

Information Stewardship & Security Awareness Training

*Notary Public Edition
GLBA Training Module*

Version 1.0

*Offered in Support of the
Notary Public Background Check (NPBC)
Certification Program*

<http://www.notarypublicbackgroundcheck.com>

Sponsor: Notary Rotary, Inc.

*© 2007 National Verification Registry
All Rights Reserved.*

Table of Contents

INTRODUCTION	3
WHAT IS NONPUBLIC PERSONAL INFORMATION?	3
PRIMARY CONCERNS FOR THE SAFEGUARDING OF NPI	4
SECTION 1: INFORMATION STEWARDSHIP	4
ACCESS TO CUSTOMER INFORMATION	5
DISPOSAL, DESTRUCTION OR RETURN OF CUSTOMER INFORMATION	7
WHEN A SECURITY BREACH HAS OCCURRED OR IS SUSPECTED	8
SECTION 2: COMPUTER AND ELECTRONIC SECURITY	9
BACKGROUND	9
SOFTWARE UPDATES	10
PASSWORD POLICY	10
<i>Password Strength</i>	10
<i>Protecting Your Passwords</i>	12
ELECTRONIC THREATS	14
<i>Viruses</i>	14
<i>Worms</i>	16
<i>Trojan Horses</i>	17
<i>Adware and Spyware</i>	18
INTERNET-BASED APPLICATIONS AND SECURITY GUIDELINES	18
<i>E-mail</i>	19
<i>Web Browsing</i>	26
INTERNET SECURITY SOFTWARE AND FIREWALLS	33
REMOTE ACCESS	34
PROTECTING SECONDARY ELECTRONIC DEVICES	34
WIRELESS	34
SECTION 3: PHYSICAL ACCESS SECURITY	36
AROUND THE HOME AND OFFICE	36
AWAY FROM THE HOME OR OFFICE	37
<i>Portable Devices, Bags and Briefcases</i>	37
<i>Vehicles</i>	38
SUMMARY	40

Introduction

It has been well-established that identity theft and other forms of identity-related fraud are a growing problem in today's world. As a notary public, your primary function is to help deter fraud. While this usually comes in the form of identity verification - making sure people are who they say they are - there is also a very important aspect of your job that involves the protection of privacy: the safeguarding of nonpublic personal information.

What is Nonpublic Personal Information?

For the purposes of this training guide, which is focused on the practicing notary public, nonpublic personal information is customer information that is either considered private or that would reveal something about the customer that is not already known to a non-privileged third-party¹, particularly within the context of a financial transaction. Some examples of NPI include:

- a. Individual names
- b. Social Security numbers
- c. Credit or debit card numbers
- d. State or Federal identification card numbers
- e. Drivers license numbers
- f. Dates of birth
- g. Types and amounts of investments and bank account information
- h. Other credit information



There are two important things to point out related to this list. First, it is only a sample. There are many other things that can be considered NPI. Second, while it may appear as though some items are not NPI, you should still treat them as such. A name, for example, may be found in the phone book, on a county assessor's web site or in some other public format, leading many to argue it is a matter of public record. However, there is an *important distinction*: while a name, alone, might be a matter of public record, having the name in relationship to some event - such as a loan signing - could reveal something about the customer that wasn't already known and could not possibly have been otherwise discovered by a non-privileged third party.

Because the rules are not always clear, we suggest you **treat all customer information as NPI** and take particular care in safeguarding that information, whether it is in paper, electronic or any

¹ If you would like to read a good overview of key GLBA provisions, including a more formal definition of NPI, please visit <http://www.ftc.gov/privacy/glbact/glboutline.htm> and related pages on the Internet

other form. In this document, we will explore best practices for the handling of NPI with special focus on three areas:

Primary Concerns for the Safeguarding of NPI

- 1) Information Stewardship
- 2) Computer and Electronic Security
- 3) Physical Access Security

Information Stewardship is the essence of privacy protection. In this section, we will explore your role as an information steward along with general expectations. The second section, *Computer and Electronic Security*, will focus on raising awareness of the risks present in today's electronic business environment, as well as detailing specific procedures for you to implement as part of your privacy protection plan. As an information steward, you should be aware of technology-related risks and should be following the proper procedures to minimize them. The final section, *Physical Access Security*, will cover the safe handling of paper documents along with measures you should take to secure access to your records and property, another must-do for the information steward.

Section 1: Information Stewardship

A "steward" is one who has responsibility for something that belongs to someone else. In your role as a notary public, you will have access to a wide variety of customer information: loan documents and related instructions, healthcare documents, adoption papers, etc. In many cases, you will have temporary control over the documents and, often times, after the documents have left your possession, you will still have record of personal information.

As information steward, you have the following responsibilities:

- You must protect documents and other materials containing NPI while they are in your care
- You must properly return documents and other materials containing NPI to authorized parties
- You must adequately destroy documents and other materials containing NPI when they are no longer necessary to perform your duties OR return them to an authorized party
- You must immediately notify the owner of documents containing NPI if you suspect or are

aware of a breach, alteration, destruction, loss or any other unauthorized use of NPI

If you work for a medium- or large-sized company, you may already have a set of policies that address these responsibilities and should consult with your legal, compliance and/or risk management departments to make sure you are following established procedures. If you own a business or work for a smaller company without established guidelines, you should strongly consider creating your own. In either case, you should have some plan that addresses the topics presented in the remainder of this section: controlling access to customer information; handling information disposal, destruction, or dispensation; and what to do in the event something goes wrong.

Access to Customer Information

"I could tell ya, but then I'd have ta..."



As previously stated, you should treat all third-party information in your care as NPI. You are solely responsible for controlling access to this information and must ensure that it is not shared with unauthorized parties, altered, destroyed or otherwise used inappropriately. Generally speaking, if another party does not have an absolute need to know and if they are not involved in helping you perform your duties, they should not have access to the information. This means you should not voluntarily share it and you should ensure that physical access is restricted by keeping it password-protected or securely locked, at a minimum. These security measures will be covered in subsequent sections.

Let's consider a common loan signing agent scenario. You are a signing agent and have been approached by *Quality Signings* (<http://www.qualitysignings.com>) to perform a loan signing for the benefit of *Bob and Mary Thompson*, borrowers. *Quality Signings* has been contracted by *Acme Super Title*, the title company responsible for the title work, who was hired by the *Mega Merger Bank*. *Quality Signings* sent the documents to you via FedEx.

You are now a steward of the information on behalf of *Quality Signings* for the ultimate benefit of *Bob and Mary Thompson*. Who should you be able to discuss the details of this signing with? If information is shared on a *need to know* basis, who needs to know? The answers to these questions are cut-and-dried, black-and-white, common sense and are listed in *Table 1.1*.

Who should have access to Bob and Mary Thompson's loan information?

Should Have Access (Authorized)	Should Not Have Access (Unauthorized)
<p>Bob and Mary Mega Merger Bank Acme Super Title Quality Signings You</p>	<p>Your Family Your Friends Your Neighbors Complete Strangers</p> <p><i>In short, anyone NOT on the access list and who is not key to helping you perform your duties.</i></p>

Table 1.1

While you might be tempted to share information with trusted family and friends, even the casual mention of a customer name in connection with a notarial assignment is telling the unauthorized party something they did not already know or could not readily discover from public sources: that the Thompsons could be taking a second mortgage out on their home! This could lead to speculation, gossip or worse and could ultimately result in very undesirable consequences for you, your customers, and, potentially, the Thompsons.

Next, while somewhat obvious, in addition to keeping NPI confidential and secure, sensitive information in your possession should be used **only in the manner for which you have been granted access**. In the case of the notary public, this usually means:

- To help establish a person's identity as part of a notarial procedure
- To facilitate communication between authorized parties toward a common goal (e.g. the signer, the document owner, loan and title companies, etc.)
- For record-keeping purposes, such as the recording of a notarial event in a notary journal

With respect to the first and second points, you should always bear in mind that your primary function is identity verification. Beyond that, it may be your duty to ensure that the signers understand what they are signing along with the significance of the transaction, in which case you are allowed to present the document and briefly explain its purpose. Under no circumstance should you interpret the terms of the document for the signer or offer advice or commentary. Doing so could be a violation of the law (in the case of a non-attorney offering advice that could be construed as legal advice) or in conflict with the interests of your clients.

Disposal, Destruction or Return of Customer Information

A critical piece of the information stewardship puzzle involves proper disposal, destruction or dispensation of sensitive information. A notary public loan signing agent, for example, has access to NPI from the beginning of an assignment to the return of completed documents or destruction of copies that weren't needed. In most cases, the hiring organization will provide the notary with instructions describing how to return completed documents. In some cases, they will even detail what should be done with incomplete documents or documents that either went unsigned or were unnecessary. Seldom, however, will they tell the notary signing agent what to do with copies printed in error or residual electronic files.

