FISHER FINANCIAL
STRATEGIES

Financial Strategies

JUNE 2007

Our June edition of Financial Strategies starts where we left off, with the topic of identity fraud.

As noted in the last newsletter, only about 10 to 15% of identity thefts with known causes have been attributed to online data theft. This statistic is not very reassuring, though. According to the Identity Theft Assistance Center, only 42% of ID theft victims are able to determine how their information was stolen. If the majority of victims don't know how their information was stolen, it may not be safe to assume that the 10–15% figure accurately represents all ID theft losses attributable to online sources.

There is some good news regarding ID theft crimes in general: the number of reported thefts has been declining in recent years, to fewer than nine million cases per year. However, the size of the average online ID theft loss is on the rise. A recent study by Javelin Strategy and Research[1] found that the average theft loss from paper mail fraud is about $4,200, while the average loss arising from viruses, spyware, and hacker-related thefts exceeded $7,000. The recent theft of 45.7 million credit and debit card numbers from TJX Companies' central database[2] demonstrates how attractive electronic ID theft has become to organized criminals. Obviously, no one can be completely protected against losses resulting from an attack on a commercial database. But it is possible to make your own home computers less susceptible to online identity theft. We'll discuss the means through which personal information can be lost online and offer some guidelines for protecting your information.

1. "Pushing Paperless: The Pros and Cons," by Eleanor Laise, Wall Street Journal, May 2, 2007.

2. "How Credit-Card Data Went Out Wireless Door," By Joseph Periera, Wall Street Journal, May 4, 2007

FORMS OF ELECTRONIC IDENTITY THEFT

As financial institutions and other companies develop greater security for the information in their corporate databases, criminals will need to become more sophisticated in order to obtain data by attacking these sources. However, there are a number of simple schemes that thieves with more modest means can use to steal personal information electronically. There are reportedly websites that offer turnkey software packages to criminals who want to employ electronic theft techniques. Generally speaking, the most common forms of online theft either involve the use of e-mail "spam," fraudulent websites, and/or unauthorized access to a computer made through an internet connection.

E-MAIL SCHEMES

Fraudulent attacks using e-mail are almost invariably carried out using what is known as "social engineering," which involves tricking someone into taking an action that exposes them to a loss. In a less technological age, practitioners of social engineering were known as "con artists." Presumably, everyone receives as many spam e-mails as I do purporting to be from lawyers in Nigeria (or soldiers in Iraq) who are eager to give me millions if only I'll help them out. This is one of the simplest forms of social engineering—yet it still works occasionally, because human nature hasn't changed.

TROJAN HORSES

Although most computer users know the risks of opening phony e-mail attachments, e-mail continues to be an effective medium for scam artists. The Trojan horse, a software incarnation of

the Greek gift recounted in Virgil's Aeneid, is a program that sneaks onto your computer by stealth and does unpleasant things, like recording your keystrokes as you log onto your bank account and sending the information to a thief. Your computer can become infected by a Trojan horse when you open an attached file in an e-mail or through a file downloaded from a website. Since Trojan programs often possess the capability to e-mail themselves to other addresses, be very cautious with e-mail attachments, even when they're from people known to you, if they accompany messages that seem peculiar or terse. Keep in mind that your first line of defense against this kind of attack is not your antivirus software; your own decisions are critical. You should not download files from a web site unless you are confident that it's a legitimate site.

PHISHING FOR TROUBLE

"Dear Amazon Customer, This is your final warning about the safety of your Amazon account. If you do not update your billing information your access to Amazon features will be restricted and the user deleted…."

So begins the text of an e-mail I received earlier this year, one of many similar messages that my spam filter catches weekly. Notice how the text is designed to provoke the recipient to follow its instructions by threatening dire consequences if the instructions are not followed immediately.

Not long ago, the e-mails of this genre that I received were obviously written by people whose spelling and composition skills were pretty weak. This recent one was an above-average fake; it even included some official-looking disclaimer language at the bottom and an "Amazon Inc." copyright statement. Except for the fact that a genuine e-mail from Amazon would address me by name, there wasn't anything about this message to show definitively that it was phony. Had I clicked on the link provided, in all likelihood I would've been taken to a fraudulent "Amazon" site where my login information would have been stolen and/or software that would have stolen other information could have been installed on my computer.

