

Protecting Your Computer and Your Identity



OFFICE OF
ENTERPRISE SECURITY
DEPARTMENT OF INFORMATION TECHNOLOGY

Security Awareness

Office of Enterprise Security
Department of Information Technology
August 2007



Table of Contents

| | |
|------------------------------------|-----------|
| Why Protect Your Computer | 3 |
| Viruses, Worms, and Trojans | 4 |
| Spyware | 6 |
| Spam | 8 |
| Phishing | 9 |
| Pharming | 11 |
| Firewalls | 12 |
| Internet Frauds and Scams | 14 |
| Avoiding Online Predators | 16 |
| Cyber Bullying | 18 |
| Identity Theft | 20 |



Why Protect Your Computer

If you have a computer that connects to the internet then protecting your computer is crucial. Your computer is not only prone to viruses, spyware and other unwanted traffic including theft of information from your computer, but can also be used for criminal or spamming purposes by hackers. It is common to think that it is not required to protect your computer if you don't have any important data in it. This misconception should be overcome as hackers can use your computer as a scapegoat to launch attacks, commit criminal acts, and send out spam hiding from within your computer, for which you may be held responsible. Your computer has more information and resources that can be useful to hackers than you think. Protect your computer as much as possible by setting various layers of security boundaries.



Viruses, Worms, and Trojans

A virus is a program that can cause damage to a computer and can replicate itself in a computer and over the network or internet. Virus code is usually buried within the code of another program. Once executed, the virus gets activated and spreads in the system. Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment. It is not enough that the email originated from an address you recognize. The Melissa virus spread rampantly because it originated from a familiar address. If files from an infected computer are sent as email attachments, it also infects the computer in which the attachment is opened. A virus can corrupt or delete files or make a computer unusable.

Worm: A self-contained program (or set of programs) that is able to spread copies of itself to other computer systems. The propagation usually takes place through network connections or email attachments.

Trojans: A program that neither replicates nor copies itself, but performs some illicit activity when it is run. It stays in the computer doing its damage or allows somebody from a remote site to take control of the computer. Trojans often sneak into your system attached to a free game.

Tips:

- **Install anti-virus software**
 - Anti-virus tools remain one of the easiest and most comprehensive defenses against malicious code.
 - You can purchase tools such as *Norton AntiVirus* or *McAfee VirusScan*, or there are also free tools such as *AntiVir Personal Edition*.
 - You should have your anti-virus software installed on your computer before connecting to the internet.
 - Make sure to keep it updated.
- **Install a Firewall**
 - A firewall will give you an extra layer of protection between your computer and the internet helping to stop incoming attacks.
- **Update Windows and your browser regularly**
 - Windows and browser will often have security holes, vulnerabilities, which need to be patched before hackers can use them to access to your computer.
- **Keep your browser security at *Medium* or *High***
 - The *Medium* security level contains dozens of tweaks that block common virus propagation techniques.



- The *High* setting goes even further, but it may prevent you from viewing legitimate sources.
- **Don't install "search-help bars" in your browser**
 - Many of these search helpers are used to invade your computer and steal your information.
 - Not all of these search helpers are untrustworthy. *Google* and *Yahoo!* Are ok. You just need to be careful with who you put your trust in.
- **Don't run executable email attachments, even if sent by a friend.**
 - Most worms today spread by infecting a machine and launching a mass email attack. You can stop that attack vector and protect your friends by not running attachments.
 - If you get an attachment you really want to open, save it to your hard drive, run a virus scan, and then open it if it is clean.



Spyware

Spyware is a means of eavesdropping and can be installed on the computer without the user's knowledge or consent by just going to the wrong website. This happens when the website executes a script on the computer (if you have not disabled scripts). Specifically, spyware is computer software that contains surveillance tools that can monitor keystroke activity, take screen snapshots, do email and chat-logging, gather information about the computer user and the user's information and reports it back to the requesting server. The threats for loss of personal confidential information and identity theft are very real. Most spyware come bundled with free programs that you download from the internet. Almost all file sharing applications come loaded with spyware and may also have the ability to download and install more spyware. Before you download free software from the internet, read the policies if available, and determine why it is being given for free. It is a good practice not to download anything from the internet that you do not know about and/or do not trust.