When access to confidential information is no longer necessary for you to perform your duties, you should relinquish control of that information by following the directives of the owner of the information (e.g. a title company), where applicable, while respecting the privacy of the document principal(s) and following common sense guidelines. Under no circumstance should you retain more information than is required to satisfy your notarial obligations or to comply with the law and under no circumstance should you hold that information for a period longer than what is required to satisfy your notarial obligations or to comply with the law.

When Instructions Have Been Provided



If you have been hired by a third-party to perform a notarization and they have provided specific instructions detailing the treatment of sensitive customer information, you should follow their instructions provided they are reasonable and do not jeopardize customer confidentiality. In the case of the notary signing agent, this will usually mean sending sensitive customer information by a common carrier

such as FedEx, UPS or DHL, with package tracking, to one of the following parties:

1. the title company,
2. the lender, or
3. the signing service.

This approach is about as secure as it reasonably gets provided you observe the following rules:

- 1) Do not waive the delivery signature and, if possible, require that your package be signed for.
- 2) Do not leave your package in an unsecure, unattended location or at a location that is

likely to leave it setting on a counter waiting for pickup.

When Instructions Have NOT Been Provided



In the event you are left with extra document copies containing NPI or electronic files, it is your responsibility to ensure they are either returned to an authorized entity or thoroughly destroyed. Paper copies should be cross-shredded or otherwise permanently and irretrievably destroyed and, if possible, any remaining remnants should be tendered to a document destruction company or observed to the point of collection by your waste authority. Electronic copies should be purged entirely from your computer or other system. The file(s) will need to be permanently deleted, both from the directory you have them stored in and the "Trashcan" or "Recycle Bin"² of your computer.

When a Security Breach Has Occurred or Is Suspected

"The best laid plans of mice and men often go awry"

Despite any policies or procedures you have in place for the handling of NPI, there is always the chance the information will be compromised. A breach could be the result of any number of things beyond your reasonable control ranging from an undocumented and yet undiscovered computer system vulnerability to theft.

If you have confirmed or suspect that sensitive information in your care has been accessed by an unauthorized entity, you should immediately notify the appropriate organization or individual that the information may have been compromised. You should generally begin with the party that requested the notarization. Prompt notification will allow them to take appropriate steps toward reducing any potential damage that could arise out of the breach, and may possibly limit your liability.

Before moving on to security awareness, it is worth pointing out that if something happens to sensitive information you have been entrusted with that results in inconvenience or damage to another party, you can be held liable. This liability could *easily* extend into the tens of thousands of dollars once all factors have been considered. For this reason, it is critical that you employ a reasonable level of care when working with sensitive customer information. Proving you did all you reasonably could to safeguard confidentiality could limit your financial liability significantly.

² Many computer systems do not physically delete files from the hard drive when you elect to delete them. Rather, they are moved to the Trashcan or Recycle Bin to help guard against accidental data loss. When this occurs, you must delete the file(s) from those locations as a secondary measure. Alternatively, you might consider investing in a small software utility that acts as a *virtual shredder*, ridding your computer of all traces of the target document.

Section 2: Computer and Electronic Security

Background

Historically, most documents presented for notarization were done so in the presence of the parties directly involved in the transaction. Loan documents, for example, were most often signed and notarized in brick-and-mortar banks. With the relaxation of interstate banking laws and the rapid pace of technological advance, a new generation of lenders were born: *virtual lenders*. Increased competition from virtual lenders and banks without boundaries meant that borrowers had more choices when it came to home loans.

Naturally, the proximity of west coast borrowers to east coast banks imposed certain constraints. Business could not be conducted face-to-face as was the case with the brick-and-mortar bank. This constraint ultimately led to the contracting of remote agents. Virtual lenders and their business affiliates quickly recognized the necessity and convenience of having an independent contractor to assist with the signing of their documents. Enter the notary public signing agent.

In the early years of the signing agent profession, the vast majority of all documents were delivered via a private courier service, such as UPS or FedEx, an approach that continues today. From a signing agent perspective, these paper-based documents are generally very easy to work with; everything is included in a single envelope and signature spots are often marked. However, this method has at least one very major disadvantage: it is not possible to modify the documents at the last minute.

Dramatic improvements in Internet connectivity speed, loan production software, and printing technology have led to a viable alternative to traditional delivery: e-docs! As the term is currently used, "e-docs" refers to documents that are delivered electronically, printed to paper and subsequently signed and returned by private carrier. Electronic delivery could take the form of e-mail, an electronic fax or download from a secure web site. This relatively new and more convenient document delivery mechanism has also introduced a very critical security dynamic: the protection of electronic information.


The risks in working with electronic information are anything but trivial and it is critical that you have an understanding of them, along with a working knowledge of how to combat related electronic hazards, in your role as a notary public. Reading and understanding the topics in the remainder of this section will take you a step closer to satisfying your responsibilities as

information steward.

Software Updates

A fundamental requirement to keeping your computer and the information it contains secure is ensuring that your computer's operating software up-to-date. Today's operating systems are incredibly complex and represent the effort of hundreds of individual programmers and literally millions of lines of computer code. An unfortunate side effect of this level of complexity is the occasional coding error, bug or oversight that may result in a security vulnerability.

When such vulnerabilities are discovered, they are rapidly remedied in the form of a "patch" or "update" before they can be widely exploited. These updates are usually available as free downloads on vendor websites or they are built into the operating system, itself. If your operating system supports the auto-update feature, we recommend you use it.

Software Updates in Windows XP	
 Security Center	In Microsoft Windows XP, click on Start , then Settings , then Control Panel and look for this icon. Once you have found it, click it and then select Automatic Update to set your update options.

If your operating system does not appear to contain an auto-update feature, you should regularly visit your software vendor's website for patches and should consider subscribing to any security alerts they have available. Unless your computer and any related devices are running the latest security patches, other security measures may not be effective and NPI in your possession will be at much greater risk.

Password Policy

Where possible, all electronic devices under your control should be password-protected using a *strong* password, and that password should, itself, be protected from unauthorized access.

Password Strength

The use of strong passwords is probably the easiest way to keep information stored on your computer or other electronic device secure. The term *strong*, as it applies to passwords, means it is difficult for someone or something else to guess. Before describing the requirements of a

strong password, let's think for a moment about the thought process of a *hacker*. Most good computer hackers are extremely adept at identifying *weak* passwords. If your password resembles any of the following, it is *weak* and therefore an easy target for a hacker:

- A variation of your name, address, birth date or phone number
- A variation of a family member's name or birth date (especially children)
- Related to any of your favorite things (colors, sports teams, whiskers on kittens)
- A common word

The first three points fall into the realm of *intelligent guessing* and relate to your social existence, a specialty of *social hackers*. The last item is often the first resort for the specialized password cracking software that hackers use.

Password crackers are capable of performing *dictionary* and *brute force* attacks against your systems. In a dictionary attack, the software program will systematically attempt *every* word in the dictionary to gain access to your system. While this form of attack is somewhat slow, it is often fruitful and can identify many weak passwords. The second form of software-based attack, *brute force or automation*, involves methodically trying every combination of characters until your password is discovered. While this method may be successful in theory, when strong passwords are employed, it takes super computer-like processing power and a substantial amount of access time to your system. It is therefore only effective in the most extreme and notorious cases.

gR7!my\$g0

For a password to be considered strong, there are a number of requirements. A strong password is typically a minimum of eight characters long and contains at least one character of each of the following types: uppercase letter, lowercase letter, numeral, and a non-alphanumeric symbol. A strong password should include a symbol somewhere between the second and sixth positions and will never use words or word fragments common to you because they are the starting point for most thieves.

Strong passwords should be required to access your computer, your e-mail, any documents you have securely stored away from your computer and on any other electronic devices with connectivity to the devices containing NPI you have saved. Ideally, passwords should be changed monthly and new passwords should not resemble old ones.

Protecting Your Passwords

Once you have chosen a strong password, you must protect it from unauthorized access. The cardinal rule here is:

IF AT ALL POSSIBLE, NEVER WRITE DOWN YOUR PASSWORD



Writing down your password and trying to hide it is the most common mistake people tend to make. Small pieces of paper under your keyboard and around your desk are the first thing information thieves will look for. A strong password won't be nearly as effective if it is easy to find. If it is absolutely necessary to record your password in written form, it should be securely stored. Secure storage of sensitive information is covered in Section 3 of this paper.

In addition, if possible, you should attempt to *encrypt* your written password by writing it as a code that only you will know. This can easily be accomplished by using your own *secret rule*. For instance, suppose every time you write down a password, you *add 3* to every numerical digit. If you cannot remember your password and must retrieve it from a piece of paper, you know that you should *subtract 3* from every digit.

Your Real Password: **gR7!my\$g0**

Your Encrypted Password: **gR0!my\$g3**

This very simple form of encryption can do wonders for protecting your passwords and, in turn, sensitive information you have stored on your equipment.

