Banking Securely Online

MARK RESCHER, US-CERT

Introduction

The rise of online banking presents new challenges to your financial security and personal privacy. Market research group Gartner reported that from June 2003 through June 2004 almost two million Americans had their checking accounts compromised, mainly as a result of online banking. With internet use on the rise, the number of incidents will only increase. If you are going to use online banking to conduct financial transactions, you should make yourself aware of the risks and take precautions to minimize them. The following practices, which are discussed further in this paper, can help you avoid common security problems associated with online banking:

- Review all privacy and policy information
- Use unique and hard to guess login information
- Protect your computer
- Check your account balance regularly
- Pay using credit cards
- Do not access your account from public locations
- Verify email correspondence from bank
- If your account is compromised, take swift action

Attacks that Target Online Banking

Several types of electronic fraud specifically target online banking. Some of the more popular types are described below:

Phishing attacks

Phishing attacks use fake email messages from an agency or individual pretending to represent your bank or financial institution. The email asks you to provide sensitive information (name, password, account number, and so forth) and provides links to a counterfeit web site. If you follow the link and provide the requested information, intruders can access your personal account information and finances (see "Recognizing and Avoiding Email Scams" for more information). In some cases, pop-up windows can appear in front of a copy of a genuine bank web site**.** The real web site address is displayed; however, any information you type directly into the pop-up will go to unauthorized users (for a more technical discussion, see "Technical Trends in Phishing Attacks" at http://www.us-cert.gov/reading_room/phishing_trends0511.pdf).

Malware

Malware is the term for maliciously crafted software code. Special computer programs now exist that enable intruders to fool you into believing that traditional security is protecting you during online banking transactions. Attacks involving malware are a factor in online financial crime (see "Technical Trends in Phishing Attacks" for more information). In fact, it is possible for this type of malicious software to perform the following operations:

- **Account information theft** - Malware can capture the keystrokes for your login information. Malware can also monitor and capture other data you use to authenticate your identity (for example, special images that you selected or "magic words" you chose).
- **Fake web site substitution** - Malware can generate fake web pages that replace your bank's legitimate web site. Such a "man-in the-middle attack" site enables an attacker to intercept your user information. The attacker adds additional fields to the copy of the web page opened in your browser. When you submit the information, it is sent to both the bank *and* the malicious attacker without your knowledge.
- **Account hijacking** - Malware can hijack your browser and transfer funds without your knowledge. When you attempt to login at a bank web site, the software launches a hidden browser window on your computer, logs in to your bank, reads your account balance, and creates a secret fund transfer to the intruder-owned account.

Pharming

Pharming attacks involve the installation of malicious code on your computer; however, they can take place without any conscious action on your part. In one type of pharming attack, you open an email, or an email attachment, that installs malicious code on your computer. Later, you go to a fake web site that closely resembles your bank or financial institution. Any information you provide during a visit to the fake site is made available to malicious users.

All the attack types listed above share one characteristic; they are created using technology but, in order to succeed, they need you to provide information:

- In phishing attacks, you must provide the information or visit links.
- With malware, you must be tricked into performing actions you would not normally do. You would have to install the malware on your computer either by running a program, such as an email attachment, or by visiting a web site through email or instant message link. Then, you would have to submit your bank login information. Your financial information would be at risk only after you performed all these steps.
- With pharming attacks, you must open an email, or email attachment, to become vulnerable. You then visit a fake website and, without your knowledge, provide information that compromises your financial identity.

Tips for Safe Online Banking

When it comes to online banking, there is no way to absolutely guarantee your safety. However, good practices do exist that can reduce the risks posed to your online accounts. The following sections describe these practices.

Review your bank's information about its online privacy policies and practices.

By law, banks are required to send you a copy of their privacy policies and practices annually; you may also request a copy of this information (see "Electronic Code of Federal Regulations *Title 16: Commercial practices, Part 313.9 – Delivering Privacy and Opt Out Notices* " for more information). Bank web sites should also have this information. As you read this information, pay particular attention to any mention of the methods used for encrypting transactions and authenticating user information. Also, check the information to see if the bank requires additional security information before authorizing a payment to a business or individual that has never received a payment before.

Before setting up any online bill payment, check the privacy policy of the company or service you will be sending payment to.

You have the right to limit the information an online bank shares with both its parent organization and any other financial institutions (see "Protecting Your Privacy" and "How Anonymous Are You?" for more information). **Be aware that some online banks may have separate procedures for handling each of these requests.** You may also want to use a service such as the Better Business Bureau to view any existing history of outstanding consumer complaints about privacy violations.

For security purposes, choose an online personal identification number (PIN) that is unique and hard to guess.

Be sure to change your PIN regularly. Do not choose a PIN that contains personal information such as your birthday or Social Security number; an attacker might be able to guess these. Regardless of the circumstances, never give someone access to your current PIN number (see "Choosing and Protecting Passwords" for more information).

Install anti-virus, firewall, and anti-spyware programs on your computer and keep them up to date.

Installing and updating this software protects your computer and its contents against unauthorized access. You should turn on automatic updates for these programs or, if prompted, always agree to download system updates as soon as they are available (see "Understanding Anti-Virus Software," "Understanding Firewalls," and "Recognizing and Avoiding Spyware" for more information).

Regularly check your online account balance for unauthorized activity.

Timing is a factor in your response to unauthorized electronic fund transactions. If you receive a paper account balance, make sure that you reconcile it with your online balance.

Use a credit card to pay for online goods and services.