Spyware is also responsible for browser hijacking leading to changing your home page on your browser. For example, if you are planning a Florida vacation, you may be surprised to see relevant ads on travel deals to Florida as pop-ups, emails or other messages. This happens because your internet activities are being monitored by the spyware. If your computer is infected with spyware, the information you transmit over the internet is captured and you will get targeted for ads.

Spyware programs run in the background of your computer without your knowledge and decrease processor performance and memory and eventually slow the overall performance of your computer.

Spyware is not classified as a virus and anti-virus programs do not block it. Spyware requires specific tools to identify and remove the spyware. Spyware is also sometimes referred to as adware. There are many good spyware tools available.

Tips:

- **Update Windows and your browser regularly**
 - Windows and your browser will often have security holes, vulnerabilities, which need to be patched before hackers can use them to access to your computer.
- **Increase your security settings**
 - Windows and browsers have a wide range of security settings to choose from in order to avoid spyware. It is a good idea to check their website for tips and ideas.



- **Carefully read User Agreements before accepting**
 - Always check to see if there will be other software installed. It will often tell you in the User Agreement.
- **Watch out for Windows warning boxes that look like advertisements**
 - Spyware developers with often try to trick you by creating pop-ups that look like windows warning boxes.
 - You should just “X” out the box instead of clicking either Yes or No because both will result in spyware being loaded on to your computer.
- **Be cautious when installing free programs or shareware**
 - Programs that are given away for free will often contain spyware that the author has installed in order to turn a profit.
 - Not all free software contains spyware, just be careful when you are choosing programs to download.
- **Install spyware detecting software**
- **Install a Firewall**
 - A firewall will create an extra layer of protection between the internet and your computer which will help to keep out intruders and spyware programs.



Spam

Spam is unsolicited junk email sent to a large number of people, usually for advertising or marketing on the internet. The act of doing this is called spamming and the people who do this are called spammers. Spammers collect email addresses from various sources and also buy from companies which share email addresses. Spam emails may have a link to click in order to unsubscribe from their email list. It is not recommended to click on those links as that would only confirm your email address and cause more spam to be sent. It is a good idea to filter spam email addresses from reaching your inbox or report them as spam to your email service provider.

Tips:

- **Limit who you give your personal email address to**
 - Only give your personal email address to family, friends, or business associates.
 - When registering your email online, read the privacy policy to make sure that your email address cannot be sold to a third party.
 - Never display your email openly online.
 - Create separate email accounts for public use.
- **Watch for bad spelling and grammar**
 - Spammers will often make spelling and grammar mistakes that would otherwise be picked up by a legitimate company's proofreader.
 - They may also misspell words in order to get passed your spam filter.
- **Don't respond to any spam**
 - Do not try to unsubscribe to the emails, it will be unlikely to stop the emails unless the email that you received required a subscription.
- **Make good use of spam blockers**
 - Check your internet service provider for spam blocking utilities it may offer.
 - Many email clients come with features that allow you to block emails from unwanted sources.
- **Reporting spam**
 - The United States has the Controlling the Assault of Non-Solicited Pornography and Marketing Act.
 - To report spam you should forward a copy of the e-mails to spam@uce.gov.



Phishing

Phishing is a criminal activity using different variations of social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by posturing as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures.

Tips:

- **Never give out personal or financial information in response to unsolicited emails.**
 - If you think that an email has come from a reputable source you should still not respond by sending them information about yourself. Instead call the institution using contact numbers you have already, not a number from the email.
- **Be able to recognize a phishing attempt.**
 - Key words will often be misspelled in order to avoid spam filters.
 - Companies will almost always address you by your name or username. Phishers will often use generic greetings, such as “Hello Valued Customer.” Greetings like this should cause you to be suspicious.
 - Account cancellation and suspension warning are often used to scare someone into divulging personal and financial information. Companies do not usually request urgent personal and financial information through e-mail.
- **Install anti-virus and firewall software.**
 - Some phishing emails will try and trick you into opening files containing a virus or malicious code. Installing a firewall will give you extra protection from these types of threats while your anti-virus software will be essential to detect viruses and malicious code that has gotten past the firewall.
- **Check your credit card and bank statements on a regular basis.**
 - If a scammer has gained access to your accounts most companies will refund you for any fraudulent transactions, but there is often a time limit to report the fraud. That is why it is essential to keep a close eye on your accounts. Don't carry too many credit cards because it will make you more vulnerable to phishing and identity theft. Cancel cards that you rarely use and make sure the cards have your correct address and contact information.
- **Report phishing attacks immediately!**



