



CITY OF PALMDALE



How  
**SAFE**  
is the  
**Internet?**



**A C S**

*Prepared by Jennifer Findley, ACS*

*Design by Kathleen McGrath, ACS*



## How Safe is the Internet?

*Prepared by Jennifer Findley, ACS*



### How safe is the Internet?

In today's world, it's easy to see why the Internet is such an integral part of our everyday lives. The World Wide Web is virtually everywhere; it allows us to access a vast wealth of resources and information and connects people around the globe with a level of convenience and speed never before seen. But how safe is the Internet?

Just about every day we find ourselves being flooded with unsolicited e-mails from people trying to sell us something, infect our computers with a virus, or trick us into giving out our personal information. We constantly hear about new dangers, such as spyware, adware, phishing, and pharming; and now we find ourselves dealing with another rapidly growing threat: computer related identity theft. The fact is, there are malicious individuals and groups out there who have made it their mission to try to damage or take control of our computers, steal our personal information (such as banking information or credit card numbers), and even steal our identities. To make matters worse, these individuals can be extremely hard to catch or even identify, and it can often be difficult to detect their activities until it's too late. It's no wonder that the fastest growing concern for Internet users is security.

*We constantly hear about new dangers, such as spyware, adware, phishing, and pharming.*

### So what can we do to keep ourselves safe?

The first and most important step towards protecting ourselves is education. There are many methods that attackers use to try to gain access to our information, and they are constantly changing. The more we understand about the threats that are out there, the more we know about how to combat them. First, (for those of you that may not be familiar with them already) we're going to start by looking at a brief definition of a few of the biggest threats currently on the Internet. Then we're going to look at several of the most important ways to safeguard our computers against such threats. Finally, the last

*Continued on next page...*



## How Safe is the Internet?

Prepared by Jennifer Findley, ACS



page contains links to various resources found on the Internet that will help keep you educated, informed, and protected.

There's no doubt about it, staying safe on the Internet is a constant challenge. However, armed with the right tools and information, we can help to ensure that our Internet experience is as safe and fun as possible-- now and in the future.

**🔒 SECURITY TIP: Most people are aware of the fact that there are malicious individuals and groups out there who are trying to steal their information. But did you know: most of these groups are not targeting large corporations; they're after regular computer users like you and me. The important thing to remember is that they will target anyone who is unprotected.**

### What Is... ?

#### Phishing

Phishing on the Internet is very similar to fishing with a rod and reel; both use bait to try to hook an unsuspecting victim. Here's an example: let's say you receive an e-mail purportedly from your bank stating that an unauthorized transaction has been made on your account, and that as a precaution, your account has temporarily been frozen. The message goes on to say that if you wish to have your account reactivated you must click on the link contained in the e-mail and verify your identity-- or risk having your account closed. What do you do?

Unfortunately, this e-mail is not what it claims to be, and clicking the link will not take you to your bank, but to a fake Web site where a malicious individual or group can track and record any information you type in, from passwords to

***Phishing:***  
*The act of someone trying to pass themselves off as a legitimate company to trick you into giving them personal information.*

*Continued on next page...*



## How Safe is the Internet?

Prepared by Jennifer Findley, ACS



account numbers. Armed with this information, the would-be thieves then have everything they need to steal your money-- and your identity. This is known as *phishing*, or the act of someone trying to pass themselves off as a legitimate company or entity in an attempt to trick you into giving them personal information.

### Pharming

Where phishing involves “bait” in the form of an e-mail or phone call, pharming actually bypasses that altogether. Instead it attempts to trick you into thinking you’re at a legitimate site when in fact you are not. For example, let’s say you want to visit your bank’s Web site. In a pharming attack, you would be able to type in the address of your bank but instead be redirected to a malicious Web site. If you’re not paying close attention, you might not even notice that you’ve been redirected. You then try to log onto this bogus site still thinking it’s your bank and guess what-- now they have your user name and password (or worse).

***Pharming:***  
*The act of attempting to trick you into thinking you’re at a legitimate site when in fact you are not.*

There are several methods a malicious individual can use to carry out an attack like this, and their deceptions can often be very convincing. Unfortunately, the very nature of this type of attack makes it all the more difficult to detect.

### Spyware/Adware

Do any of these advertisements look familiar?

- ◆ *Free spyware removal! Remove spyware, adware, and viruses. Just click here!*
- ◆ *Free smileys for your computer-- insert smileys in e-mails or chat!*
- ◆ *Free music downloads! Download music, documents, software, images, screensavers and games.*
- ◆ *Keep your computer time accurate! Now you can synchronize your computer with the US Atomic clock!*

*Continued on next page...*



### **Spyware/Adware continued...**

One day, you're at home (or the office) surfing the Web when you notice an advertisement like this. It looks harmless, you definitely can't beat the price, and if it doesn't work out, you can always remove it-- so you decide to give it a try. For awhile everything seems to be going fine, but then you start to notice some problems. Maybe your computer is running a bit slower than it used to. There may be a couple of programs or icons on the machine that you don't remember seeing before. And now your Web browser has started opening Web pages or search engines that you didn't want. You decide that it's definitely time for the downloaded program to go. But worst of all, even though you've tried several times to remove the program, it just keeps coming back.