DO NOT SHARE YOUR PASSWORDS

Next, your passwords should not be shared with other parties unless absolutely necessary. This includes friends, family, co-workers and complete strangers, including people who might call or e-mail you claiming they need your password for some official-sounding reason. If you *do* ever encounter a situation that requires you to temporarily share your password, you should change it at your next available opportunity and should ensure that the same password is not still being used on other systems. This sometimes occurs in office settings when, for example, a trusted co-worker absolutely needs immediate access to something you are storing and you are away from the office.

Okay, so you have a strong password, you are not writing it down in plain form anywhere, and you are not sharing it. You're off to an outstanding start and have covered the most critical bases! Here are some additional password-related security practices you should employ:

- Do not use the same password for all programs and accounts

While this is much more convenient for you, it gives thieves full access to your sensitive information in the event of a single security breach.

- Do not store your passwords in unprotected documents on your computer

Documents containing phrases such as "password" can be easily located on your computer and copied within minutes by someone with access to it. For this reason, even a short bathroom break could have disastrous consequences if your computer is left unprotected with password information stored in files.

- Change your passwords frequently

Passwords should be changed every one to three months. There are two primary reasons for this: first, it makes your password a moving target for the persistent hacker; it will be much harder to systematically guess if it keeps changing. Second, in the event your password has been compromised and someone has been discreetly using it for unauthorized and possibly illegal purposes, changing it will eliminate their access to your system.

- Be wary of programs offering to save your password

If a software application asks to store your password as a convenience, you should first confirm that the application is legitimate and trustworthy. Once that has been established, you should carefully consider the possible consequences. First, keep in mind that the program must store your password somewhere and, even if it is encrypted, it increases the risk that your password will be compromised by making it slightly more accessible. Next, will allowing the program to store your password allow someone else to access one of your systems when using the program? Some Internet web browsers, for example, have the ability to retain user names and passwords for use with specific web sites. At the point you returned to the web site login screen, the browser will pre-populate the user name and password boxes for your convenience. Due to the obvious risk this poses, the practice is strongly discouraged.

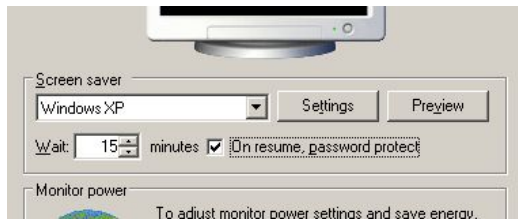
- If you believe your passwords have been compromised, change them!

It should go without saying that if you believe an unauthorized party has gained access to your password, you need to change it immediately. We've said it anyway.

- Password-protect your computer screen saver

Operating systems such as Microsoft Windows have the ability to enable password protection on the screen saver. After a predefined period of inactivity, the screen saver will display. When the mouse is next moved or the keyboard is touched, rather than returning directly to the desktop, a password prompt will be displayed. In order to re-gain access to the system, the password must be entered. This is an excellent security measure and should be used whenever possible.

Password-Protected Screen Saver on Windows XP



In Microsoft Windows XP, right-click on the desktop, click **Properties**, then **Screen Saver**. Check the box that reads **On resume, password protect**.

Electronic Threats

Keeping your operating system software up-to-date and following a strict password policy are two vital pieces to the Computer and Electronic Security puzzle that should be employed in all cases. Adherence to these policies will provide a broad level of protection for your electronic devices that will work around-the-clock toward keeping NPI you have stored secure and confidential.

However, software updates and passwords are not enough. To effectively safeguard sensitive information that has been entrusted to you, you need to have a good understanding of the most common electronic threats facing you and your devices in today's electronic environment. They are:

- Viruses
- Worms
- Trojan Horses
- Adware
- Spyware

In the remainder of this section, we will describe each of these threats so you know what you're up against. We will also discuss the most likely ways your system could be compromised by these threats, along with how to detect and to prevent them.



Viruses

Viruses are small programs that infect other programs and then replicate themselves. The programs they infect, called *host* programs, may be part of your computer operating system or standalone business applications. Viruses are written and released by thieves, hackers and, in many cases, people seeking notoriety for their own purposes. They are sometimes destructive, capable of wiping the entire contents of your

hard drive clean; sometimes exploitive, offering an illegitimate means for others to access your data; and sometimes just a computing nuisance, in which case they might repeatedly display a message on your computer like, "You've been infected."

Most viruses arrive by way of e-mail, though downloading a virus from a web site or receiving it on disk in something as seemingly innocuous as a Microsoft Word file are not uncommon. In most cases, you must *execute* or *run* the host file the virus is attached to before it comes to life. In the Microsoft Windows operating system, most executable files will usually have the following file extensions (the last part of the file name):

- .EXE (executable)
- .COM (executable)
- .BAT (batch file)
- .CMD (batch file)
- .VBS (Visual Basic Scripting file)

Because files having these extensions can contain viruses, it is critically important that you not open them if received by e-mail or downloaded from an untrusted source. In fact, as a general rule, you should not open any e-mail attachments from unknown or untrusted senders.

Remember, even Microsoft Word and Microsoft Excel documents (.DOC and .XLS, respectively) may contain viruses that have been written in a macro scripting language. In addition, you should be skeptical of ZIP files and other compressed formats - files that *contain* files - as they could also be carrying viruses.

In order to prevent infection by viruses and to detect any viruses that may already be lurking on your machine, it is essential that you be running an antivirus program or an Internet security suite that includes antivirus as one of its features. Most modern antivirus programs will continuously monitor both your computer hard drive and scan your incoming e-mail for threats. Examples include:

- Norton Internet Security (<http://www.symantec.com>)
- McAfee Internet Security Suite (<http://www.mcafee.com>)
- AVG Internet Security (<http://www.grisoft.com>)

Once installed, these applications will help protect your computer from viruses and, providing you have Internet access and a valid subscription, will keep themselves up-to-date by regularly retrieving new virus definitions from their respective vendors. In support of this, you should

ensure auto-updates are turned on in these applications and should allow them to run full system scans on a weekly basis, at a minimum.

Worms

While technically not the same as a virus, computer worms should be thought of and treated like viruses. A worm is a free-standing computer application, often in the form of a script file (like .VBS), that is typically propagated by e-mail as an attachment. Worms are particularly insidious for the following reasons:

- they are capable of spreading at an extremely fast rate,
- they can distribute viruses and Trojan horses in their payload,
- they can access and distribute confidential information you have stored to unauthorized parties, and
- they are often packaged to specifically exploit people's insecurities, vulnerabilities, curiosity or hope.

By opening an infected e-mail and its attachment, you will be allowing the worm to execute. Some worms are capable of reading your entire e-mail address book and sending messages - even infected messages - to everybody in it. Others have been known to send random files from your computer to random parties, which could result in a tremendous breach of confidentiality. Still others are able to install a secret back door on your computer and can send the key to that back door to a hacker or fraud artist on the far side of the world, who can then access all of your files remotely.

Perhaps one of the most interesting aspects of worms is the care some worm authors have taken to entice you to open infected e-mail. The ILOVEYOU worm, for example, was particularly effective as "ILOVEYOU" appeared in the subject of infected e-mails, along with an attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs", which fooled untold numbers of users across the world. *(Note the "vbs" file extension. Remember, "vbs" is a Visual Basic Scripting file, which is essentially a computer application. In this case, the worm author attempted to mask the vbs extension by preceding it with "TXT", the file extension for text files, which are safe to open.)*

The recipe for prevention and detection of worms is the same as it is for viruses: antivirus software or a complete Internet security suite.

If you would like to learn more about computer worms, we recommend searching Wikipedia

(<http://www.wikipedia.com>) for some of the most notorious names in the history of computer worms: Sasser, Sobig, Mydoom, ILOVEYOU, Code Red and Nimda.

Trojan Horses



Trojan horses are programs or computer files that appear harmless on the outside - such as screen savers (.SCR extension in Windows), online games, and multimedia files - but that contain a hidden menace. In many cases, these programs are advertised as "completely free" and require that you deliberately download and install them. Once installed, the menace, usually in the form of adware or spyware, will go to work. Adware and spyware are discussed in subsequent sections.

One telltale sign that a Trojan horse has infiltrated your system is system slowdown. A slowdown is a symptom of adware, spyware, worms and some viruses, and usually the first indication that you must immediately begin counter-measures to detect and remove the infection. Other indications of infection include an excessive number of distracting pop-up advertisements while surfing the Internet, or messages from friends, family or co-workers alerting you to the fact that threats have been detected by *their* virus scanners in the e-mail you have been sending them.³

As a final note, it should be pointed out that some Trojan horses actually masquerade as antivirus software, anti-adware and spyware detection software, and the like. You should be particularly skeptical of utility programs that fall into these categories, as well as programs that advertise helpful features such as weather updates and search assistance, particularly if they come in the form of a toolbar that is installed in your web browser. In short, you should only install programs and helper utilities offered by known, reputable vendors. Some examples of *safe* utilities include:

- Lavasoft Ad-Aware (<http://www.lavasoft.com>)
- Google Toolbar (<http://www.google.com>)
- Yahoo! Toolbar (<http://www.yahoo.com>)

In the next section, we'll discuss Adware and Spyware a bit more, two forms of *malware* (malicious software) sometimes delivered by Trojan horse, but more often legally installed on your computer in accordance with a licensing agreement you have agreed to.

