client agreements (for regular and electronic banking), and security and privacy requirements/recommendations from banks' websites. These highlight real-world security and usability issues.

2. User Survey on Satisfying Online Banking Requirements. We report on a questionnaire-based survey of 123 computer science students, professors, researchers and professionals. Even most of these security aware users fail to satisfy common online banking requirements in practice.

3. Glimpse of System Security for Informed Research. What kind of systems do people actually use for highly-sensitive online tasks such as Internet banking? Banks' security requirements for online banking (e.g. password, anti-malware, up-to-date operating system and browser) encompass several aspects of system security for average users. Our work provides a glimpse of overall system security of home computers owned/operated by technically advanced users. Security attributes and user habits as revealed in our study provide a view to what security (and usability) researchers may expect at best from average users; we believe this is essential for informed discussion and design for usable security.

4. Who Bears the Responsibility for Security. In the future, we may be using Internet-enabled home computers for tasks potentially even more security-sensitive than online banking. But even for online banking, is it enough for service providers to simply impose on users, in a customer agreement, whatever responsibilities they deem appropriate? On the other hand, should users take no responsibility for the security of their PCs and Internet usage? Where should the balance of responsibility rest? Our work aims to spur discussion on these questions.

Overview. Related work is discussed in Section 2. SSL-based bank site authentication is discussed in Section 3. Banks' anti-malware requirements are discussed in Section 4. We discuss banking agreements in Section 5. Software updates and miscellaneous issues (including user authentication) related to online banking are discussed in Sections 6 and 7 respectively. We provide the results of our online banking survey in Section 8. Section 9 concludes.

2. RELATED WORK

Related work is discussed both here and other appropriate places throughout the paper. Hertzum et al. [32] analyzed the usability of Danish online banking security for a particular task (money transfer to a specific account) with respect to the usable security definition of Whitten and Tygar [73]; and evaluated installation of special client-end e-banking software (as required by some Danish banks), logon, money transfer, and logoff. Several usability weaknesses in online money transfer were revealed. Chung et al. [12] studied

the effectiveness of web interfaces of several banks in New Zealand. Nilsson et al. [52] exposed the security implications of system generated versus user password for online banking. Singh [68] examined (through a user study) the users' perspective on the security of online banking in Australia, and concluded that one way to increase users' perception of online security is 'to have customers believe the provider will not allow them to suffer fraudulent transactions.' Edge et al. [21] analyzed online banking (money transfer in particular) security using *attack trees*, and proposed solutions to known attacks using *protection trees* and multi-factor authentication. Karjaluoto et al. [38] conducted a survey among non-users and users of Finish online banking, and analyzed differences of the demographic profile of these two groups of users. A similar survey [7] attempts to examine the effects of trustworthiness among online banking users. Jin et al. [35] briefly analyzed online banking risks for banks, and how these risks may be managed. As opposed to analyzing the usability of offered features or any specific security mechanism (e.g. password) for online banking, we focus on the usability of major online banking requirements.

3. BANK SITE AUTHENTICATION: SSL CERTIFICATE

In this section, we discuss what we see as serious usability issues related to SSL certificates. Bank websites generally present an SSL certificate on an online login page to be authenticated by a user. Banks expect users to visit the correct URL of a bank, check for visual clues (e.g. the lock icon and `https` on the address bar) of an SSL protected site, and check certain items on the site certificate before entering any login information. Banks emphasize that the presence of an SSL certificate implies that a website is *secure* and *genuine*, and that no one can see a user's information other than the bank (e.g. BMO states that an SSL certificate is an electronic *passport* for a website). Although a certificate may authenticate a website, it of course does not *secure* the site, and malware on a PC can easily access all (including SSL-protected) user information. Below we discuss more SSL-related issues in detail.

Login URL. Users may be redirected to spoofed or malicious websites if a memorized bank URL is misspelled. A bookmarked login URL may be replaced by a phishing site URL by malware on a user PC. Banks strongly recommend users to check the URL of a bank website before entering the bank card number and password. Nevertheless, when a login URL is `https://www.txn.banking.pcfinancial.ca/a/authentication/preSignOn.ams?referid=loginBox_banking_go`, it is unclear how users should make a decision as to whether this is a *correct* URL. Some banks (e.g. PC Financial) even state that the 's' in the `https` implies the website is 'secure' even though a self-signed site certificate can easily be used to show `https`. In a user study as reported by Dhamija et al. [19], 23% of users relied only on the content of a page to determine legitimacy, i.e., did not check the URL at all, and many users did not understand the syntax of domain names. Downs et al. [20] reported that only 35% of the participants of a user study noticed the text `https` on a URL; some who noticed the `https` did not understand the significance of the extra 's.' Nearly 45% did not look into the URL at all in their study. We thus believe that banks have unrealistic expectations of users 'checking' URLs.

The SSL lock icon. The display of an SSL padlock is strongly emphasized as an indication of a secure website (though not all emphasize that this should be on the browser chrome). As banks state, generally the lock icon is displayed on the lower-right corner of a browser. However, different browsers, and even different versions of the same browser, show the padlock in different places on the browser chrome. Internet Explorer 7 (IE7) has recently moved the padlock location from the traditional lower-right corner to the address bar. Although CIBC and PC Financial login pages have SSL certificates, the Opera browser (version 9.22 on Windows XP, and version 9.2 on Mac OS X) does not display the lock icon unless the login page is re-loaded (i.e. refreshed); in fact, Opera's site information dialog states that "Site not secure...The communication is done in plain text, and there is no way to guarantee the identity of the server." PC Financial states that there is a known bug affecting earlier versions of IE (e.g. 5.5); when a user selects the padlock icon, IE warns, "This certificate has failed to verify for all of its intended purposes." The bank advises users that this is not a concern as the SSL certificate is actually okay.

The lock icon is displayed inside the sign-on pages of all banks. Many phishing websites use a closed-padlock inside the browser chrome – which has nothing to do with SSL protection – to *assure* users that the website is secure. Average online users do not generally understand that any webpage can display within the page content itself whatever icon or text the page designer wishes; thus an embedded lock icon may conflict with the SSL lock icon (on a browser chrome) and confuse users. A website can also display any icon at the beginning of the site's URL as a *shortcut icon*. This icon is displayed on most current browsers' address bar. For example, the website `http://www.ljean.com` (as of Aug. 27, 2007) has the lock icon as its shortcut icon although this is not an SSL protected site.

Only a small portion of users (23%) has been reported [19] to look for or notice the padlock icon on the browser chrome. Recently an increasing number of phishing sites is reported to have SSL certificates (mostly self-signed) to gain confidence of somewhat technically advanced users [49], i.e., users who might check the existence of a closed-lock and the corresponding SSL certificate. Another user-study by Downs et al. [20] reported that most participants (85%) noticed the secure site lock icon on a website. However, only 40% of those who were aware of the lock icon knew that the lock must be on the browser chrome to signify an SSL-enabled website. Some participants stated that SSL certificates were a 'formality,' like an 'elevator certificate.' 32% of users would log into a website even if the site presents a self-signed certificate. In one real-world incident [49], only one in 300 customers of a New Zealand bank chose to abandon the SSL session upon a browser warning indicating an expired SSL site certificate; the bank accidentally allowed a certificate to expire for a period of 12 hours. We conclude that banks have unrealistic user expectations with respect to the SSL lock icon.