Credit cards usually have stronger protection against personal liability claims than debit cards. Some credit cards limit personal liability for unauthorized transactions to $50. Personal liability for debit cards can be higher. According to the Federal Reserve's Regulation E, if you report an electronic fund transaction problem involving debit cards to a bank or financial institution in the first two days, you are only liable for $50. Reporting that same incident between 3 and 60 days increases your personal liability to $500. After 60 days, there are no financial restrictions placed on your personal liability (see "Electronic Code of Federal Regulations (e-CFR). *Title 12: Banks and Banking, Part 205 – Electronic Fund Transfers (Regulation E)*" for more information).

Avoid situations where personal information can be intercepted, retrieved, or viewed by unauthorized individuals.

You should conduct online bank transactions in locations that are not subject to public monitoring. When you are entering login information, you should avoid using unsecured or public network connections (for example, at a coffee shop or library). As a general rule, you should avoid using any computer that other people can freely access; the end result could be unauthorized access of your financial information. Remember, it is possible for your account information to be stored in the web browser's temporary memory (see "Guidelines for Publishing Information Online" for more information).

If you receive email correspondence about a financial account, verify its authenticity by contacting your bank or financial institution.

You should not reply to any email requests for security information, warnings of an account suspension, opportunities to make easy money, overseas requests for financial assistance, and so forth. Also, links found in these suspicious emails should not be clicked. Forward a copy of the suspicious email to the Federal Trade Commission at uce@ftc.com and then delete the email from your mailbox.

If you have disclosed financial information to a fraudulent web site, file reports with the following organizations:

- your bank
- the local police
- the Federal Trade Commission – http://www.ftc.gov
- the Internet Crime Complaint Center – http://www.ic3.gov
- the three major credit bureaus – Equifax, Experian, and TransUnion (see "Preventing and Responding to Identity Theft" for more information).

Conclusion

Online banking involves certain risks. It is important to educate yourself about these risks, how unauthorized access to your financial information occurs, and the steps you can take to protect your financial information. Learning about your rights and responsibilities as an online banking consumer can make a difference to your financial well-being by changing the age-old saying “A penny saved is a penny earned” to “A penny saved is a penny kept.”

References and Further Reading

Arnfield, Robin. Enterprise Security. "Banks Get Wise to Phishing Fraud." *NewsFactor Magazine Online*, May 15, 2006. http://www.newsfactor.com/story.xhtml?story_id=03300000UMLI.

Bank of America. *Online Practices Privacy Policy*. http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_onlin.

Bank of America. *Reporting & Resolving Fraud.* http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_unauthorised_acc_use.

Crawford, Michael. "Social engineering replaces guns in today's biggest bank heists." *Computerworld*, May 15, 2006. http://www.computerworld.com.au/index.php/id;736453614.

Electronic Code of Federal Regulations (e-CFR). *Title 12: Banks and Banking, Part 205 – Electronic Fund Transfers (Regulation E).* http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr;sid=11057238dc784417ec286eb70e1831f7;rgn=div5;view=text;node=12%3A2.0.1.1.5;idno=12;cc=ecfr.

Electronic Code of Federal Regulations (e-CFR). *Title 16: Commercial Practices, Part 313 – Privacy of Consumer Financial Information*. http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=cc73f177a89c3d4458ed52195abf00e3&rgn=div5&view=text&node=16:1.0.1.3.37&idno=16.

Federal Deposit Insurance Corporation. *Safe Internet Banking*. http://www.fdic.gov/consumers/consumer/index.html

The Federal Reserve Bank of Boston. *Phishing and Pharming: Helping Consumers Avoid Internet Fraud*. http://www.bos.frb.org/consumer/phishpharm/index.htm.

Federal Trade Commission. *Taking Charge: Fighting Back Against Identity Theft (formerly: "ID Theft: When Bad Things Happen to Your Good Name").* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

Grimes, Roger A. "How SSL-Evading Trojans Work." *InfoWorld*, May 1, 2006. http://www.infoworld.com/article/06/05/01/77515_18FEsslmalwareworks_1.html.

Grimes, Roger A. “E-Commerce in crisis: When SSL isn’t safe.” *Computerworld*, May, 17, 2006. http://www.computerworld.com.au/pp.php?id=822775843.

Liberman, Gail & Lavine, Alan. Consumer Watch. “If you go online, watch your bank accounts.” *MarketWatch*, May 15, 2006. http://www.marketwatch.com/News/Story/Story.aspx?guid=%7BC2858553-3D00-4668-853D-9BA0FC31FD90%7D.

Milletary, Jason. *Technical Trends in Phishing Attacks*. http://www.us-cert.gov/reading_room/phishing_trends0511.pdf.

The Office of the Comptroller of the Currency. *Consumer Protection News: Internet Pirates Are Trying to Steal Your Personal Financial Information*. http://www.occ.gov/consumer/phishing.htm.

The Office of the Comptroller of the Currency. *Consumer Protection News: OCC Fighting Identity Theft*. http://www.occ.gov/Consumer/idtheft.htm.

Sabatini, Patricia. Business News. “Debit card fraud grows.” *post-gazette.com*, May 5, 2006. http://www.post-gazette.com/pg/06125/687615-68.stm.

Sullivan, Bob. Online Banking Special Report. “Online banking fraud concerns customers: Account holder rights vary based upon situation.” *MSNBC.com*, December 14, 2004. http://www.msnbc.msn.com/id/6713033/.

Sullivan, Bob. Online Banking Special Report. “Survey: 2 million bank accounts robbed: Criminals taking advantage of online banking, Gartner says.” *MSNBC.com*, June 14, 2004. http://www.msnbc.msn.com/id/5184077/.