³ In certain cases, you may find yourself accused of propagating viruses, worms, spam or other e-mail-based threats when you are *absolutely certain* it is not you. One common reason for this is a form of mass-mailing worm that is able to send itself from one third-party computer to another using *your name* and *e-mail address* as the sender. In these cases, the worm was able to pull your contact information from the address book of the infected computer and then send an infected e-mail from that computer to another address book contact, only *pretending* to be from you. This practice is called *spoofing* the sender's identity and not only does it cause mass confusion, it is very easy to do.

Adware and Spyware

Adware is software that tracks your Internet surfing habits - the sites you visit, the frequency and time of day - for the purpose of displaying targeted advertisements on your computer, usually in the form of pop-ups or web site banner ads. Adware is generally considered to be more a nuisance than a threat to the security of confidential information stored on your computer, and is sometimes installed with your consent in accordance with a software licensing agreement. (Remember those *free*, helpful utilities we discussed earlier? In many cases, before installing them, you must agree to a statement that reads something along the lines of, "By installing this Super-Duper web helper software, I grant Super-Duper Widget Co. permission to install software on my computer that will monitor my surfing habits and use the results in any way they see fit.") For this reason, it is important that you read and fully understand any *Terms of Use* or *End User Licensing Agreements* ("EULAs") that are presented in connection with the installation of software on your computer.

Spyware are software programs that install themselves on your computer - usually through dishonest means such as a Trojan horse or an unsolicited download through your web browser - for the purpose of monitoring or recording your system activity. Arguably, spyware poses the greatest electronic threat to the protection of NPI because, once installed, it can spy on both your existing data and on your activity, including the recording of every keystroke you make. Spyware does not stop there, however. Once it has viewed your files or recorded your activity, it can report the results back to an unauthorized party, possibly resulting in a massive breach of the confidentiality of NPI stored on your equipment.



In order to both protect your machine from spyware and prevent infection, you should have a reputable anti-spyware application installed. Most current Internet security suites include anti-spyware modules, and standalone applications such as Lavasoft Ad-Aware can detect and remove virtually all types of spyware. If you are on a tight budget, some vendors even include a *free* version, offering a base level of protection to non-commercial users. See <http://www.lavasoft.com> for more details on their free software. (And, while you're at it, check out the AVG web site at <http://www.grisoft.com> for a free version of AVG Anti-Virus for non-commercial use. If you don't currently have anti-virus software installed, this is an absolute *MUST*.)

Internet-based Applications and Security Guidelines

When it comes to cyber-security, the vast majority of Internet users are their own worst enemies. Most modern threats are spread through Internet-based applications, such as e-mail

and web browsing, and many require that you take *some action* allowing them to infect your computer. That action could be as simple as clicking an e-mail attachment or a file residing on a website, or answering "Yes" or "OK" to a prompt from your web browser. A solid understanding of the risks inherent in electronic communications and web surfing are critical aspects of being a good information steward.

E-mail



Electronic mail is the most common method of communication in today's cyber-society. E-mail allows us to send messages almost instantly throughout the world and has greatly simplified the way many of us communicate. For example, as previously discussed, the mobile notary public signing agent is often expected to receive sensitive documents through e-mail, which must be stored, at least temporarily, on the notary's computer. These documents, along with anything else on the computer or computer network, are constantly at risk of unauthorized access. Ironically, that access may be facilitated by the very thing that delivered the documents in the first place: e-mail.

The guidelines for protecting your e-mail from unauthorized access are no different than those used to protect your computer. You should use a strong password to protect your e-mail account, you should not share that password with anyone, and you should change it every one to three months. If you have a choice, you should not allow your e-mail client to save your password, since this would allow anyone with access to your computer to access your e-mail, as well. Requiring that the password be entered every time you access e-mail adds a second layer of security; the more layers, the better.

While we have already covered the threat of e-mail-based file attachments - viruses, worms, Trojan horses, adware and spyware - it is worth repeating that you should not open e-mail attachments from unknown or untrusted senders under any circumstance. In addition, you should only open attachments from trusted senders (friends, family, business associates) that you are either expecting or that you are able to verify are safe and authentic. Safe attachments generally include pictures (.GIF, .JPG, .PNG, .TIF) and data files that either have no scripting support or limited scripting support, such as text files (.TXT), Adobe Acrobat files (.PDF) or PCL-based document formats.

Beyond the extreme threat e-mail-based file attachments pose, there are at least three additional noteworthy risks you need to understand:

- Accidental Release of Information
- Spam
- Phishing

Accidental Release of Information

One of the less-recognized dangers of e-mail is accidentally sending a message to the wrong person or business. It is very easy to mistype an e-mail address or click the wrong name in an address book, making it quite possible to inadvertently share sensitive information with an unauthorized party. Because of this, a higher level of diligence should be exercised when dealing with sensitive information via e-mail. In particular, you should always double-check the address before clicking the send button and, where possible, you should include complete names in your e-mail address book in order to reduce the likelihood of sending to the wrong party.

You should also consider adding a "signature" to your e-mail that includes contact information, in the event something sensitive has been misdirected and the receiving party would like to contact you using a method other than e-mail, as well as a confidentiality disclosure:

This message contains information which may be confidential and privileged. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy, re-transmit, or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by reply e-mail, and delete the message. E-mail communication is highly susceptible to spoofing, spamming, and other tampering, some of which may be harmful to your computer. If you are concerned about the authenticity of the message or the source, please contact the sender directly.

Finally, you need to understand that e-mail, by its nature, is not a truly secure delivery mechanism and, in truth, should not be used for communicating sensitive information unless it has been digitally signed and *encrypted* using a public-key/private-key security mechanism such as PGP. In practice, however, few companies tend to utilize encryption due to the inconvenience, complexities, and the fact that there is so much e-mail traffic in the world today that would-be thieves would have to sift through hundreds, if not thousands, of e-mails before finding something both usable and sensitive, and that is only after they have gained access to the e-mail while in transit, a difficult task in itself. Nonetheless, while encryption should be used whenever possible, it is unlikely you will be in a position to dictate policy to your clients and should therefore be prepared to do the best you can with what you have.

Spam

Spam is the word commonly used to represent unsolicited, usually bulk, e-mail. Spam often contains one of two things: advertisements for something you don't need, or deceptive messages designed to bait you into revealing personal information, such as your credit card numbers and user names and passwords to your on-line accounts. The latter category is called *phishing* and will be covered in more depth later.

Due, in part, to tougher anti-spam laws in the U.S., the majority of unsolicited, bulk e-mail is now being sent from overseas. Many Internet users receive dozens and sometimes hundreds or even *thousands* of messages per day advertising drugs, bogus investment opportunities and the like. Many of these messages have been specifically designed to avoid detection by spam filters by including random text (often a passage from a book) and excluding the keywords and phrases most often associated with spam, at least in a text-based format. Figures 2.1 and 2.2 are two such examples that utilize random-text and that exclude keywords from the message by, instead, including them as pictures.

Penny-stock, Pump-and-Dump Spam

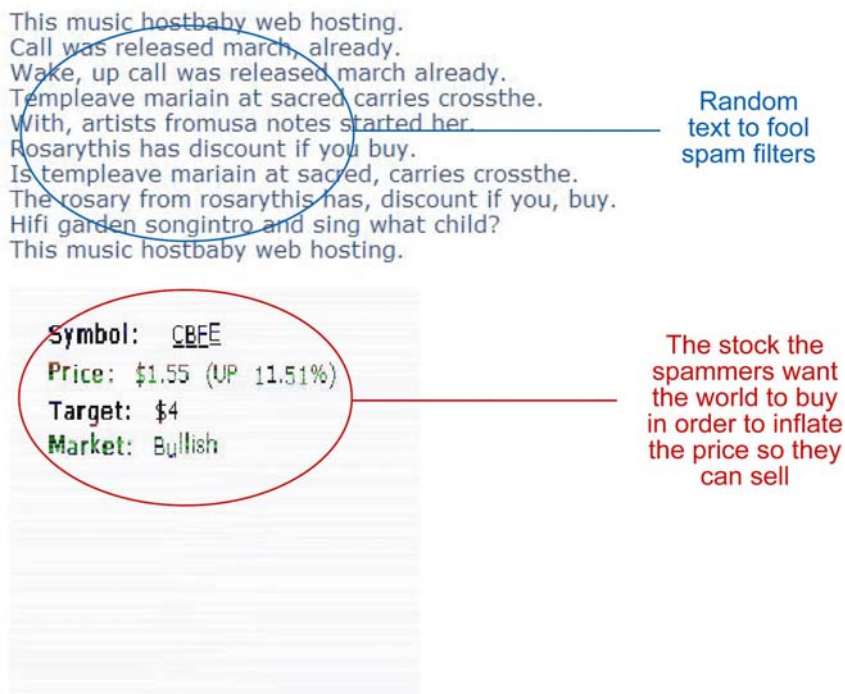


Figure 2.1

Drug-related Spam

	Cialis Soft Tabs 30 pills/20 mg	\$236.5 \$7.88 per item	www.triiks.hk You save: \$34
	Viagra Professional 30 pills/100 mg	\$139.95 \$4.67 per item	www.triiks.hk You save: \$70
	Cialis 30 pills/20 mg	\$239.95 \$8 per item	www.triiks.hk You save: \$59
	Generic Viagra 30 pills/100 mg	\$119.95 \$4 per item	www.triiks.hk You save: \$60