Security toolbar. TD Canada Trust provides a free tool from Symantec called Norton Confidence Online (NCO). NCO is installed as an ActiveX control in IE, and is designed to detect spoofed TD Canada Trust websites. The tool is added to IE toolbar, and is displayed as a closed lock, similar to the SSL lock. Such visual similarity may confuse

average online users. A user is notified with a dialog box when a spoofed TD site is detected, but users may ignore this and visit the site anyway [53]. NCO is available only when accessed from IE on Windows. Installation of the ActiveX control requires administrative privileges. Also any such toolbars may still miss a significant portion of phishing websites as revealed by Zhang et al. [79] (similar results were reported by Wu et al. [75]). In fact, in one recent (Aug. 2007) real-world case [8], when the Bank of India website was compromised for several hours and serving more than 22 pieces of malware to each site visitor, most well-known online 'trust brokers' (e.g. Netcraft toolbar, McAfee SiteAdvisor, Google Safe Browsing) reported the site to be valid.

Certificate components.[4] Banks ask users to check the SSL site certificate of a bank on a login page, but do not illustrate exactly what a user should look for in a certificate. Table 1 summarizes important components of SSL certificates provided on sign-on pages of different banks. As evident from the Common Name (CN) column of Table 1, CNs are quite arbitrary and different than banks' advertised homepage URLs. For example, CIBC's main webpage URL is `www.cibc.com`, but the CN on the sign-on page SSL certificate is `www.cibconline.cibc.com`. However, there is a different SSL certificate for CIBC's 'Contact Us' page with `www.cibc.com` as the CN. After logging into online banking, the TD SSL certificate changes (for no obvious reason), showing different names as CN, e.g., `easyweb37z.tdcanadatrust.com`, `easyweb45z.tdcanadatrust.com`. Following the tabs on the online baking page brings other TD pages with different CNs on their SSL certificates, e.g., `www.tdcanadatrust.com`, `www.tdwaterhouse.com` (this is true for other banks too). Understanding the details of an SSL certificate is already complicated for many users, and so many different SSL certificates may confuse users even further.

To understand CNs, a user must understand the domain name hierarchy, e.g., the important part of `www.txn.banking.pcfinancial.ca` is the domain `pcfinancial.ca`. Otherwise, CNs do not provide much useful information; attackers may generate SSL certificates with a CN such as `www.pcfinancial.secure-banking.ca`. The Organisation (O) items on some SSL certificates also differ from a bank's otherwise well-known name. For example, PC Financial's SSL certificate Organisation is 'Loblaw Companies LTD.' For average Internet users, encryption algorithm specifications and Certificate Authority (CA) names probably mean almost nothing. Users must also know that Verisign is a trustworthy CA, but Verisecuresign is probably an imaginary CA (generated by phishers). Also users must understand the browser security model, i.e., there are root certificates embedded with browsers from several (about 100) 'trusted' CAs (trusted by browser providers – users have no role in such decisions); these embedded CA certificates are used to verify a given website's SSL certificate. Users must understand that not all CAs are trustworthy, at least not to the same level. Shortcomings of the browser security model are well known and have been exploited in the past; e.g., as described in an article after the Katrina disaster [22]. (Note that several shortcomings of SSL are in fact inherent to public key cryptography; see, e.g., Davis [18].)

[4]We do not discuss IE7 *extended validation* certificates, which solve some problems but arguably raise many others [34].

Possible domain name conflicts. PC Financial's online banking URL is `www.pcfinancial.ca`. If a user types in `www.pcfinancial.com`, an under-construction website owned by directNIC is displayed. However, for CIBC customers, `www.cibc.ca` redirects to the regular CIBC site at `www.cibc.com` (the same is true for RBC, TD, BMO, and Scotiabank websites). The CIBC branch locator service is provided externally by a different company and the URL is `cibc.via.infonow.net`. Thus valid CIBC pages are sometimes served from domains other than `cibc.com`. The domains `cibc.net` and `cibc.org` are not owned by CIBC. The domain `wwwcibc.com` is also registered by someone other than the bank; this may trick many CIBC users if used in a phishing attack. Similar naming conflicts are quite common for other banks as well. If we take the possible similar domain names under other countries' top level domains, understanding domain names gets even more complicated. In fact, a domain name search at Netcraft's website (`searchdns.netcraft.com`) results in more than 500 entries with 'rbc' as part of a domain name. All banks suggest users look into the URL displayed on a browser's address bar to identify possible phishing sites. Nevertheless it is unclear what exactly users should look for, and how to interpret a domain name in the presence of such conflicting names. Assuming users understand complex domain name policies seems to be very far from a sound security principle.

4. ANTI-MALWARE REQUIREMENTS

Most banks' customer agreements require users to install and maintain up-to-date copies of anti-virus, firewall, and anti-spyware programs. In this section, we discuss several issues related to banks' anti-malware requirements.

Cost of anti-malware. Banks advertise 'free' anti-malware products on their websites although the free products are generally trial or detection-only versions. Banks recommend users to buy anti-malware from reputable vendors such as Symantec and McAfee. Users must also pay for subscription renewal fees every year; in some cases subscription renewal is automatic and difficult to cancel [74]. The use of multiple computers to access online accounts multiplies the anti-malware cost. Thus evidently, users must spend a significant amount of money to be eligible to use *free* online banking services. For example, according to CIBC's anti-malware recommendation, a user must spend around $80 to buy discounted products from Symantec and Webroot. The monthly fee for maintaining a checking account at CIBC is approximately four dollars, thus yearly a user might be paying less than $50 for accessing all other banking services, e.g., bank tellers, bank machines, point-of-sale payments through a bank card, and telephone banking. Although there exist decent quality anti-virus, firewall and anti-spyware programs (e.g. `avast!`, `ZoneAlarm`, and `AdAware` respectively) which are offered for free for home users, banks do not mention those on their websites. These free anti-malware programs have been rated highly by many reviews, e.g., see `AV-test.org`.

In addition to anti-malware, banks also ask users to run various 'free' security tools. For example, RBC recommends users to test computers using `Shields Up` (from Gibson Research) and Symantec `Security Check`. Shields Up is a web-based Internet vulnerability profiling tool to asses file sharing, common port vulnerabilities, messenger spam etc.

	Common Name (CN)	Organization (O)	Signing CA	Encryption
CIBC	www.cibconline.cibc.com	Canadian Imperial Bank of Commerce	RSA	RC4 128
RBC	www1.royalbank.com	Royal Bank of Canada	Verisign	RC4 128
TD	easyweb.tdcanadatrust.com	The Toronto Dominion Bank	RSA	AES-256
Scotiabank	www.scotiaonline.scotiabank.com	Bank of Nova Scotia	RSA	RC4 128
BMO	www1.bmo.com	Bank of Montreal	Entrust.net	RC4 128
PC Financial	www.txn.banking.pcfinancial.ca	Loblaw Companies LTD	RSA	RC4 128

Table 1: Comparing SSL certificate components

Symantec Security Check is also a web-based tool for network vulnerability tests and virus detection; it requires installing an ActiveX control and Java run time environment. To fix any detected vulnerabilities or malware, users are advised to buy security products from McAfee/Symantec.

Usability and maintenance. Proper installation and maintenance of anti-malware requires time and a certain level of technical expertise. Maintenance tasks include downloading malware signature updates (although this is somewhat automated), product security updates (e.g. updates that fix known vulnerabilities within the product itself), and yearly license renewal. Sometimes users may have to deal with more complex issues such as failure of an auto-update or scheduled virus check. Completing such maintenance tasks correctly remains challenging for many average computer users. Banks do not take any responsibility for any difficulties, consequences or costs of installing and maintaining any recommended anti-malware. While reporting a possible fraud, CIBC users are asked to attach scan-logs from anti-virus and anti-spyware programs. How reliably an average Internet user can perform such operations is apparently an open question. Although banks advertise that online banking can be used from *anywhere*, users must ensure that up-to-date anti-malware programs exist in all computers used for online banking 'including a computer at work, the library, an Internet cafe or another public place' (according to CIBC).