Had I clicked on the link provided, in all likelihood I would've been taken to a fraudulent "Amazon" site where my login information would have been stolen…

When you receive this kind of e-mail, examine it carefully. More and more of the spam that comes to me actually includes my full name, so the presence of one's name is no longer a sure sign that a message is genuine. (This is especially the case if your personal information is available at MySpace[3] or other networking sites.)

How should you respond to such an e-mail if you're not sure it's legitimate? In this case, it was easy to ignore the message, but if you're uncertain, the best procedure is to log on to the relevant site in the way that you normally do, usually by selecting the address from the "favorites" list in your browser. Doing this, instead of clicking on a link in an e-mail of unknown origin, generally ensures that you are going to a legitimate site. If you regularly receive e-mails from your bank or another company with links in them, be sure that you're familiar with the standard format of their messages. If you are expecting a message and have good evidence that it is legitimate, there's no reason not to click on a link that is provided. Remember that reputable vendors, including Amazon, PayPal, eBay, and financial institutions will never e-mail or otherwise contact you asking you for sensitive information.

The best protection against these threats is to be cautious about any such contacts, via any medium. Caller ID systems can be "hacked" to display phone information, so don't assume that a caller appearing to be from a legitimate source should be given your confidential information. Also, don't assume that someone who calls or e-mails you and who already knows your account number is legitimate. In cases where an account number has been compromised by some other means, this type of contact is merely a ruse to obtain additional information, like a Social Security number or account password. Be careful not to disclose this kind of information if you are contacted unexpectedly. If the contact is genuine, you should be able to contact the institution at a number (or web address) that you know is valid because it's printed on an account statement, the back of your credit card, or a phone book.

Be aware that there is a variant of phishing, called "vishing," in which an e-mail message directs you to call a phone number and provide your Social Security number, account number, or some other information. Occasionally the initial contact is made via an automated phone message instead of an e-mail. Because these scams are less dependent on the use of a specific technology than they are on manipulating human behavior, the possibilities are endless; new methods will evolve as new technologies arise. In a technique called "SMiShing"[4] (who comes up with these names?), would-be thieves send an SMS to a victim's cellphone purporting to be from a social web site where the individual actually is registered, warning that the victim is about to be charged a fee and urging them to log into an address listed in the message. Doing so, the recipient unwittingly downloads software to the cellphone that will steal his or her personal information.

TURN ON, TUNE IN…GET HACKED?

If you have an Internet connection that is on continuously, such as one provided via DSL or cable modem, you are especially vulnerable to being attacked by hackers who may

3. "MySpace users big targets for ID thieves," by Gary Gentile, http://www.msnbc.msn.com/id/16352839/

4. "McAfee warns of SMiShing attacks," John Blau, IDG News Service (http://www.pcworld.com/article/id,126932-c,trojanhorses/article.html)

access information on your computer or who otherwise hijack[5] your computer by copying malicious programs directly to it. Dial-up connections are less vulnerable because they are less likely to be on long enough for an attacker to discover them, but they are not impervious to this type of attack. The best protection is to make your computer a difficult target, so that a hacker will choose to break into connections that are less secure than yours.

To protect access to your computer, the most common solution is a "firewall," which can either be software or a device. If you have a broadband router, you already have a firewall that will block unwanted incoming Internet traffic. If your computer uses either the Windows XP or the Mac OS X operating system, you already have a firewall that blocks unwanted incoming connections. However, neither of these solutions will protect you from malicious software that you download inadvertently or that you activate by opening an infected e-mail attachment. Once such a program is running on your computer, it can establish its own outgoing connection and send personal information found on your computer to a thief. If you want protection from unauthorized outbound Internet traffic, you need a software firewall, such as ZoneAlarm Firewall or one of the Norton Internet software products. If you need to buy protection software and don't understand the difference between spyware, viruses, and firewalls, ask a geeky friend for assistance, or try using one of the resources at the end of this article. To check the vulnerability of your computer's Internet connection, try the free testing software available at Gibson Research Corporation[6].