- If you believe you have received a phishing attack, you can report it to the Internet Fraud Complaint Center at <http://www.ifccfbi.gov>. The Anti-Phishing Working Group, <http://www.antiphishing.org>, is also a good resource for information on various phishing scams.
- If you think that you have been scammed by someone notify all of your account holders immediately and contact the credit bureaus and request a fraud alert on your credit files.



Pharming

Pharming is a hacker's attack aiming to redirect a website's traffic to another (bogus) website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses - they are the "signposts" of the Internet. The term pharming is a word play on farming and phishing. The term phishing refers to social engineering attacks to obtain access credentials such as user names and passwords. In recent years both pharming and phishing have been used to steal identity information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming. Pharming is becoming the attack of choice for today's hackers.

Tips:

- **Pay careful attention to the spelling of the address.**
 - You may click on a link that you think is <http://www.mybank.com> but when you look at the address bar it says <http://nsmymybank.com>.
- **Check the website's certificate**
 - Do this by going to the "File" menu and then select "Properties". Click the "Certificates" box and make sure that the certificate's name matches the name of the web site.
 - Sites with a SSL certificate will also have <https://> in the address bar.
 - If an attacker attempts to impersonate a secure web site, the user will receive a message from the browser indicating that the web site's "certificate" does not match the address being visited. Users should NEVER click "Yes" in response to such a window.
- **Look for a padlock or key at the bottom of your browser**
 - A locked padlock, or a key, indicates a secure, encrypted connection.
 - A broken padlock or a broken key indicates that the connection is not secure.
 - An encrypted connection does not necessarily mean that the site is secure. You need to then check the certificate as stated above.
- **Update Windows and your browser regularly**
 - Windows and browser will often have security holes, vulnerabilities, which need to be patched before hackers can use them to access to your computer.
- **Pharming attackers are advancing their methods constantly so it is important to be careful with your personal information.**



Firewalls

A firewall is hardware and/or software that is used to protect a computer or private network resources from intruders or hackers who might try to break into those systems. Basically, a firewall filters all network packets to determine whether to forward them toward their destination. A firewall provides an extra level of protection that is not provided by an anti-virus program.

Hardware Firewall vs. Software Firewall

Hardware firewalls provide a strong degree of protection from most forms of attack coming from the outside to the internal network. Hardware firewalls can protect computers on a local area network and they can be implemented without much configuration difficulty.

Software firewalls are installed on individual computers and they need sufficient configuration to be effective. Software firewalls contain a set of related programs, usually located at a network gateway server, that protect the resources of a private network from users on other networks or from internal users. Software firewalls allow application screening to verify the interaction between the requesting client and the requested resource.

There are three main types of firewall architecture: Stateful Inspection, Proxy based, and Packet Filtering.

Stateful Inspection actively examines the state of any active network connections and based on this information determines what packets to accept or reject. Stateful Inspection provides the highest level of access control and protection against unwanted intrusions into the network.

Proxy based firewalls requires two components: a proxy server and a proxy client. A proxy client talks to the proxy server rather than to the "real" server that is needed for the requested resources. After connecting to the proxy, the user is authenticated. If the request is approved, the proxy server contacts the real server on behalf of the client (explaining the term "proxy"). The proxy firewall may also perform detailed logging of traffic and monitoring of events on the host system. However, because they are more involved in the connection, proxy firewalls tend to have lower performance than packet filters.

Packet filtering is the simplest of the firewalls and filters packets (allows them through or disallows them) based on certain rules determined by the site's security policy.



Hardware and software firewalls each have their own advantages. The best preparation is to have a combination of both hardware and software firewalls to have a well protected system.