To clean a PC infected with known malware, users may need to follow one or more steps from the following list (note, this list is not comprehensive): (i) completely re-install the OS (as acknowledged by Microsoft [24]); (ii) check the infected PC's hard disk by running anti-malware from another *malware-free* PC; and (iii) check the infected PC by running it in a 'safe mode' (i.e. a reduced functionality mode). Performing any of these tasks is challenging for average users.

Despite the efforts of making personal firewalls user friendly, a cognitive study [33] of 13 most popular firewalls reveals several usability drawbacks of these products. (Effective use of enterprise firewalls is also subject to dispute, see e.g. Singer [67].) Like any other security products, a misconfigured personal firewall may endanger a user's safety more than no firewall at all due to a false sense of security (cf. [9], [33]). One user study [43] of 378 U.S. respondents revealed a significant gap between the user-reported and actual state of security of their computers. For example, while 92% of participants reported to have up-to-date anti-virus (AV) software, in reality, only 51% had an AV signature file updated within the past week. Some statements regarding anti-malware programs, as provided on several banks' websites, are also misleading and too broad in reality. For example, TD Canada states that firewalls allow only "the connections that are known and trusted," which is generally far from the current Internet reality; e.g., firewalls may do nothing when a user visits a phishing site.

As a step towards the fight against spyware, RBC's recommendations include: (i) Google search a product name to find out whether it contains any spyware; (ii) always carefully read licensing agreements and privacy policies of a product; and (iii) use anti-spyware if the user 'suspects' any spyware activities, e.g., frequent pop-up advertisements, computer performance degradation. Only technically advanced users seems likely to take advantage of Internet search to explore whether a file is malicious or contains embedded malware. Expecting users to read and understand software agreements seems unrealistic (see Section 5). Spyware may not be explicitly visible on a PC, and a computer's performance may degrade for several other reasons, e.g., disk fragmentation, diminishing free disk space, increased number of start-up programs. Therefore, it remains unclear how a user may 'suspect' spyware infection on a given PC. Removing spyware from a computer may be 'difficult' as stated by BMO; the bank encourages users to consult a trusted third party that specializes in computer maintenance and repair assistance (at their own expense).

In a user study by Downs et al. [20], 95% of users were familiar with the term 'spyware;' 70% of the participants used online banking. Interestingly, several users believed that spyware was 'protecting' their computer. Expecting such users to understand and follow a bank's anti-malware requirements may lead to unwanted consequences.

Shortcomings of anti-malware. Most current anti-virus (AV) programs are signature based, i.e., they mainly detect known malware. However, a signature is typically generated only when malware attempts to actively propagate in the wild. Small-scale attacks in which only a few computers are targeted, generally remain undetected by many anti-virus solutions. Commodity anti-virus vendors generally take an extended period of time to generate signatures of such malware, if at all. For example, Shipp [65] reported that a targeted trojan first released in June 2006 was detected by only four AV products in Oct. 2006; other AV products could not detect the malware even after months of its release. An AusCERT study [78] reported that popular AV products have an 80% miss rate on new malware as malcode authors generally test their malware against commonly used AV products before releasing it to the wild. In a malware trend report [14], Commtouch reported to detect 42,652 distinct variants of the Storm-Worm in a period from Jan. 18-30, 2007, i.e., 3,824 variants per day. Apparently it is very difficult for traditional anti-virus to generate so many signatures so quickly. In a recent (Aug. 2007) anti-virus test [17], only three out of ten AV products could

catch all 18 (known) sample viruses. AV products often fail completely against malware that exploits zero-day vulnerabilities (i.e. *unknown* to the public domain). According to one study [2], as of June 16, 2007, the average lifetime of a zero-day bug is 348 days (with shortest and longest lifetime of 99 and 1080 days respectively). While AV products often fail to detect malware, sometimes legitimate programs are falsely identified as malicious, e.g., Symantec AV falsely detected malware on `Filezilla` and `NASA World Wind` [59]; such incidents further reduce users' trust on anti-malware.

Several recent instances of malware, when installed on a PC, e.g., by exploiting a zero-day vulnerability, attempt to remove or disable all common anti-malware on the infected PC. Some also change the `HOSTS` file on a Windows PC or otherwise poison a user's local DNS cache to redirect security-related websites, e.g., Windows update and McAfee, to marketing-related or malicious websites.

Virtual machine based rootkits, e.g., SubVirt [41], Blue Pill [56] may take complete control over a commodity OS, and may only be removed through a complete OS reinstallation. Rootkits installed on a graphics or network card [31] can even survive a low-level re-formatting of an infected hard disk following a full OS re-installation.

Attackers are also targeting security flaws in widely used anti-malware programs; one reason is that these programs generally run in a higher privilege mode than other applications. In a 15-month period ending Mar. 31, 2005, 77 separate vulnerabilities were discovered in security products from well-known vendors including Symantec, F-Secure and CheckPoint [77]. Symantec has disclosed 22 security advisories for its products so far (Aug. 13) in 2007.[5] In Nov. 2006, bot programs were reported to spread by exploiting known vulnerabilities in Windows and Symantec anti-virus (corporate edition) [64]. In one global snapshot[6] of current attacks as of Apr. 18, 2007, 70.5% of attacks were attributed to the Symantec anti-virus remote stack buffer overflow vulnerability (`CVE-2006-2630`) even though the vulnerability was reported on May 24, 2006, and a patch was promptly released. Evidently, users do not (or cannot) keep up with software updates (see Section 6), and their PCs may be compromised through their use of anti-malware tools. Of course, banks accept no responsibility of such unfortunate situations.

Banks also advise users to scan emails with an anti-virus program. Banks ask users to be cautious about emails from unknown sources to prevent users from phishing attacks. However, phishing or spam email may be sent from a known contact's email address, and can even mimic patterns of a regular email from that contact [4]. Current anti-malware does not detect such attacks, and even most cautious users may fall prey to such an attack. We thus conclude that banks have unrealistic expectations with respect to users dealing with malware and spyware.

5. DOCUMENTATION AND AGREEMENTS

Banks strongly advise customers to review banking related user agreements including online banking, client card, and privacy agreements. Users' banking responsibilities are outlined in these agreements and on bank websites. Users must read and review these documents to understand important conditions and requirements of the 100% reimbursement guarantee. When we were setting up bank accounts with the six major banks, not one bank representative made us specifically aware of important online banking issues other than protecting the password (e.g. not to write down a password); we were assumed to have read and agreed to all terms and conditions as laid out on the agreements and websites. However, all banks provided us a printed copy of the agreements. Using the bank card or online banking confirms that 'you have read and understood the agreement and agree to its terms and conditions' (as stated by RBC). Banks also state that agreements can be changed *at any time*, and users will be notified by 'a notice on our website.' We argue that many users do not read client agreements or security advice on bank websites, and therefore may remain unaware of the requirements they must fulfill to do online banking *safely*. In fact, the survey results in Section 8 support our conviction.

Banks also ask users to read software agreements carefully to avoid spyware/adware installation. However, RBC admits that information about spyware installation may be embedded in a third-party license agreement, and "These references may be hard to find and the user may not realize the full implications of the install." Grossklags and Good [30] conducted user studies evaluating the readability and usability of End User License Agreements (EULAs) using 50 popular software programs from `download.com`. The average EULA length was 2752 words. (In comparison, lengths of RBC's electronic access agreement,[7] bank card agreement, and privacy policy are about 5100, 3600, and 500 words respectively.) Only 1.4% of participants reported reading EULAs often and thoroughly, while 66.2% admitted to rarely reading or browsing the content of EULAs. It is also questionable how many users understood the implications of EULA content even when read thoroughly. In addition to software agreements, banks also advise users to check privacy policies of websites where a user may provide sensitive personal information (e.g. PayPal). RBC also asks users to check third-party security bulletins regularly, especially for OS and browser security updates. We conclude that banks have unrealistic expectations with respect to users reading and understanding legal and technical documents including online banking agreements, account policies, and EULAs.