These are things you're bound to run across anytime you're on the Internet. Pop-ups or Web sites can offer applications that promise to help make your life, both at home and at work, easier and more fun. And sometimes they can! But there's something that most of these advertisements fail to mention: when you click on their links, **YOU ARE DOWNLOADING SPYWARE!** Spyware is basically a software application that runs undetected in the background, collecting information-- and sending the information it finds to a third party. It can come in many forms; monitoring your activities and habits on the Internet (for advertising purposes), gathering information you've stored on your hard drive, and even collecting e-mail addresses, passwords, and credit card information. In many cases, it leaves your system vulnerable to attack, and you may find that someone has been hijacking and controlling your computer-- and you never even knew they were there.

***Spyware:***  
*Software that collects information from your computer and sends it to a third party.*

**🔒 SECURITY TIP: Spyware can also be installed in the background without your knowledge or consent, so be very cautious what Web sites you visit when you're on the Internet. For more information on preventing spyware please check out the following section on how to protect your computer.**

*Continued on next page...*



### How can I protect my computer?

#### 1. Use a Firewall.

A firewall is a software or hardware based solution that monitors and controls all traffic between your computer and the Internet. It acts as a personal security guard, only allowing legitimate traffic to pass to or from your system. Dangerous or suspicious traffic is blocked, thwarting possible attacks launched by hackers or other malicious individuals. Some firewalls will allow you to configure them yourself by choosing what should be considered safe and what shouldn't, while others are preconfigured and can be used straight out of the box. There are many brands and types to choose from, each with different capabilities and options, and even some that are free. In fact, Windows XP automatically comes with a built-in firewall that you can use. Other popular brands include Symantec and McAfee (among many others). The key is choosing a firewall that best suits your needs.

 **SECURITY TIP: Most often, when it comes to firewalls, you get what you pay for.**

#### 2. Install Antivirus.

Antivirus software monitors your system for viruses and cleans or removes infected files. It also blocks new viruses from being installed on your machine. In most cases, it even includes protection against spyware and phishing attempts. Without Antivirus, it's not a question of *if* you will be infected by a virus, but *when*-- it's only a matter of time. **Make sure you are protected.** As with firewalls, there are many brands of Antivirus to choose from, including some that are free. Depending on price range, several brands on the market right now even come with a built-in firewall, spam filter, pop-up blocker, and built-in Parental Controls that will help you control and monitor the sites visited by your younger Internet users.

*Continued on next page...*



**🔒 SECURITY TIP: Viruses can infect your computer through many avenues, including music downloads, e-mails, and even through attachments sent through Instant Messaging. If you receive e-mails or attachments that you haven't been expecting, especially from someone you don't know, don't open them. Whenever you're downloading something from a site on the Internet, use extreme caution and stick with well-known, reputable sites.**

### **3. Keep your Antivirus up to date.**

As new viruses hit the Internet, Antivirus companies respond by sending out updated virus definitions. Once installed on your computer, these updates tell your Antivirus software what to look for and block, so you don't become infected. Many Antivirus companies have also started including spyware and phishing definitions with their virus updates to help protect you from these newer types of threats. **Make sure you keep your Antivirus up to date.** Most types of Antivirus have the option of enabling automatic updates. Whenever you're connected to the Internet, whether it be through dial-up or high speed, the Antivirus software will automatically check for updates on a regular schedule, and then download and install the updates with no intervention necessary on your part. You can also choose to update your Antivirus manually. Whatever option you choose, please remember that this step is just as critical as steps 1 and 2; after all, having out of date virus definitions is virtually the same as not having Antivirus at all.

### **4. Keep your Operating System and Applications up to date.**

This is a critical, but often overlooked way to help keep your computer safe. Software inherently contains holes and vulnerabilities that can be exploited by an attacker. As these vulnerabilities are discovered, many software companies create patches and hotfixes that address these issues and help make your computer less susceptible to attack. An example of this is Microsoft's Windows Update, which contains updates and patches for Microsoft operating systems and other applications such as their Office Suite. Depending on what operating system you're running and what programs you have installed, you'll need to

*Continued on next page...*



visit the appropriate Web sites regularly and check to see what updates are available (or configure them to update automatically if possible).

### **5. Install Anti-Spyware software.**

There are many great applications out there that are designed to remove spyware, many of which are free of charge. One such application is Microsoft's Windows Defender, a free tool that you can download from Microsoft's Web site. Like most applications of its kind, it gives you the option of scheduling scans to be run on your computer as well as automatically updating its spyware definitions. Again, whichever brand you decide to go with, make sure you **keep it up to date**. Also, while it can be very beneficial to install two or more compatible brands of spyware-removing software on your computer (what one brand misses another might catch), it is usually not a good idea to run scans of your computer with more than one at a time.