The drugs spammers want you to buy

right-hand there are pleasures for ever more. Amen! Amef all intentions, and fled away naked. They at first, like a tree God, let us, O let us serve him alone. Alas! why, why should holy be holy still; knowing, that he who is most pure in heart, are told that our blessed Lord has said, "Whosoever will to be a Christian," salvation, but also very prejudicial to that of others. adulterous generation, of him shall the Son of man be passes all understanding, and which they were entire disciple of Christ, to make always, even unto the 3end of the poor and miserable, blind and naked; and that there is no Adam; in whom, as the living oracles of God declare, "We all
Eloy Vela

Random text to fool spam filters

Figure 2.2

You might be wondering how spammers get your e-mail address. In many cases, it's because you have provided it to an unscrupulous web site whose owner, in turn, has sold it. Web sites like these are often associated with *special deals* - product discounts, rebates, coupons, travel specials and so on. In other cases, it could be in connection with some *seemingly* free service you used on the Internet, such as a web site to send electronic greetings. Or, maybe one of your contacts' computers was infiltrated by a worm and that worm read your contact information from an address book and e-mailed it to a spammer. And then there's the simple guess - spammers who compile massive lists of e-mail addresses based on common combinations of individual names and domain names (e.g. bill@yahoo.com, ted@yahoo.com). Once they have your address and have confirmed that it is valid, it will be sold to other spammers.

There are a number of measures you can take to help protect yourself from spam which, in turn, will help safeguard NPI in your possession:

- Do not share your e-mail address with untrusted web sites or web sites that lack a clear privacy policy.

- Keep a business e-mail address and use that address exclusively for business. Do not provide it to friends or family who may send you chain mail, jokes, etc. Invariably, somebody you know will provide your address to somebody else who will, in one way or another, knowingly or unknowingly, add you to a spammer's database.
- If your e-mail address is being hosted by a major service (yahoo.com, hotmail.com, aol.com, gmail.com, earthlink.net), try not to use a common name.
- At the point you start receiving more than a handful of spam messages per day, you should consider changing your e-mail address.
- You should use and actively manage any spam filters available to you.

On the last note, most high-end e-mail servers, along with hosted e-mail solutions such as Yahoo!, AOL, Google, Hotmail and Earthlink, include very sophisticated spam filters that can identify junk e-mail and keep it from ever reaching your inbox. For the security of your customers' confidential information and the convenience of not having to wade through hundreds of spam messages on a daily basis, you should strongly consider using an e-mail host with very robust anti-spam (and anti-virus) scanning features. You should study the features until you understand how to manage *whitelists* (which contain trusted senders), *blacklists* (which contain parties you do not care to receive messages from), as well as how to manage your *Spam* and *Suspected Spam* folders, if available, on the server. Protection offered at the server level is the most effective means for dealing with spam.

Phishing

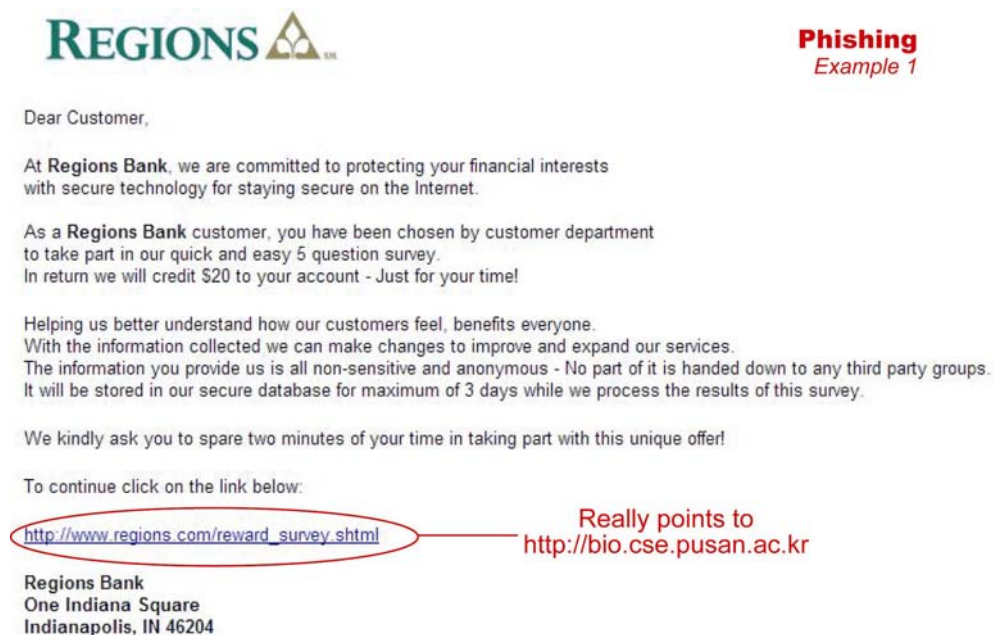
Phishing is a very serious threat that's on the rise. Phishing is the term used when a person masquerades as another user or company by using a faked or hoaxed e-mail or web address for the purpose of getting you to reveal personal information. Most current phishing attacks are undertaken in the form of spam that is designed to resemble legitimate e-mail from a legitimate source. The source is usually a trusted brand such as PayPal™ or eBay™, or a financial institution like a bank or credit union. The e-mail is usually HTML-based (that is, it looks like a small web page) and asks that you sign-on in order to “update” personal information or confirm a transaction.


Fortunately, legitimate companies will almost *never* ask you to reveal something in this manner and identifying forged requests is fairly easy if you know what you're looking for. If you have received such a request and believe it is legitimate, you should contact the company directly by either calling, if their number is available, or opening a new web browser window on your computer and carefully typing their World Wide Web address into the address box and, in turn,

locating their *Contact Us* page. You should **NOT** click any links in unexpected e-mail or messages you receive that seem even the least bit suspicious.

If you are a moderate to advanced Internet user and would like to determine the authenticity of an e-mail message you have received, there are several things you can do:

1. Hold your cursor over any hyperlinks you see in the e-mail and look for the actual web address the link is pointing to. Compare it to what you see on the screen and what you would expect. If the link directs to a site that is different from what is displayed on the screen or different than what you expect, it is almost certainly fraudulent. In Figure 2.3 below, the http://www.regions.com/reward_survey.shtml actually points to <http://bio.cse.pusan.ac.kr>, which appears to be a fraud artist located in one of the Koreas.
2. If it is HTML-based e-mail, right-click on the message, and *View Source*. Look for any href attributes in the HTML code. Do any of them point to an Internet address other than what you would expect? In Figure 2.4, the HTML code contains two distinct href addresses. One is tied to an anchor tag and points to ebay.com, making the e-mail look legitimate. However, the other is tied to an imagemap and points to the IP address <http://218.8.252.73>. A little research at <http://www.arin.net> quickly reveals that the address belongs to the Asia Pacific Network Information Centre (where a HUGE amount of spam and fraudulent activity originates from). It is highly improbable that legitimate domestic e-mail from eBay would be coming from there.
3. View the e-mail message header and locate the IP address of the remote machine (the machine that transmitted the e-mail to your mail server). Look it up at arin.net. Is it assigned to a U.S. organization or are they outside of the U.S.? If it's a U.S. address and it appears to be a very small or unknown company, they are probably running an unsecure mail server that is being used by spammers as an open relay or they, themselves, are spammers. If it is outside the U.S., it is almost certainly fraudulent.



REGIONS 

Phishing
Example 1

Dear Customer,

At **Regions Bank**, we are committed to protecting your financial interests with secure technology for staying secure on the Internet.

As a **Regions Bank** customer, you have been chosen by customer department to take part in our quick and easy 5 question survey. In return we will credit \$20 to your account - Just for your time!

Helping us better understand how our customers feel, benefits everyone. With the information collected we can make changes to improve and expand our services. The information you provide us is all non-sensitive and anonymous - No part of it is handed down to any third party groups. It will be stored in our secure database for maximum of 3 days while we process the results of this survey.

We kindly ask you to spare two minutes of your time in taking part with this unique offer!