6. SOFTWARE UPDATES

Banks strongly advise users to keep an OS and browser up-to-date with security patches. Nonetheless, out-dated browser versions such as IE 5.5 and Firefox 1.0 remain listed as supported by most banks. Beyond the web browser, generally there are many more applications commonly used by millions of users, and thereby being targeted by attackers. Microsoft Office products such as Word and Excel are popular targets. Media players such as Windows Media Player, Realplayer, iTunes, and Winamp also pose security threats if unpatched. Vulnerabilities in Instant Messaging (IM) and desktop email clients have also been widely exploited. In fact, users must keep *all* applications up-to-date to avoid known attacks – a daunting task even for ad-

[5]For a list of Symantec product advisories, see `http://www.symantec.com/avcenter/security/SymantecAdvisories.html`.

[6]Arbor Network's ATLAS Dashboard `http://atlas.arbor.net`.

[7]From `https://www.rbcroyalbank.com/onlinebanking/bankingusertips/agreement/termsindex.html` (Apr. 3, 2007).

vanced users, especially in a Windows environment. Other operating systems, e.g., Ubuntu Linux and Mac OS X provide an update mechanism to keep all installed (native) software packages updated – but these are used by less than 5% of the population.

After installing a new OS, updating the OS and other software on the computer is not the first task that a user might want to do. However, an Internet connected PC may survive only minutes[8] before being compromised via unpatched vulnerabilities. A Windows XP installation requires downloading 70 to 260 MB of security updates from Microsoft [45] (a 13-page SANS report [57] provides guidelines for surviving the first day of an XP installation). Downloading such large updates is highly problematic for users with a dial-up or slow-speed Internet connection.

Updating OS, browser, firewall and anti-malware is challenging for many Internet users. *Patch management* includes collecting all necessary patches, dealing with post-patch conflicts, determining the trustworthiness of a patch source etc. [9], which is a difficult problem even for enterprise IT departments. In addition to usability problems, such updates may even frustrate or fool diligent users. For example, Bellissimo et al. [6] showed that some popular software updates (e.g. McAfee VirusScan) were vulnerable to man-in-the-middle attacks; i.e., a malicious party could install malware exploiting several software update vulnerabilities. Malware such as `Trojan-Dropper.MSWord.Lafool.v` [39] even attempts to propagate as a security update alert from reputable vendors (e.g. McAfee). Some critical security patches released by Microsoft may even crash a system or make it unusable [23]. The critical Windows XP SP2 update stopped many programs including anti-virus from working properly [70]. A Symantec signature update in May 17, 2007 falsely identified (and deleted) two critical system files of the Chinese edition of Windows XP SP2 as trojans, and thereby failed thousands of PCs to boot [15]; even though Symantec fixed the bug quickly, many users had to go through XP's recovery console (a not-so-user-friendly command-line tool) to fix the OS. Malware that upgrades exploiting Windows Update have also been reported in the wild [5].

Only 7 days in 2004 were without an unpatched known vulnerability in IE – the browser recommended by all banks; i.e. IE was unsafe 98% of the days in 2004 [62]. Even if IE or other popular browsers have improved their security more recently – which is arguable – this seems untrue of application software in general on users' PCs. Overall, while the research community recognizes patching as an open problem,[9] banks assume average home users can adequately deal with it.

7. USER AUTHENTICATION AND OTHER ISSUES

We now briefly discuss online user authentication and some other important security and privacy related issues.

User authentication. Canadian banks largely rely on user-chosen passwords and Personal Verification Questions (PVQs) for online authentication. We limit our discussion here as the usability of passwords has been well-studied by others (e.g. Sasse and Adams [1]). Table 2 compares online password and PVQ requirements of different banks. Passwords are case-sensitive, but some banks restrict use of special characters (e.g. #, @). BMO allows only numeric passwords of length six. Fixed-length and small upper limits (e.g. eight) on password length create usability problems.

	Password	PVQ answer
CIBC	6-12	4-21 (2 PVQs)
RBC	8-32	4-20 (3 PVQs)
TD	5-8	functionality absent
Scotiabank	8-16	functionality absent
BMO	6	functionality absent
PC Financial	6-12	1-20 (3 PVQs)

Table 2: Comparing password and PVQ answer length across six banks

Banks recommend that all passwords and PVQs be unique. Most people use several password-protected accounts,[10] and many reported having multiple bank accounts in our survey (Section 8). It is generally difficult to create and memorize many unique secrets [1]. Banks strongly recommend (but do not force) users to change passwords as frequently as every month (e.g. PC Financial). Some banks force users not to reuse a recently used password. Sasse et al. [61] reported that login failures increase after a password change as the new password interferes with the old one. Most users are also reported to use a word with a number at the end when a frequent password change is enforced [60]. Such a password strategy may help attackers to design more efficient password crackers [76]. Banks' policies require that users log-out from online banking when a banking session is over. However, users who navigate away from online banking through links on online banking pages may not see the sign-out button.

Besides strong recommendations such as password uniqueness, CIBC asks users to promptly reset a banking password over telephone or from a *trusted* computer, after accessing online banking from a public computer. Despite such advice, most banks allow obviously *weak* passwords, e.g., '123456' and '111111.' An example of a 'rock-solid' password according to RBC[11] is `iwthyh` (mnemonic of The Beatles' "I want to hold your hand"); but this does not even even meet RBC's password length requirement. Although recommended [1] (see also the NSPW 2001 paper [76]), no bank provides feedback on the strength of a user selected password (cf. [44]).

Users can set up PVQs for resetting a forgotten password (e.g. CIBC, RBC, PC Financial) or as part of the login process (e.g. RBC, CIBC). Online password reset reduces help desk calls (and therefore costs) for banks, and is also convenient for users at the usability cost of memorizing more secrets (cf. Schneier's weblog [63]). As PVQs are rarely used, i.e., users do not need to recall the 'secret' answers often, users tend to choose easily memorable answers. A PVQ answer is typically case-insensitive, free of any special charac-

[8]The average time between attacks is reported as 5 minutes (Apr. 21, 2007) at `http://isc.sans.org/survivaltime.html`.

[9]However, patching is as old a problem as software, e.g. see Glass [27].

[10]A large scale (over half a million participants) survey [25] recently reported that an average user has about 25 password-protected accounts with 6.5 unique passwords as reported (see also [26]).

[11]Accessed Apr. 24, 2007, from `http://www.rbc.com/security/safe_passwords.html`.

ters, and shorter in length than a password. A 6-character password-protected CIBC account can be accessed by answering two PVQs, as short as 4 characters each. Interestingly, a 6-character case-sensitive password can be overridden by a 3-character case-insensitive secret as implemented by PC Financial; there are three PVQs, but each PVQ answer can be as short as a single character. In effect, PVQ answers are allowed to be weaker than passwords, although PVQs are as good as a password to get into an account. Answers to PVQs (e.g. mother's maiden name) may easily be guessed by close contacts of a user as reported even in a pre-Internet era user study by Zviran and Haga [82] (see also [37]). The abundance of personal information on the web (or otherwise available online) enables even complete strangers to make informed guesses (e.g. [42]). Authentication guidelines of the Office of the Privacy Commissioner of Canada [54], recommend that authentication secrets should not be derived from personal identity facts.

Anti-phishing email tips. To distinguish phishing emails from real CIBC emails, users are asked to look for personalized email messages (e.g. customer's real name on the message). Attackers may collect public domain information for deploying targeted phishing attacks (also known as *spear phishing*). Social networking websites such as MySpace have been compromised in the past to extract personal information from user accounts [50]; such information could be used to launch spear phishing attacks. In reality, there have been reported cases of fake Microsoft Update patch email with malicious URLs, including the targeted users' full names in the email body [58]. CIBC reports that 'Properties' of the sender address in an email shows the 'actual' email address, although everything in an email header can be spoofed. RBC suggests users look for misspelled words, and distorted images in emails. RBC also warns users to be suspicious about websites that collect confidential information but are not SSL-enabled. These recommendations are of little help as phishing attacks are now more professional; for example, some scam-spammers are reported [10] to make use of sophisticated *mind game* tricks, and some phishing sites are even SSL-protected [49]. In fact, a Microsoft sponsored survey [3] of 2,482 American adults revealed that 58% of the participants were not at all aware of online threats, while 17% had fallen victim to some forms of online frauds.