### **6. Don't take the phishers' bait.**

As we talked about before, phishers use bait, usually in the form of legitimate looking e-mails, in an attempt to trick you into sharing personal information. Is it possible to tell if an e-mail is phish or not? There are actually several indicators you can look for; for example, is the message full of typos and grammatical errors? Does it address you in a generic way (Dear Valued Customer or Dear Madam or Sir) instead of by your first and last name? When you rest your cursor over the links contained in the e-mail, does the address that pops up in the message bar match the address of the Web site it claims to represent? Does it ask you to provide personal information such as account information or credit card numbers? These are all red flags to look out for that usually (though not always) indicate phish. Generally speaking, the best rule of thumb is to assume the e-mail is not legitimate and contact the company directly, either by phone or by visiting their Web site, to validate the message and conduct your business. Also, always be sure to visit these Web sites by typing in the address yourself-- never by clicking on a link in an e-

*Continued on next page...*



mail. For more information on phishing and how to identify phishing attempts, please check out the resource section on the last two pages.

**🔒 SECURITY TIP: When you do business online, it's always best to go directly to the Web site of the company you intend to do business with. However, if you are about to share sensitive information on a Web site, you first need to check to make sure the site is secure. There are two things to look for: first, the address should begin with https (instead of http), and second, there should be an icon that looks like a closed lock (🔒) on the status bar at the bottom right side of your screen. If *both* of these conditions are not met, information you submit will not be secure.**

### 7. Always stay on the alert

No matter how sophisticated the latest firewall might be, or how thorough your antivirus software is, there is still no replacement for your computer's single-most important security asset: *you*. After all, you are the only one that can decide if an e-mail looks suspicious or not, or if a Web site looks dangerous or questionable. Always be on the lookout and *trust your instincts*. If something makes you uncomfortable, steer clear of it. Remember, never, ever share personal information of *any* kind unless you have verified who you're sharing it with, and don't share the information by insecure methods such as e-mail (see tip below). If at any time you feel that your information has been compromised, notify the proper authorities *immediately*. For more information on what to do if your identity is stolen, please check out the resource section on the last page.

**🔒 SECURITY TIP: It's never, ever a good idea to share personal or sensitive information by e-mail, which is *not* a secure method of transmission. Unless you use special software to encrypt and authenticate your messages, e-mails are easily spoofed, easily intercepted, and easy to read since they are sent in clear text.**

*Continued on next page...*



For more information and resources on...

(in alphabetical order)

### **Antivirus**

- <http://www.symantec.com/index.htm>
- <http://us.mcafee.com/>
- <http://www.sophos.com/>
- <http://www.pandasoftware.com/home/default.asp>
- <http://www.trendmicro.com/en/home/us/personal.htm>

### **Apple Product Security**

- <http://www.apple.com/support/security/>
- <http://support.apple.com/kb/HT1222>

### **Firewalls**

- <http://www.zonelabs.com/>
- <http://www.symantec.com/index.htm>
- [http://www.mcafee.com/us/security\\_wordbook/firewall.html](http://www.mcafee.com/us/security_wordbook/firewall.html)
- <http://www.agnitum.com/products/outpost/>

### **Microsoft Updates**

- <http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us>
- <http://office.microsoft.com/en-us/officeupdate/default.aspx>

### **Mozilla Security**

- <http://www.mozilla.org/security/>

*Continued on next page...*



## How Safe is the Internet?

*Prepared by Jennifer Findley, ACS*



### **Pharming**

- [http://reviews.cnet.com/4520-3513\\_7-5670780-1.html](http://reviews.cnet.com/4520-3513_7-5670780-1.html)
- <http://www.microsoft.com/hk/protect/yourself/phishing/pharming.mspix>
- <http://www.microsoft.com/protect/fraud/phishing/spoof.aspx>

### **Phishing**

- <http://www.antiphishing.org/>
- <http://www.onguardonline.gov/topics/phishing.aspx>
- <http://www.microsoft.com/athome/security/email/phishingemail.mspix>

### **Security Bulletins**

- <http://www.us-cert.gov/>
- <http://www.microsoft.com/security/default.mspix>

### **Security Tips**

- <http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm>
- <http://www.onguardonline.gov/>
- <http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec15.pdf>

### **Spyware/Adware/Malware**

- <http://www.onguardonline.gov/topics/spyware.aspx>
- <http://www.microsoft.com/athome/security/spyware/default.mspix>
- <http://www.microsoft.com/security/malwareremove/default.mspix>
- <http://lavasoft.com/>

*Continued on next page...*



---

## How Safe is the Internet?

*Prepared by Jennifer Findley, ACS*

---



### **Viruses**

- <http://www.sarc.com/>
- <http://vil.nai.com/vil/>
- <http://www.f-secure.com/virus-info/>
- <http://threatinfo.trendmicro.com/vinfo/>

### **What to Do If Your Information Has Been Compromised**

- <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt150.shtm>
- <http://www.microsoft.com/protect/yourself/phishing/remedy.mspx>