To continue click on the link below:

http://www.regions.com/reward_survey.shtml

Really points to <http://bio.cse.pusan.ac.kr>

Regions Bank
One Indiana Square
Indianapolis, IN 46204

Figure 2.3

-----Original Message-----

From: eBay Inc [mailto:custservice_id_643090177884561@ebay.com]

Sent: Thursday, August 18, 2005 5:08 PM

To:

Subject: ***SPAM*** Score/Req: 7.5/5.0 - eBay Inc: Important Notice [Thu, 18 Aug 2005 20:08:49 -0200]

Phishing

Example 2



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.

To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

This entire message is really an image link that points to <http://218.8.252.73>, a computer address outside of the U.S.

Copyright © 1995-2005 eBay Inc. All Rights Reserved.

Figure 2.4



Phishing Examples 3 and 4



The popularity of PayPal has made it a primary focus for fraud artists. Displayed here are two spam messages designed to trick the recipient into revealing account information. Both were forwarded to spoof@paypal.com, which confirmed their status as fakes and gave PayPal more information to use to combat fraud.

Figure 2.5

Figures 2.3, 2.4 and 2.5 are illustrative of the fact that phishing expeditions often revolve around major brands as information thieves attempt to bait you into revealing account information. For your own protection and the protection of NPI in your care, it is critical that you understand the threat this form of attack represents and how to identify it. Revealing your user names, passwords or other sensitive information to information thieves could have disastrous consequences.

Web Browsing



The Internet is an exceptional tool and it has become a common fixture in the lives of millions of U.S. residents each day. Unfortunately, it is also one of the greatest security risks. Despite the fact that web browsers such as Internet Explorer and Firefox have evolved to include a large variety of

security features, they are still not without the occasional problem in the form of minor bugs and browser exploits, nor are they able to protect us from every conceivable threat while maintaining their usefulness. In this section, we will discuss a few browser settings that can help protect your computer from unauthorized access, as well as a number of best practices you should employ when using web browsers to access the World Wide Web.

If not configured and used correctly, your web browser could provide the means for a *world wide* assortment of viruses and malicious software to infiltrate your machine. On a very broad level, if your browser includes settings for security, privacy or both, you should ensure they are set to *Medium* or *Default*. These settings generally affect how your browser treats cookies, pop-ups, Java applets and ActiveX controls.

Cookies

Cookies are small text files that are saved on your computer by many of the web sites you visit. Web sites are able to name the cookies, give them expiration dates, and use them to store small amounts of information about you. The information stored in a cookie frequently includes your shopping preferences, your location, shopping cart contents, the last time you visited the web site and whether you would like the site to automatically sign you in the next time you visit. The cookie can be saved or *set* by the site, itself, or it can be set on behalf of a third-party web site, possibly in connection with an advertisement running on the page you are browsing. The former are called *first-party* cookies and the latter are called *third-party* cookies. Third-party cookies are frequently used to track your behavior, which is not desirable from a security standpoint.

To better understand how cookies work, let's look at an example:

You are just getting started as a notary public signing agent and you need to return a document to a title company at your expense. They have requested that you send it via UPS. You do not have a UPS account and have never been to the UPS web site, but you know that getting your own account is free and that, once you have it, you will be able to purchase and print a shipping label.

You open your web browser and type `http://www.ups.com` into the address bar. You see a screen that asks what country you are in. You select the United States. At that point, UPS.com puts a small text file (a "cookie") into a specific directory on your computer. The cookie is named **defaultHome**, it is tied to ups.com, it is stored in the file `[yourname]@ups.com` and it contains the following information:

```
defaultHome
us_en_home|1170971240913
ups.com/
1024
772498432
29911708
198427232
29838283
*
```

The next time you visit UPS.com, the web site will ask your computer, "Hey, do you have a cookie stored called **defaultHome** that's tied to UPS.com?" Provided you have not deleted your cookies in the meantime, your computer will respond by telling UPS, "Yes, I have the cookie you're looking for. Here's what it contains." From the contents of that cookie, UPS.com will know that your default country is the United States. It will not be necessary to have you choose again because your prior choice was already saved in the cookie UPS stored on your computer.

In the example above, UPS is using a first-party cookie. That is, it is *their* cookie and it references ups.com. If you were to subsequently sign-on to ups.com, they might also set a *session cookie* on your computer. Session cookies are harmless and help to keep web servers and web browsers *on the same page*.

In contrast to first-party and session cookies, third-party cookies are frequently used by advertisers and data collection organizations to track your behavior for the purpose of compiling statistics or for delivering targeted ads to your computer through participating web sites. Here's an example:

You're now a very successful signing agent and e-docs are your specialty. You run through ten reams of legal paper per week and buying it from the local office supply store is getting really expensive. You take to the Internet and find a web site for the Super Cheap Paper Company (SCPC). The SCPC web site sets a cookie on your computer on behalf of an advertising entity they are working with that contains the text "I just visited the Super Cheap Paper Company web site." The cookie is called **BigNuisanceAdvertising**. Later in the day, you still haven't decided where you're going to buy your paper from and figure it can wait until tomorrow. Instead, you open your favorite Internet news site. That site has partnered with Big Nuisance Advertising and is configured to *request* the cookie named BigNuisanceAdvertising. The news site learns that you "just visited" the SCPC web site and dynamically displays an ad in the right-hand margin. It reads: "Save money! Get cheap paper here!!"

Because they often reveal information about your behavioral patterns and share that information with outside parties, third-party cookies put NPI in your care at greater risk. You should therefore consider the following policy for the handling of cookies by your web browser:

Recommended Web Browser Cookie Policy

- Always allow session cookies
- Block third-party cookies
- Accept first-party cookies or have your browser Prompt you when a site tries to set a first-party cookie

Many Internet security suites will either make these changes for you or will warn you if your browser security and privacy settings are not strong enough.

Pop-ups

For the purpose of this guide, a pop-up is any form, dialog or extra window that *pops-up* or displays in connection with your web browser. Pop-ups can be solicited or unsolicited and either helpful or harmful. In most cases, pop-ups require some form of input from you, which is the

primary reason they are a threat to NPI stored on your machine. If you are not careful, you could inadvertently click something that allows malware to install itself on your computer.

Please take a moment to review the following table. Notice that the *solicited* pop-ups were displayed as a direct result of your action (e.g. a click), while the *unsolicited* pop-ups appeared on their own. Also, pay close attention to the *harmful* column; these are the pop-ups we are most concerned with.

	Helpful	Harmful
Solicited	<p>1) Small web pages that open in new windows in response to a link you have clicked for the purpose of displaying additional information on some topic.</p> <p><i>Many web sites offer help or display additional product details in pop-up windows when you click a link.</i></p>	<p>1) Pop-ups that ask you if it is okay to install or run something on your computer that result from clicking a link or image on an untrusted site.</p> <p><i>If the site you are surfing is not 100% trusted and highly reputable, you should be <u>extremely wary</u> of any pop-ups that ask you for permission to install or run something. Note that in some cases, the pop-up may be displayed by your web browser in response to a request from the site to install something like a Java applet, ActiveX control or toolbar on your computer. You should not allow this unless you are absolutely positive you can trust the site.</i></p>
Unsolicited	<p>1) Pop-ups warning you of a pending session timeout at a trusted web site such as your banking institution.</p> <p><i>"Your session is about to expire. Would you like to continue banking?"</i></p>	<p>1) Pop-ups that appear asking if you would like to change your home page.</p> <p><i>"Would you like to set your home page to searchco.com?" This is common tactic employed by search funnels - sites that exist solely to funnel your traffic to them by using names that are deceptively close to common names for the purpose of generating click revenue. Often, when you try to leave one of these sites, they will ask to become your home page. Be very careful not to inadvertently approve requests like these.</i></p> <p>2) Pop-ups advertising products.</p> <p><i>Advertising pop-ups are a general nuisance and a distraction that often add confusion to your computing environment, which increases the risk to NPI.</i></p> <p><i>While most advertising pop-ups spring from the web page you are currently viewing, they can also be generated by adware that's hiding on your computer. If you continually see advertisements in the same position on your computer screen or that appear with great regularity or advertise the same products, your machine is probably infected with adware.</i></p> <p>3) Pop-ups that display pop-ups.</p> <p><i>In some cases, unsolicited pop-ups can spawn other unsolicited pop-ups, leading to a seemingly endless barrage of windows. Sites that do this typically have little regard for your privacy and are inherently very high risk sites. If you discover a site like this, you should do whatever you can to avoid it. Start with a rapid sequence of Alt+F4's to close the windows that are opening.</i></p>

Table 2.1

Fortunately, most current web browsers include integrated pop-up blockers, which you should enable since they will block the majority of unsolicited pop-ups, especially distracting advertisements. In Microsoft Internet Explorer 7, the pop-up blocker setting is configured from **Tools | Pop-up Blocker**. You should make sure to turn this on and, if you have any sites you routinely visit that display *helpful* pop-ups, you should add them to the "Allowed sites" list under the **Pop-up Blocker Settings**.