Scotiabank sends news and helpful tips to users through 'The Vault' mailing list. The bank does not illustrate how users can verify the authenticity of emails received through the Vault. These emails contain live (click-able) links and users are encouraged to subscribe to the Vault; there is a chance to win $1000 every month for subscribers. Such practices may help phishers in several ways, e.g., phishing email may be sent to users stating that they have won the Vault prize, and need to sign-on to Scotiabank online (actually a spoofed website) to collect the prize.

Several banks (e.g. CIBC, RBC) provide a *secure message centre* for sending important messages/notifications to users. Users can also send messages, e.g., banking instructions or questions, to banks using the message centre. The message centre can only be accessed after logging into a bank website. This is apparently a more secure way of communication than regular email. However, banks may notify users through regular email when a new message is posted on the message centre. As viewing messages from the message centre requires login to online banking, such notifications via email may open a new avenue to phishing attacks.

Unnecessary information collection. Banks suggest that users not provide their Social Insurance Number (SIN) as an identification token when other types of identifiers may be sufficient. However, we were asked by most banks to provide the SIN when opening even a regular checking account. Although we declined to provide the SIN, all accounts were opened successfully. Bank representatives also asked for several other unnecessary personal information, e.g., family size, income, rent, dependents, which were in no way related to a checking account. When asked, bank representatives told us they were collecting such information which might be required to 'better serve' us in the future, e.g., if we apply for credit cards. However, we argue that such unnecessary information collection should be avoided as it may pose increasing risks to privacy and security, and allows banks to collect information (for marketing purposes) which users may misunderstand as being required by banking standards to open new accounts.

8. USER SURVEY

We conducted a survey to gain insight on user compliance with online banking requirements. In this section we discuss the results. We compiled a questionnaire (attached in Appendix A) from some common requirements and recommendations of Canadian online banking. This was reviewed and approved by our university ethics committee. The survey was anonymous and voluntary.

Participants and results. There were 123 participants in the survey. Our participants include under-graduate (3^{rd} and 4^{th} year) and graduate students, professors, post-doctoral fellows, network administrators, security researchers and professionals, mostly from the computer science department of our university. Participants in this study are not representative of general online banking users; but we conducted the survey to understand whether highly technical and security-aware users fulfill a subset of banks' requirements and recommendations. Tables 3 to 11 summarize our findings. Note that other than their honesty, participants were in no way motivated to complete the survey or answer correctly. We presented a preliminary version of this work in a graduate course, and some participants mentioned that they attended the class talk and their online banking habits were thereby influenced (e.g. they became more aware of the banking requirements – thus if anything, our results over-report actual security compliance). For some questions a few users chose the "Don't know" option. We did not include those answers to the results. We allowed space for comments on the questionnaire. Some other requirements and recommendations which have not been discussed earlier in the paper were also included in the survey; these include file sharing through Windows or peer-to-peer (P2P) clients, clearing browser cache and closing the browser after a banking session, and checking bank statements.

Discussion. About 93% of participants (115 of 123) reported using online banking (but note that several users refused to participate in the survey, potentially biasing this statistics). One participant who does not use online banking, commented that he/she 'read the agreement and thought it [online banking] too risky; it is impossible to comply with

	RBC	CIBC	TD	Scotiabank	BMO	PC Financial	Other
No. of users	24	12	28	32	13	17	12

Table 3: Users per bank

	Browser				Operating System			
	IE6/IE7	Firefox/Mozilla	Safari	Other	Windows	Mac	Linux	Linux LiveCD
No. of users	33	102	7	5	95	13	34	2
% of users	23	69	5	3	66	9	24	1

Table 4: Browser and OS usage

	Anti-virus			Firewall			Anti-spyware		
	Yes	No	Some	Yes	No	Some	Yes	No	Some
Users	61	27	14	77	14	10	45	35	15
%	60	26	14	76	14	10	47	37	16

Table 5: Anti-malware usage

	OS		Browser		Anti-malware	
	Yes	No	Yes	No	Yes	No
Users	114	12	118	6	85	18
%	90	10	95	5	83	17

Table 6: Maintaining an up-to-date system

	P2P file sharing		Windows file sharing	
	Yes	No	Yes	No
Users	62	42	45	56
%	60	40	45	55

Table 7: File sharing from the online banking PC

	Sign-out		Clear cache		Close browser	
	Yes	No	Yes	No	Yes	No
Users	99	7	32	66	55	48
%	93	7	33	67	53	47

Table 8: Actions at the end of a banking session

	Unique password		Unique PVQs	
	Yes	No	Yes	No
No. of users	71	32	56	37
% of users	69	31	60	40

Table 9: Unique passwords and PVQs

	Read agreement			State 3 conditions			
	Yes	No	Other	None	One	Two	Three
No. of users	31	68	6	93	5	6	6
% of users	29	65	6	85	5	5	5

Table 10: Agreement and requirement awareness

	Password change		Bank statement check	
	Within a year	Don't change	Within a month	Don't check
No. of users	32	70	100	2
% of users	31	69	98	2

Table 11: Password change and bank statement check frequency

the conditions.' Another wrote 'too many requirements to ensure. I don't trust the bank to pay up if something goes wrong.' Other comments for not using online banking were 'do not trust it,' 'too insecure' etc.

Table 3 lists the number of users per bank. Many users reported to have accounts with multiple banks, which implies these users must maintain several unique passwords, PINs, and (optionally) PVQs. Most participants use Firefox/Mozilla on Windows (Table 4) – indicating a technically-biased survey group. Many participants use multiple web browsers and/or operating systems for online banking. Although Firefox/Mozilla is very popular, Scotiabank and PC Financial do not list it as a recommended browser. All banks support Netscape, but none in our survey reported using it. Two-thirds of IE users use IE6 even after months of the release of IE7, i.e., many users do not use the latest 'secure' browser version as recommended for online banking. (Note that IE7 is a 'critical update' according to Microsoft.) Linux is used by almost a quarter of the participants; two of them use Linux LiveCD. Banks do not explicitly mention support of Linux (except RBC) or LiveCD, although these are apparently better choices for secure OS.[12] Using LiveCD may seem paranoid, and shows users' lack of trust of commodity operating systems (which may be justified as regular OS installations are commonly infested with several forms of malware). Linux and Mac users may find it difficult to comply with banks' anti-malware requirements as there are only few anti-virus and anti-spyware products for those platforms.

Table 5 summarizes anti-malware use. Most users (76%) have a firewall on all machines that they use for online banking, while 10% do not use any firewall and 14% use firewall on some machines. Less than half of the users always use anti-spyware on machines used for banking. More than a quarter of the participants do not use anti-virus at all. Most users also keep their OS, browser and anti-malware updated (Table 6). We also collected statistics on update mechanisms (auto/manual). Many users use both automatic and manual updates (we added them together), and some use automatic

[12]Although banks recommend Windows and Mac as preferred OS, one analysis [71] reported that before patched, both Windows XP and Mac OS X offer attackers more remotely exploitable vulnerabilities than Linux variants.