For additional protection, it's important to keep your antivirus software updated regularly. If you have a Windows-based computer system, be sure to keep up with the frequent security patches issued by Microsoft in order to keep your computer protected from attacks. As more attacks are being launched[7] from web sites containing malicious code, you should consider buying software like Norton Internet Security, Norton 360, or McAfee's Site Advisor to provide a further layer of protection.

PASSWORDS AND YOU

It's virtually impossible to use the Internet with any frequency without also using passwords. Consequently, we tire of creating and remembering new passwords and are tempted to use the same trivially-easy-to-remember password over and over. When setting passwords for your computer or your online banking and other important accounts, it's extremely unwise to use easily-discovered passwords like your mother's maiden name, your birthday, your pet's/spouse's/child's name, or the ever-popular "123456." Unfortunately, there are several websites (like www.birthdatabase.com , www.zoominfo.com , and www.zabasearch.com) where a certain amount of your personal information is probably available right now to anyone who wants to use it as a starting point.

Avoid using overly simple passwords. If someone wants to hack into your computer or one of your accounts, there are plenty of tools (with names like "wwwhack"[8] and "brutus"[9]) available online to help them try logging in repeatedly using random combinations of characters in order to discover your password. A 6-character password that uses only numbers or only lowercase letters can be cracked with one of these programs in a matter of minutes. The simple inclusion of uppercase characters, and special characters (like %, $, @, *, ^, etc.) makes a much stronger password. If you use names or words found in a dictionary, this makes an easily-compromised password, because a determined hacker has tools to test such words rapidly.

> If someone wants to hack into your computer or one of your accounts, there are plenty of tools available online to help them ...

A good password should be fairly complex and should include at least eight characters. Here's a suggestion for creating strong passwords that you have a decent chance of remembering: Start with two words that are memorable for you. For example, suppose your childhood pet was named "Trooper," and your high school football team was called the Tigers. Change the letter "o" to the numeral "0," the letter "i" to the numeral "1," and the letter "s" to the character "$." In each case, the substituted character resembles the original, so you have an easy mnemonic device for remembering the change. You've now transformed words which individually would have been terrible passwords into "Tr00perT1ger$," which is a much stronger password.

Resist the urge to use the same password for multiple accounts. If a thief were deliberately stealing information from you and obtained a password that works on one account, his first assumption would be that it's also used for your other accounts. This creates an obvious problem: how do you keep track of all those passwords? One solution is the use of a password management program like AccountLogon or Roboform. These programs store your passwords in a password-protected encrypted file, so that if someone hacks into your computer files, your passwords are not readily available to them. The management program will remember your other passwords for you (of course, if you forget the critical password, you've got a big problem).

If you don't want to use a password management program, here's

5. "FBI pulls plug on several botnet hackers," by Lara Jakes Jordan, AP Writer, June 13, 2007, http://www.physorg.com/news101047647.html

6. http://www.grc.com/default.htm (be forewarned: this site is not for techno-phobes!)

7. "Web attackers get better at hiding," by Joris Evers, CNET News.com, http://news.com.com/Web+attackers+get+better+at+hiding/2100-7349_3-6177424.html ; "A New Battleground for Computer Security," by Riva Richmond, Wall Street Journal, March 6, 2007

8. http://www.darknet.org.uk/2006/12/wwwhack-19-download-wwwhack19zip-web-hacking-tool/

9. http://www.hoobie.net/brutus/

a rather unorthodox suggestion: it's better to write down a list of your passwords and keep it in a locked drawer than to use easy-to-crack passwords. If you can't remember multiple passwords this approach is better than the alternative of using weak ones. Online hackers can't get into your desk drawer, but be careful: as we noted in the previous newsletter, identity theft is often committed by people who know their victim personally. Never leave your passwords in an unsecured location, and don't carry them in your wallet or purse.

SAFE SHOPPING ONLINE

Online purchases are not necessarily riskier than other transactions, provided you stick with reputable websites. Be sure that the online vendor uses encryption (look for the lock icon in your browser when you're making a transaction). If something should go wrong, online shopping with a credit card (not a debit card—see our Fall issue) gives you considerable protection, since credit card companies are usually eager to waive your liabilities in the event of online fraud. Check with your credit card providers to see if they offer any special online protection services, such as the generation of random temporary credit card numbers for use in online transactions. In any case, credit card shopping at the encrypted site of a reputable vendor is safer than handing your credit card to a waiter at a restaurant[10], and you'd probably do that without a second thought.