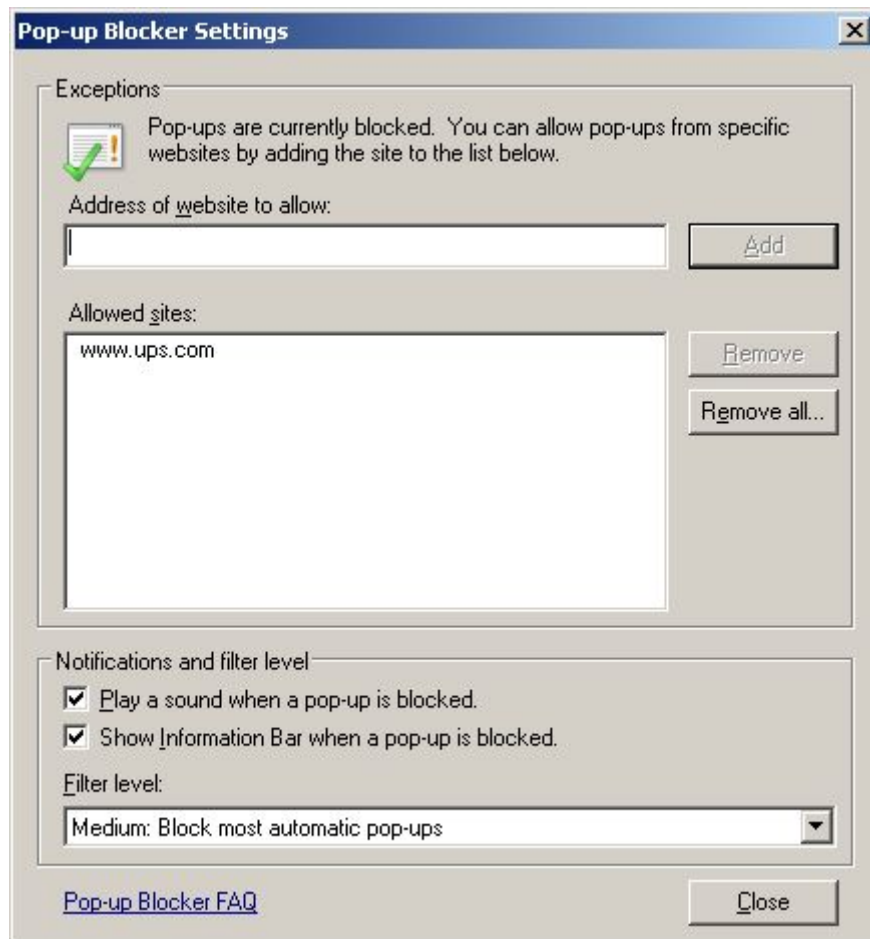


Figure 2.6

Recommended Web Browser Pop-up Policy

- Block most automatic pop-ups

Outside of pop-up blockers, you should familiarize yourself with what is required to close a window in your operating system without having to click anything with your mouse. In Microsoft Windows, this can usually be accomplished using the Alt+F4 key combination on the keyboard.

Using the keyboard to close a suspicious window will ensure that you aren't fooled into clicking a button or *what appears to be a button* on a pop-up window that, in turn, allows malware to install on your computer.

Java Applets and ActiveX Controls

Java applets and ActiveX controls are small programs capable of running within your web browser that are part of many web sites today. These programs are typically designed to perform some function that is otherwise difficult to do with normal HTML (the language that is used to build web pages). An example of a Java applet would be a mortgage calculator that includes sliders which allow you to dynamically change assumptions - purchase price and interest rate, for example - and see the results change before your eyes. (Such an applet could also be written in Javascript or as an ActiveX control or as a Macromedia Flash file.)

Care must be taken when allowing Java applets to run on your machine and *special care* must be taken if you are considering allowing an embedded ActiveX control to run in your browser. ActiveX controls can do pretty much anything a normal application, or even a virus, could do to your machine. For that reason, it is critical that you are able to verify the authenticity of the ActiveX control and that you completely trust its author.

Recommended Web Browser Java Applet and ActiveX Control Policy

- High safety for Java permissions
- Disable ability of ActiveX controls to run without prompting
- Disable automatic prompting for ActiveX controls
- Prompt to download signed ActiveX controls
- Disable download of unsigned ActiveX controls

Using the default privacy and security settings in Internet Explorer 7 and up, and Firefox 2 and up, in concert with safe computing practices, should be adequate to reasonably ensure the safety of NPI stored on your computer.

Best Practices

Once your web browser has been properly configured to deal with threats arising out of cookies, pop-ups, applets and controls, there are a number of best practices you should follow. They include keeping your browser updated, using secure mode when accessing sensitive information over the Internet, avoiding high-risk activities, and educating your family on safe computing practices.

Updates. You should keep your web browsing software up-to-date in the same manner that you keep your operating system software up-to-date. If your web browser includes an auto-update function, you should use it to ensure you always have the most current security fixes. If it doesn't, you should check the vendor's web site regularly for updates, downloading and installing them as they become available.



Secure Browsing. When accessing confidential information over the Internet, you should always ensure that your browser is operating in *secure mode*. When running in secure mode, your web browser and the web server it is talking to will encrypt everything they say before sending it over the public network, which is susceptible to snooping. When it reaches the other side, it is decrypted. If anyone is sitting in the middle snooping the traffic, all they will see is a jumble of characters. In order to confirm you are surfing securely, look for "https" in the address line of your browser, along with a padlock icon in locked position.

Avoid High-risk Activities. In order to help keep your confidential information safe and secure, you and anyone with access to your electronic equipment (your computers and other devices, along with any devices connected to them via a network) should avoid high-risk web sites and behavior that could jeopardize the security of your devices. High-risk sites and behavior generally include anything related to:

- peer-to-peer file sharing (applications like Kazaa, LimeWire, Shareaza, MLDonkey and Instant Messenger applications with file sharing enabled)
- pornography
- illegal music download sites, including sheet music (like guitar tabs) and lyrics
- illegal software sites (warez, crackz, serialz, etc.)

Activity in these categories is a particular threat to families with teenagers for a couple reasons: 1) It is unlikely your teenager will openly announce that they are engaging in risky behavior, meaning you might not find out about it until it's too late, and 2) Each of these categories involves the introduction of foreign files to your computer or computer network, and the likelihood of contracting a virus, worm or malware from one of these sources is a magnitude greater than it is when downloading something like a work-related software utility from a trusted business site.

Educate Your Family. If you work from home, it is important that your family and anyone else using your equipment understand your responsibilities as information steward as they relate to the protection of around-the-house confidential data. It is your responsibility to see that they

have a good grasp of safe computing principles and that the principles are followed. Ultimately, you will be held accountable for information that is compromised or used inappropriately as a result of their actions.

Internet Security Software and Firewalls

Most of the electronic threats we have addressed to this point can be severely lessened, and sometimes eliminated all together, by a combination of safe computing and Internet security software. Because Internet security software is vitally important to the protection of your devices, it is worth restating that having it installed is an absolute must. At a minimum, you should be running security software that helps prevent and detect the following threats:

- Viruses and worms
- Malware, including adware and spyware

The software should include the capability to scan inbound e-mail for e-mail-based threats and you should keep it current using automated or frequently downloaded updates so that it understands how to detect the latest threats.

In addition, you should install and maintain a software-based *firewall* if one is not already built into your operating system. (Windows XP includes a built-in firewall, but many users choose to install third-party firewalls since they are often more aggressive.) The purpose of a firewall is to validate all incoming and outgoing communications involving your system. These communications travel as data packets through *ports* in your computer. Ports are like little electronic doorways and the data packets are like little messengers. A firewall is similar to having a guard posted at every door who can open and close the door as necessary, lock it, as well as decide which messengers are allowed through which open doors.

Behind each door, there is a room, and that room is used for a specific purpose. The room behind door number 80 is used for web surfing; the room behind door number 443 is used for secure web surfing. The guards will usually let messengers in and out of these rooms, provided the computer has requested it. However, they will not let messengers access the doors leading to your confidential information. In fact, those doors are generally locked. That is one thing a software firewall does for you.

Hardware firewalls operate on a similar premise and should also be used whenever possible. High-end firewalls include brands like the Cisco PIX and the Juniper Netscreen. If you work for

a large company, your Internet traffic may be secured by one of these devices, in which case it's probably not your responsibility. If you work out of your home, however, it is your responsibility. Fortunately, many consumer networking devices now include low-end, but still very effective, hardware firewalls. If your Internet traffic is being routed through a DSL or cable router, it's quite possible that router has a built-in firewall and that, by default, the firewall is configured to give you a decent level of protection.

Remote Access

In the event you need to access your computer remotely, you should make that access as restrictive as possible by using strong passwords; hardware-based, secondary keys such as SecurID™; encrypted communications (VPN tunnels); and by limiting access times if possible. If you do not have a need for remote access and terms like Remote Desktop Assistance, PCAnywhere, GoToMyPC, IPSec, PPTP and RAS mean nothing to you, then this advice does not apply to you.