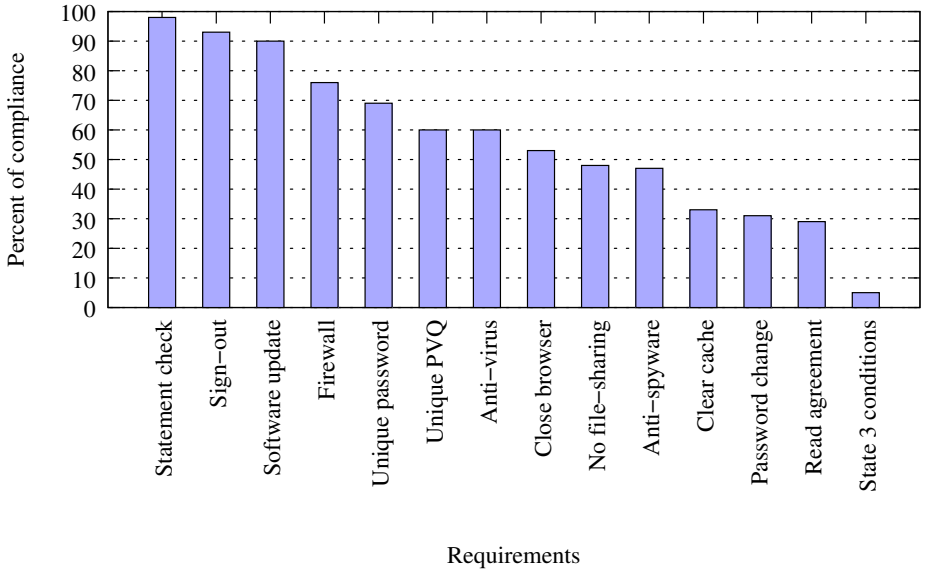

Figure 1: Summary of conformance

notification but manual update. Auto updates are used by 70% (OS), 77% (browser), and 74% (anti-malware) of the users who keep their systems updated. One user does not update the OS or browser but relies on a firewall for protection against network attacks. Another updates 'only if forced.' Some users do not update their firewall as it requires a firmware upgrade of a home router. One user commented that updating anti-malware is 'a pain.' Around half of the users use P2P software and/or Windows file sharing (Table 7) against some banks' recommendations. However, a few users mentioned that they do not run P2P clients while performing online banking. One user reported to use an admin account for online banking, and a regular user account for running P2P.

Only few users do not sign-out from online banking when they are done (Table 8). One user even reported to reboot the PC after a banking session. However, compliance with clearing the browser cache (one-third) or closing the browser (just over one half) is pretty low. Two users mentioned using the auto clear cache feature of Firefox. Closing the browser after a banking session is being 'rather too paranoid' according to one user.

A significant portion of the users do not use unique passwords or PVQs (31% and 40% respectively), and 69% of users do not change their password (Tables 9 and 11). Only four users reported changing their banking password every month. Apparently most users, and more specifically PC Financial users, do not follow the 'frequent' password change recommendation. One user's comment about PVQs was 'I hate those questions.' Another commented that 'I hope I will remember them' (cf. [63]).

65% of the participants did not read any banking agreements (Table 10), although all banks assume their customers have 'have read and agreed' to all related banking policies when users sign on to online banking. Several users commented that they only skimmed through these agreements. One mentioned reading the agreements, 'but did not understand [those] at all.' Another reported these agreements and policies as 'too complicated to understand.' One participant does not use online banking as a result of carefully reading the online banking agreement.

85% of the participants (Table 10) were unable to state any major conditions for being eligible for the 100% reimbursement guarantee.[13] Only six users (5%) could state three conditions although some of those were not accurate; two of them mentioned to be aware of these conditions as they were present in our previous class talk. Several participants answered as 'not a clue,' 'no idea,' 'impossible conditions to achieve' etc. One mentioned 'use their credit card' as a requirement (we did not count such answers as valid). We believe that participants could easily state three conditions directly from the questionnaire if they had read online banking agreements; note that 29% of the participants claimed to have read the banking agreements, and thus we believe participants over-reported this item.

Most users apparently check their bank statements within a month. Several check their statements weekly or even daily, although we did not ask "how diligently." Two participants mentioned not checking their statements. Note that all banks require users to check statements carefully and to report any errors promptly. If a fraudulent transaction is not reported within a certain period (generally 30 days), banks may refuse any reimbursement.

Summary of results. Many users reported using Firefox/Mozilla; we did not collect data on versions. Most IE users use IE6 which is less secure than IE7 (according to Microsoft). Many users use Linux, but other than RBC, no banks explicitly mention supporting it. A significant portion (about 50%) of participants do not comply with anti-virus, close-browser, and unique password/PVQ requirements (or recommendations). The majority (more than 50%) do not comply with the requirements (or recommendations) regarding anti-spyware, file-sharing, clear-cache, password change, and reading agreement. Very few participants were able to state three conditions for the 100% reimbursement guaran-

[13]Some participants may have simply been too lazy to answer; we cannot tell as we held no follow-up interviews.

tee. Almost all participants sign-out from online banking, and check their bank statements. Firewalls are deployed by a good portion of the participants. Most also reported to keep their OS, browser, and anti-malware software up-to-date; note, however, that many IE6 users did not upgrade to IE7. Figure 1 summarizes our findings.

9. CONCLUDING REMARKS

Banks advertise that users can start online banking 'in minutes.' However, to comply with the security requirements and recommendations, we expect most users would be delayed hours or days, if indeed technically capable of doing so at all. Banks state that security is a 'shared responsibility.' Our analysis and survey suggest that the users' share of this responsibility is large and unrealistic given the current Internet environment and available technologies. Most participants did not fulfill all the listed requirements in our survey. We argue that if such predominantly technical and security-aware participants fail to satisfy online banking requirements, expecting average home users to meet all such requirements is extremely naïve. Therefore, we conclude that most average users are ineligible for the 100% reimbursement guarantee banks assert, and doing online banking with 'confidence' and 'peace of mind' is no more than a marketing slogan which misleads users.

Indeed, as simply one recent example, in January 2007, CIBC reported the loss of a computer hard drive with unencrypted personal financial information (including name, address, social insurance number, date of birth, signature) of about 470,000 mutual fund customers [47].[14] Many Canadian customers are also affected by the recently-reported (Mar. 2007) TJX data breach [13] of about 45 million users. In customer agreements, banks do not indicate how they would notify or compensate users in such incidents. Note that Canadian banks are currently not legally bound to disclose such breaches. Banks also do not specify whether users will be reimbursed other than for monetary losses, e.g., time lost in recovering from financial fraud and theft. Banks discourage users using P2P file-sharing from the same PC as they perform online banking with; ironically, analyzing P2P traffic for 'inadvertently' disclosed sensitive files of top 30 US banks, Johnson et al. [36] reported to discover a significant number of files with confidential banking information, including a spreadsheet with personal details of 23,000 business accounts, and a detailed manual of a bank's security review process.

As stated in an updated personal account agreement (effective from April 1, 2007), CIBC may close a customer's bank account 'without notice...to prevent future losses if you are a victim of fraud.' Thus a defrauded customer may lose her bank account as a consequence of using the heavily advertised 'free' online banking service, and thereby becoming a *double victim*. Banks emphasize that as long as users maintain the 'security' of a bank card number and password, no one can gain access to their online banking accounts. One bank (CIBC) also assures customers that the bank will not 'provide [any] service that compromises the security and confidentiality of customer information.' In contrast, new malware attacks (*bank-stealing Trojans* or *session-hijacking*, e.g. Win32.Grams [11]; see also CERT [46]) can perform fraudulent transactions in real-time after a user has logged into an online banking account. Banks do not specifically advise users how to protect against such attacks, nor do they explain how unique 'rock-solid' passwords, 128-bit SSL encryption or other 'enhanced' security techniques may help users against these attacks. In fact, most existing or proposed solution techniques are susceptible to these new attacks (e.g. including [55] and two-factor authentication such as a password plus a passcode generator token). Banks may reimburse any money lost due to online banking, at least when users meet banks' requirements; however, users pay with their own personal time and mental energy to address consequences of credit-card fraud and identity theft as enabled in part by the use of online banking. In general, we argue that several security-sensitive online services are now being offered (and even heavily pushed) to average home users without the availability of appropriate *usable* tools to perform those tasks safely. The growing disconnect between service providers' expectations, and technical capabilities of the general user population, may result in increasing loss of trust in the web over the long run.