It should be noted that firewalls do not protect you from viruses, so having a firewall does not mean that you don't need an anti-virus program.



Internet Frauds and Scams

The internet has become a great place for buying, selling, trading, and auctioning items. There are many legitimate businesses that sell products and services online. But at the same time there a lot of fraudulent companies and individuals using the Internet as a way to lure and scam people. There are numerous scams on the internet and I few of them include:

Tips:

- **“Get-Rich-Quick” Schemes**
 - The internet is full of claims to get rich quickly and easily. If it sounds too good to be true, it most likely is.
- **Online Auctions**
 - You can find almost anything at an online auction. However, sellers may not hold up their side of the bargain, or merchandise may have been misrepresented.
- **Nigeria email scam**
 - This was an infamous internet scam where crooks from Nigeria or other countries sent out emails that claim they need your help accessing money being held in a foreign bank. If you assist them in accessing their money, they will transfer lots of money into your account in return for assisting them. Inevitably, emergencies come up requiring more of your money and delaying the transfer of funds to your account. In the end the scammer will clear out your account and then vanish.
- **Charity and Disaster-Related Scams**
 - Sometimes scammers will attempt to take advantage of the good nature of people asking them for money to help those in need. When in reality they are just taking all the money that you give them and might even be stealing your account information.
- **Medical Scams**
 - Emails claiming that a product is a quick and effective cure for ailments or diseases, and that there's a limited availability, require payment in advance and offer a no-risk, money-back guarantee. Most include testimonials from customers or doctors verifying its effectiveness. All are intended to steal your money or identity.
- **Credit Card Fraud**



- Fraudulent credit card offers often promise to repair credit reports for a “fee” or to get credit cards for persons with credit problems.



Avoiding Online Predators

Online predators are a serious threat to children online so it is important to educate your children on how to use the internet appropriately. It has been shown that one in five children who use a computer chat room have been sexually solicited online and only one in four children who received a sexual solicitation reported the incident to an adult.

Tips:

- **Keep user names and profiles generic and anonymous.**
 - Many children provide too much of their personal information online.
 - Talk to your children and make sure that their screen names and profiles are non-specific.
- **Remind your children that online friends are still strangers.**
 - Predators trick their victims into believing that they have similar interests and groom children to desire a more intimate relationship.
 - The best defense is to keep your children informed and knowledgeable.
- **Place the family computer in an open area.**
 - You should always accompany your child when they are exploring the internet to provide them with support and direction should they be subjected to aggressive solicitation or inappropriate material.
 - It is important to make sure that you become a constructive part of your child's online experience.
- **Be aware of phone calls or mail deliveries from unfamiliar persons.**
 - Predators will often call or send gifts in an attempt to warm the child up and groomed to meet them.
- **Learn about the internet.**
 - The more you know about the internet the better prepared you are to teach your children about how online predators operate and what you can do together to identify and elude them.
- **Respect children's privacy**
 - It is important to respect your child's privacy, but make certain he or she knows everyone on his or her email or instant messenger



Buddy list. Work to generate parent and child trust that supports open and honest Internet use.



Cyber Bullying

Cyber bully can be defined as any and all verbal harassment that occurs on the internet. This would include but not limited to a nasty instant message, a web site that mocks others, using someone else computer and impersonating them online, and/or forwarding private messages, video, or pictures to other. Cyber bullying, although it may not seem as such, is a serious problem online. It can be used to intimidate, threaten, or scare people into paying a cyber bully money. Yes, some people have went as far as to send death threats to others saying that if they do not pay them a certain amount of money they will kill them. If you are being made the victim of a cyber bully's attack it is important that you remember that persons screen name or address so you will know who to report. Once you have identified who the cyber bully is it is important not to open any other messages or emails from that person. Make sure that you report an attack to the Internet Service Provider, the school, or law enforcement immediately in order to stop the attacks quickly.