HERE ARE ADDITIONAL TIPS ON PROTECTING YOUR CONFIDENTIAL INFORMATION FROM ONLINE THEFT:

1 *Wireless Internet*—If you install a wireless router or other network device with a password, change its default password after installation. There are websites[11] that list the defaults for all kinds of equipment, and hackers know to try these passwords if they wish to access your system. Be cautious when using unsecured public wireless networks. You take a considerable risk if you log into your bank or other financial accounts while using these systems. If you have a wireless home network, be sure to use its encryption features. There are unencrypted wireless networks in almost every neighborhood, and you'll be a less attractive target if yours isn't one of them. Further, although it's extremely unlikely that anyone would attempt to break into your home's encrypted wireless network, you should understand that if someone really wanted to do so, there are resources available that make it possible.

2 *Common Computers*—It's a bad idea to log into financial or other sensitive accounts using computers that are publicly accessible. The possibility always exists that someone has installed key logging software on such a computer in order to harvest personal information from unsuspecting users.

3 *Laptops* — Don't leave your laptop computer in your automobile. This simple precaution ensures that any sensitive information you have on the computer will not be lost in a car theft or a break-in. To provide further protection in the event of a theft, access to laptop computers should be secured with strong passwords. If you must keep confidential information on your laptop, you should secure it with one of several data encryption programs[12] that are available.

4 *Old computers* — Prior to selling or disposing of an old computer, use an overwriting program to obliterate your hard disk's information (reformatting is not enough), or remove and physically destroy the hard disk.

Finally, here are some resources to help you avoid online ID theft (or deal with it when it happens):

Federal Trade Commission Phishing Avoidance Guidelines
http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm

Consumer advice from the Anti-Phishing Working Group
http://www.antiphishing.org/resources.html#advice

To test the strength of your passwords and read more about creating strong, memorable passwords, see http://www.microsoft.com/protect/yourself/password/checker.mspx

The SEC has information for preventing and dealing with online brokerage account theft:
http://www.sec.gov/investor/pubs/onlinebrokerage.htm

Information on PC firewalls: www.firewallguide.com

If your confidential information has been compromised:
www.identitytheftassistance.org

Some states let consumers put a "freeze" on their credit files. Once in place, a freeze prevents new accounts from being opened in your name. The details vary from state to state; for information, see http://www.uspirg.org/financial-privacy-security/identity-theft-protection/summary-of-state-laws or contact your state's Department of Consumer Affairs. The freeze must be "thawed" prior to obtaining loans or new credit cards.

In the Fall issue, I mentioned that you can have a fraud alert added

10. According to Visa USA, restaurants represent about 40% of the incidents in which credit-card information is compromised, and many restaurants don't comply with credit card security rules. "Card Companies Crack Down on Restaurants," by Robin Sidel, Wall Street Journal, March 24, 2007

11. http://www.phenoelit.de/dpl/dpl.html

12. Two possible options are at www.pgp.com and www.cypherix.com

to your credit report. A fraud alert warns companies to call you before opening new accounts; it is not a foolproof method and is not the same as a "freeze." You can request a 90-day alert (by phone, 877-478-7625 or online at https://www.experian.com/consumer/cac/InvalidateSession.do?code=SECURITYALERT). A 7-year alert can be established if you submit proof (e.g., a police report) that you've been a victim of ID fraud.

The Fall issue also discussed the risks associated with paper checks. Here's a further tip: if you must write a check, the use

FISHER FINANCIAL STRATEGIES

Thomas A. Fisher

Suite 1800
245 First Street
Cambridge, MA 02139

Phone: 617-444-8555
Fax: 866-312-5605

Tom@FFScambridge.com
www.FFScambridge.com

of a gel-type pen (like the Uni-ball 207) will make it harder for a thief to subsequently alter what you've written.

(More ID theft resources can be found in the Fall, 2006 edition of Financial Strategies)