[14] See `http://www.caslon.com.au/datalossnote2.htm` for well-known consumer data losses from major banks.

Acknowledgements

We thank anonymous NSPW reviewers for their comments, and NSPW 2007 attendees and members of the Carleton's Digital Security Group for their enthusiastic discussion on this topic. The first author is supported in part by an NSERC CGS. The second author is Canada Research Chair in Network and Software Security, and is supported in part by an NSERC Discovery Grant, and the Canada Research Chairs Program.

10. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Comm. of the ACM*, 42(12), 1999.

[2] J. Aitel. The IPO of the 0day: Stock fluctuation from an unrecognized influence. In *Symposium on Security for Asia Network (SyScan)*, 2007. Keynote address.

[3] ArsTechnica.com. Half of Americans clueless about online threats. News article (Aug. 14, 2007).

[4] J. Aycock and N. Friess. Spam zombies from outer space. In *EICAR*, 2006.

[5] BBC News. Malware 'hijacks Windows Updates'. News article (May 16, 2007).

[6] A. Bellissimo, J. Burgess, and K. Fu. Secure software updates: Disappointments and new challenges. In *USENIX Workshop on Hot Topics in Security (HotSec)*, 2006.

[7] J. Benamati, M. A. Serva, and M. A. Fuller. Are trust and distrust distinct constructs? An empirical study of the effects of trust and distrust among online banking users. In *IEEE Hawaii International Conference on System Sciences*, 2006.

[8] Beskerming.com. How the online trust model is broken - the BankOfIndia.com attack. News article (Aug. 31, 2007).

[9] M. Bishop. Psychological acceptability revisited. In "Security and Usability: Designing Secure Systems that People Can Use." Edited by L. Cranor and S. Garfinkel. O'Reilly, 2005.

[10] J. Blascovich. Mind games: A psychological analysis of

common email scams. McAfee Avert Labs white paper (June 25, 2007).

[11] CA Virus Information Center. Win32.Grams.I, Feb. 2005. http://www3.ca.com.

[12] W. Chung and J. Paynter. An evaluation of Internet banking in New Zealand. In *IEEE Hawaii International Conference on System Sciences*, 2002.

[13] CNET.com. TJX says 45.7 million customer records were compromised. News article (Mar. 29, 2007).

[14] Commtouch.com. Malware outbreak trend report: Storm-Worm. Online article (Jan. 31, 2007). http://www.commtouch.com/downloads/Storm-Worm_MOTR.pdf.

[15] ComputerWorld.com. Symantec false positive cripples thousands of Chinese PCs. News article (May 18, '07).

[16] Consumeraffairs.com. Consumers losing confidence in online commerce, banking. News article (June 28, '05).

[17] DarkReading.com. Antivirus tools underperform when tested in LinuxWorld 'Fight Club'. News article (Aug. 9, 2007).

[18] D. Davis. Compliance defects in public-key cryptography. In *USENIX Security Symposium*, 1996.

[19] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *CHI*, 2006.

[20] J. S. Downs, M. Holbrook, and L. F. Cranor. Decision strategies and susceptibility to phishing. In *SOUPS*, 2006.

[21] K. Edge, R. Raines, M. Grimaila, R. Baldwin, R. Bennington, and C. Reuter. The use of attack and protection trees to analyze security for an online banking system. In *IEEE Hawaii International Conference on System Sciences*, 2007.

[22] Entrust.com. Katrina scams show browser security model is broken. Entrust blog (Sep. 9, 2005).

[23] eWeek.com. Microsoft patches causing breakages, lockups. News article (Apr. 17, 2006).

[24] eWeek.com. Microsoft says recovery from malware becoming impossible. News article (Apr. 4, 2006).

[25] D. Florêncio and C. Herley. A large-scale study of web password habits. In *World Wide Web (WWW)*, 2007.

[26] S. Gaw and E. W. Felten. Password management strategies for online accounts. In *SOUPS*, 2006.

[27] R. L. Glass. Patching is alive and, lamentably, thriving in the real-time world. *ACM SIGPLAN Notices*, 13(3), 1978.

[28] Globe and Mail. globeandmail.com: Mary Kirwan. News article (Nov. 16, 2006). http://www.theglobeandmail.com/servlet/story/RTGAM.20061116.gtkirwan1116/BNStory/Technology/home.

[29] S. J. Greenwald, K. G. Olthoff, V. Raskin, and W. Ruch. The user non-acceptance paradigm: INFOSEC's dirty little secret. In *New Security Paradigms Workshop (NSPW)*, 2004.

[30] J. Grossklags and N. Good. Empirical studies on software notices to inform policy makers and usability designers. In *Workshop on Usable Security (USEC)*, 2007.

[31] J. Heasman. Implementing and detecting a PCI rootkit. White paper (Nov. 15, 2006). http://www.ngssoftware.com.

[32] M. Hertzum, N. Jørgense, and M. Nørgaar. Usable security and e-banking: Ease of use vis-à-vis security. *Australasian Journal of Information Systems*, 11, 2004.

[33] A. Herzogl and N. Shahmehri. Usability and security of personal firewalls. In *IFIP Security Conference*, 2007.

[34] C. Jackson, D. Simon, D. Tan, and A. Barth. An evaluation of Extended Validation and picture-in-picture phishing attacks. In *Workshop on Usable Security (USEC)*, 2007.

[35] N. Jin and M. Fei-Cheng. Network security risks in online banking. In *IEEE Wireless Communications, Networking and Mobile Computing*, 2005.

[36] M. E. Johnson and S. Dynes. Inadvertent disclosure – information leaks in the extended enterprise. In *Workshop on the Economics of Information Security (WEIS)*, 2007.

[37] M. Just. Designing secure yet usable challenge question authentication systems. In "Security and Usability: Designing Secure Systems that People Can Use." Edited by L. Cranor and S. Garfinkel. O'Reilly, 2005.

[38] H. Karjaluoto, T. Koivumäki, and J. Salo. Individual differences in private banking: Empirical evidence from Finland. In *IEEE Hawaii International Conference on System Sciences*, 2003.

[39] Kaspersky.com. Malicious mass mailing sent using McAfee email address. Virus News (Nov. 2, 2006).

[40] Keynote.com. Online banking critical to bank selection and brand perception. Press release (Jan. 6, 2005).

[41] S. T. King, P. M. Chen, Y.-M. Wang, C. Verbowski, H. J. Wang, and J. R. Lorch. SubVirt: Implementing malware with virtual machines. In *IEEE Symposium on Security and Privacy*, 2006.

[42] MacDevCenter.com. How Paris got hacked? News article (Feb. 22, 2005).

[43] McAfee and National Cyber Security Alliance (NCSA). McAfee-NCSA online safety study, Oct. 2007.

[44] Microsoft. Password checker. http://www.microsoft.com/athome/security/privacy/password_checker.mspx.

[45] Microsoft Support. Detailed installation walkthrough for Windows XP Service Pack 2. http://support.microsoft.com.

[46] J. Milletary. Technical trends in phishing attacks. US-CERT, Reading room article, http://www.us-cert.gov.

[47] National Post. Watchdog pushed CIBC on lost file. News article (Jan. 26, 2007). http://www.canada.com.

[48] Netcraft.com. Bank, customers spar over phishing losses. News article (Sep. 13, 2006).

[49] Netcraft.com. More than 450 phishing attacks used SSL in 2005. News article (Dec. 28, 2005).