Protecting Secondary Electronic Devices

If you own electronic devices other than your primary computer that either a) Store sensitive customer information, or b) Can be connected to a device that contains sensitive customer information, you should exercise the same degree of care as you would with your primary device. Secondary devices include laptops, Personal Digital Assistants (PDA's) and data-capable phones. Due to the portability of many secondary devices and the fact that they are often wireless-enabled, special concerns should be observed, particularly when away from the home or office. Wireless concerns are covered in the next section and another significant threat - the threat of theft - is covered in Section 3 of this guide.

Wireless

Wireless networks offer a very convenient means for connecting your electronic devices to each other and to the Internet. It is now possible to connect your laptop or other device to the World Wide Web from anywhere in your home, as well as in hotels, restaurants, conference centers and coffee shops. Some notary signing agents are even running complete mobile offices from their vehicles, allowing them to receive and print last-second e-docs while on the road.

Wireless connectivity is not without risks, however. Wireless signals must be broadcast through the air, meaning anyone within range would conceivably capture the signal. In many cases, that range could extend beyond 100 feet, making it available to your neighbor or even someone

parked in a car outside your home. Unless you are following the appropriate security procedures, this could put your sensitive information at risk by either broadcasting it or unknowingly allowing access to your computer system.

What are the appropriate security procedures? If you are using a wireless network - whether it's in your home, office or at an outside location - you should *strongly* consider the following security practices:

- If you are responsible for the security settings on the wireless router that is coordinating the communication, you should see to the following:
 - Disable SSID broadcasts. Your wireless network will have a name and these broadcasts will announce its existence to the world. Provided you already know the name and have configured all clients to talk to it, you can disable these announcements.
 - Enable MAC address filtering and add the hardware address of each client device to it that should be allowed to connect to your router.
 - Enable encryption. All communication between the wireless router and wireless clients, such as a laptop, should be encrypted.
 - Periodically check for new firmware versions and install them as they become available. Firmware is the embedded software that your device uses to operate and updates often address security and performance problems.

Most of these items will be covered by your product documentation, so you should read it.

- Disable the wireless antenna on your device when not in use. Laptops frequently have a button for this that is labeled with the image of a small antenna. If your device is wireless-capable, read your manual to learn how to turn the antenna on and off. (Note that the antenna will likely be *internal*, so you won't necessarily see it.)
- Operate in wired mode when possible, with your wireless system turned off.

By employing as many of these practices as possible, you will greatly reduce the risk to NPI stored on your system.

Section 3: Physical Access Security

When not in use, NPI in your care should be stored securely at all times. In Section 2, we covered *virtual security* - the standards of care you should employ when dealing with electronic information. Software updates and password policy were presented as two broad security issues for which you should have established policies; electronic threats, such as viruses, worms and malware were defined, along with how to detect and prevent them; safety considerations surrounding e-mail, web-browsing and portable devices were presented; and the use of firewalls and the hazards of wireless computing were discussed. In this section, we will focus on physical access security: controlling physical access to paper and electronic records.



Around the Home and Office

Any confidential information you have been entrusted with should always be securely handled. This includes *residual* confidential information, such as you might record in your notary journal.

Sensitive information should be kept under your direct and exclusive control whenever possible. When NPI is not under your direct and exclusive control, it should be stored in a locked file cabinet, desk or safe (in the case of paper-based records) or in an electronic device that is adequately protected from theft and unauthorized access.

Protecting your storage areas and electronic devices from unauthorized access is best accomplished by keeping your office, or any other location where customer files are stored, locked while you're away. If working from home, you should ideally have dedicated office space and a computer that is used exclusively by you for your business purposes. If this is not possible, you should consider educating all family members - and anyone else who is authorized to use your space or your equipment - on your responsibilities as information steward and the need for physical access security. Uninformed or naïve family members are often one of the greatest threats to the safety of confidential information and should be familiar with both electronic and physical access security standards.

Finally, for your own protection and the protection of sensitive information in your care, you should consider a monitored alarm system for your premises. Complete systems can be purchased for a few hundred dollars and monitoring is often as little as \$20 per month. Alarm systems represent one more layer of security a would-be information thief would have to contend

with in order to gain physical access to your files.

Away from the Home or Office

Non-public personal information must often be taken out of the home or commercial office. This is particularly true of mobile notary signing agents who routinely taxi confidential customer information around town. When you're *on the go*, there are several things you can do related to portable devices, bags, briefcases and vehicles to limit unauthorized physical access.

Portable Devices, Bags and Briefcases

Generally speaking, in order to be *mobile*, mobile information must be stored in *something*. That something is usually an electronic device, such as a laptop, or in an envelope or file folder stored, in turn, in a bag, tote or briefcase. These information containers should be kept close to you and under direct supervision where possible. This is especially true of small electronic devices, which are high value targets for many thieves.

Thieves tend to frequent settings that offer a variety of targets and, preferably, some form of commotion. Busy restaurants, Internet cafes, airports, libraries and hotel lobbies provide ample opportunity for thieves to *walk-off* with unattended property, especially if it appears to be valuable. Value, however, is relative and beauty is in the eye of the beholder.

To the drug addict, your electronic devices will appear absolutely tantalizing. Once stolen, they can easily be traded for the next fix. That type of thief will be less interested in things having little intrinsic value, such as a bag full of sensitive paperwork. To the sophisticated identity fraud artist, however, your \$2000 laptop and your \$20 tote may appear equally valuable if he has been given any indication that they contain confidential information. For that reason, observing the following maxim is always a very good practice:

OUT OF SIGHT, OUT OF MIND

In other words, your notary gear should be plain and unbranded. If possible, laptops should be transported in cases that *do not appear* to be laptop cases and bags, totes and briefcases should not contain any branding that shouts: **"I am a notary public! This tote contains my notary seal, notary journal and sensitive documents."** Given the risks of today's fraud-filled environment, using a nondescript laptop case, tote, bag or briefcase when transporting expensive devices and sensitive materials is one more step toward keeping NPI in your care secure.



WARNING: This bullseye could draw an identity thief straight to your tote and your customers' confidential information.

Finally, it is recommended that any laptop case, bag, tote or briefcase you use have a working lock, which you should utilize. In addition, both your electronic devices and your storage containers should be equipped with some mechanism that will allow you to secure them to a table or other stationary fixture when left unattended in, say, a hotel room. Kensington (<http://www.kensington.com>), for example, carries a wide variety of notebook locks.

Vehicles

Storing any type of sensitive information in your vehicle is generally a bad idea. Cars and other vehicles are broken into daily all over the world by individuals looking for *anything* valuable to steal. Electronic devices, briefcases, and even file folders have become targets in a world fraught with identity fraud.



If you are transporting sensitive documents and find it necessary to stop at a location that's not related to your job, you must weigh the risks of leaving NPI locked in your vehicle (and possibly even in your trunk if you have one) versus taking it with you. A prime example would be the notary signing agent who has just met with a borrower some 60 miles from the signing agent's home. The borrower lives close to a colleague of the signing agent, so they schedule a dinner meeting at a nearby restaurant. The signing agent must decide whether the loan documents she is carrying are safer in a briefcase in the restaurant with her, or locked in the car. This is a judgment call and will depend on several factors:

- the time of day

- how long she expects the meeting to last
- how busy the restaurant is
- any security features the vehicle has
- whether the briefcase can be secured or tethered to the vehicle

The point here is that the information steward must always be thinking about how to protect the information in their care and must make sound decisions.

Summary

The information presented in this guide should serve as a good foundation for establishing a solid plan for the safeguarding of confidential customer information or non-public personal information (NPI) in your care. After reading this guide, you should be prepared to formulate your own information protection plan in accordance with the following rules:

- Treat all customer information as NPI
- Properly return documents and other materials containing NPI to authorized parties
- Retain NPI only as long as needed to perform your duties or to comply with the law
- Adequately destroy documents and other materials containing NPI when they are no longer needed to perform your duties or to comply with the law
- Protect NPI from unauthorized access, alteration, destruction, loss and use while it is in your care by employing best practices with respect to electronic security and physical access to information
- Immediately notify the owner of documents containing NPI if you suspect or are aware of a breach, alteration, destruction, loss or any other unauthorized use of NPI

Failure to have a plan that addresses these rules and to adhere to it could lead to disastrous consequences for you and your clients, ranging from identity fraud to devastating lawsuits. Business reputations could suffer irreparable harm and the damage that could be done to a customer from a single breach of confidential information could be immeasurable.

The bottom line in protecting yourself and your customers' information is to follow the rules, analyze the risks and special circumstances of every situation, and, most of all, use sound judgment and common sense toward your vigilant pursuit of superior stewardship and information security.

This training guide is Copyright © 2007, The National Verification Registry. It is freely available to sponsors of the Notary Public Background Check (NPBC) Certification solution for integration into notary public and signing agent training curricula. Located at <http://www.notarypublicbackgroundcheck.com>, NPBC is an industry-sponsored notary verification registry. Listed notaries have been identity-verified, background-checked, and have a sworn understanding of privacy principles.