[50] Netcraft.com. Myspace accounts compromised by phishers. News article (Oct. 27, 2006).

[51] New Zealand Bankers' Association (NZBA). Code of banking practice. Fourth Edition (July, 2007).

[52] M. Nilsson, A. Adams, and S. Herd. Building security and trust in online banking (extended abstracts). In *CHI*, 2005.

[53] C. Nodder. Users and trust: A Microsoft case study. In "Security and Usability: Designing Secure Systems

that People Can Use." Edited by L. Cranor and S. Garfinkel. O'Reilly, 2005.

[54] Office of the Privacy Commissioner of Canada. Guidelines for identification and authentication, Oct. 2006. http://www.privcom.gc.ca/information/guide/auth_061013_e.asp.

[55] B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. In *Financial Cryptography (FC)*, 2006.

[56] J. Rutkowska. Introducing Blue Pill, June 2006. Presented at SyScan Conference.

[57] SANS Institute Internet Storm Center. Windows XP: Surviving the first day, Nov. 2003.

[58] SANS Internet Storm Center. Fake microsoft patch email -> fake spyware doctor! Handler's diary (June 26, 2007).

[59] SANS Internet Storm Center. Symantec false-positive on Filezilla, NASA World Wind. Handler's diary (July 16, 2007).

[60] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology*, 19(3), 2001.

[61] M. A. Sasse and I. Flechais. Usable security: Why do we need it? how do we get it? In "Security and Usability: Designing Secure Systems that People Can Use." Edited by L. Cranor and S. Garfinkel. O'Reilly, 2005.

[62] scanit.be. Browser security test: A year of bugs, 2004. http://bcheck.scanit.be.

[63] B. Schneier. The curse of the secret question. Blog (Feb. 11, 2005), http://www.schneier.com.

[64] SecurityFocus.com. Bot spreads through antivirus, Windows flaws. News article (Nov. 28, 2006).

[65] A. Shipp. Targeted trojan attacks and industrial espionage. In *Virus Bulletin Conference (VB)*, 2006.

[66] Silicon.com. Banks must boost security to drive online banking. Forrester Research News article (Mar. 29, 2005).

[67] A. Singer. Life without firewalls. *;login: The USENIX Magazine*, 28(6), 2003.

[68] S. Singh. The social dimensions of the security of Internet banking. *Journal of Theoretical and Applied Electronic Commerce Research*, 1(2), 2006.

[69] Statistics Canada. Canadian Internet Use Survey 2005, Aug. 2006. http://www.statcan.ca.

[70] M. Tulloch. Resolving Windows XP SP2 – related application compatibility problems. Microsoft article on using XP.

[71] M. Vea. 2006 Operating System vulnerability summary. Online article published at OmniNerd.com (Mar. 26, 2007).

[72] C. Wharton, J. Rieman, C. Lewis, and P. Polson. The cognitive walkthrough method: A practitioner's guide. In "Usability inspection methods," John Wiley & Sons, Inc., 1994.

[73] A. Whitten and J. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX Security Symposium*, 1999.

[74] WindowsSecrets.com. Microsoft, McAfee, Symantec charge cards repeatedly. News article (May 17, 2007).

[75] M. Wu, R. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks. In *CHI*, 2006.

[76] J. J. Yan. A note on proactive password checking. In *New Security Paradigm Workshop (NSPW)*, 2001.

[77] ZDNet.com. Security tools face increased attack. News article based on Yankee Group report (June 20, 2005).

[78] ZDNet.com.au. Eighty percent of new malware defeats antivirus. News article (July 19, 2006).

[79] Y. Zhang, S. Egelman, L. F. Cranor, and J. Hong. Phinding phish: An evaluation of anti-phishing toolbars. In *Annual Network and Distributed System Security Symposium (NDSS)*, 2007.

[80] M. E. Zurko. User-centered security: Stepping up to the grand challenge. In *ACSAC*, 2005. Invited essay.

[81] M. E. Zurko and R. T. Simon. User-centered security. In *New Security Paradigms Workshop (NSPW)*, 1996.

[82] M. Zviran and W. J. Haga. Cognitive passwords: the key to easy access control. *Computers & Security*, 9(9), 1990.

APPENDIX

On the following page, we attach the questions used for the survey reported in Section 8.

A. SURVEY QUESTIONNAIRE

The following questions were included in our survey.

1. Do you use online banking?
   ☐ Yes ☐ No Comments _____
   (If No, you don't need to answer the following questions.)
2. Which bank do you use for online banking?
   ☐ Prefer not to say ☐ RBC ☐ CIBC ☐ TD Canada Trust ☐ Scotiabank
   ☐ BMO ☐ PC Financial ☐ Other _____
3. What browser do you use for online banking?
   ☐ Internet Explorer 6 (IE6) ☐ IE7 ☐ Firefox ☐ Mozilla ☐ Netscape ☐ Opera
   ☐ Safari ☐ Konqueror ☐ Other _____
4. What operating system (OS) do you use for online banking?
   ☐ Windows ☐ Mac ☐ Linux ☐ Linux LiveCD ☐ Don't know
   ☐ Other _____
5. Do you keep your operating system (OS) up-to-date with security patches?
   ☐ Yes, by ☐ No ☐ Don't know Comments _____
   ☐ automatic update
   ☐ manual update
   ☐ don't know
6. Do you keep your web browser up-to-date with security patches?
   ☐ Yes, by ☐ No ☐ Don't know Comments _____
   ☐ automatic update
   ☐ manual update
   ☐ don't know
7. Do you have the following anti-malware tools in some or all computers you use for online banking?
   (a) Anti-virus: ☐ Yes on all ☐ Yes on some ☐ No ☐ Don't know
   (b) Firewall (software or hardware): ☐ Yes on all ☐ Yes on some ☐ No ☐ Don't know
   (c) Anti-spyware: ☐ Yes on all ☐ Yes on some ☐ No ☐ Don't know
8. Do you keep your anti-malware tools up-to-date with updates and security patches?
   ☐ Yes, by ☐ No ☐ Don't know Comments _____
   ☐ automatic update
   ☐ manual update
   ☐ don't know
9. On the same computers that you use for online banking:
   (a) Do you run file-sharing or P2P software, e.g., bittorrent, eMule, KaZaA?
   ☐ Yes ☐ No ☐ Don't know Comments _____
   (b) Do you use Windows file sharing (e.g., sharing files on LAN, default is ON) on them?
   ☐ Yes ☐ No ☐ Don't know Comments _____
10. When you are finished with an online banking session which of the following do you do promptly:
    (a) Sign-out from your bank: ☐ Yes ☐ No ☐ Don't know Comments _____
    (b) Clear the browser cache: ☐ Yes ☐ No ☐ Don't know Comments _____
    (c) Close the browser: ☐ Yes ☐ No ☐ Don't know Comments _____
11. How frequently do you change your online banking password?
    ☐ Monthly ☐ Yearly ☐ Don't change ☐ Don't know ☐ Other _____
12. How often do you check your bank statements?
    ☐ Weekly ☐ Monthly ☐ Don't check ☐ Don't know ☐ Other _____
13. Did you read your banking agreement, privacy and security policies of your bank?
    ☐ Yes ☐ No ☐ Don't know ☐ Other _____
14. Do you use a unique password (i.e., not related to your other passwords) for online banking?
    ☐ Yes ☐ No ☐ Don't know ☐ Other _____
15. Do you use unique personal verification questions and answers for online banking?
    ☐ Yes ☐ No ☐ Don't know ☐ Not applicable ☐ Other _____
16. All major Canadian banks provide 100% reimbursement guarantee in case of online frauds, if you comply with their policy. If you know them, state up to three major conditions that your bank requires you to fulfill to be eligible for such reimbursements.

    (a)_____ (b)_____ (c)_____