Tips:

- **Educate your children on the danger of cyber bullying**
 - Many children will not only be frightened but also confused on what to do if they are the victim of a cyber bully.
 - Be sure to educate your children and encourage them to tell an adult if they are being bullied.
- **Don't open or read any messages from a cyber bully**
 - Your child will not be intimidated by a cyber bully if he does not open messages sent by them
 - Teach your child to ignore and report messages from a cyber bully to a trusted adult.
 - Many email clients and messaging services have features to block messages from certain individuals. Make use of these utilities. They will be helpful in eliminating the cyber bully's attacks.
- **Don't respond to the cyber bully with anger**
 - A cyber bully will feed off of your anger since that is the reaction that they are looking for. Don't give them that satisfaction. It will only fuel them even more.
- **Save the evidence and report cyber bullying**



- Internet service providers are sometimes able to block cyber bullies. Schools and law enforcement also have their own procedures they follow when it comes to cyber bullies.
- Make sure that you save any and all emails and/or messages sent by the cyber bully because they may be needed to take action.
- **Report any type of threat to law enforcement immediately**
 - If a threat is made on your life or on your child's life report it to law enforcement immediately even if you do not know who is sending the message.



Identity Theft

In a time when information is everything identity theft is the fastest growing crime in the United States. It is more important now than ever to make sure that you protect your personal information. Identity theft is a serious crime that can cost the victims months or even years to recover from and can cost those people thousands of dollars if not more. In the time that a person has become a victim of identity theft they could lose job opportunities, be denied loans, and even be arrested for crimes that they did not commit.

With almost all of your personal information stored electronically somewhere it has become essential that we all learn how to protect that information. However, even if you are careful with your personal data identity thieves can still find ways to access your information. They can steal your information from other institutions by stealing records or information while they are on the job, bribing employees to give them your information, hacking into their records, and/or conning information out of employees. They may also look through your mail for bank statements, new checks, credit card statements, or credit card applications. More and more identity thieves attempt to steal your personal through email, phone calls, or phishing where they impersonate a legitimate company or institution.

Once they have your information they can use it in a number of ways. They could change the billing address on your credit cards and then run up charges on your account or they could open a new credit card in your name and all of the unpaid bills will then be filed on your credit report and since you will not be able to monitor the billing you may not find out for some time. They may also try to counterfeit checks or open a new account in your name and write bad checks. They may be able to create wireless or phone services, buy a car, apply for loans, or file fraudulent tax returns all in your name. They could even go as far as to give your name to the police if they are charged with a crime and if they fail to show up in court a warrant will be put out for your arrest.

There are many precautions that you can take to try to prevent your identity from being stolen but sometimes there is nothing that you can do to prevent it. It can be a very frustrating, angering, and time consuming ordeal when you are a victim of identity theft. That is why the Federal Trade Commission (FTC), with the help of other government agencies, has been working on ways to help victims of identity theft in order to relieve some of the stress that they may be having.

If you have had your **financial account** information stolen then you should close your credit cards and bank accounts immediately. When you open new accounts be sure to put passwords on them and make sure that the passwords cannot be guessed. If your **social security** number has been stolen there is a toll-free fraud number of any three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. Early action will prevent someone from opening new accounts in your name. If they steal your



driver's license or other identification contact the agency that issued the ID and cancel the documents and get them renewed.

Tips:

- **Monitor your accounts regularly**
 - Check your credit report at least once a year and make sure that there haven't been any unusual or fraudulent charges made.
- **Be very careful when provide your information online.**
 - Legitimate companies will not send unsolicited requests for personal information.
 - Make sure that you only give information of this type to a trusted business.
- **Don't respond to unsolicited emails, links with emails, or pop-up ads**
 - Identity thieves use spam, spyware, adware, pharming, and/or phishing techniques in order to acquire information from potential victims.
- **Shred all documents that you plan to throw away**
 - These documents include bank statements, pre-approved credit card offers, utility bills, and any other documentation with your social security or account numbers.
- **Try not to keep too many credit cards if you don't use them regularly**
 - It is more difficult to monitor your accounts if you have numerous credit card accounts that you are not using.
- **Protect and store personal information at home**
 - Make sure that you store your person data and files in a safe place that is inaccessible to visitors.
- **Protect your mail**
 - Send your bills, checks, or other personal correspondence from a secure location like your local post office.
 - Install a locking mailbox at your residence. Identity thieves often obtain the information they need by intercepting mail in unlocked street mailboxes.
- **Beware of "shoulder surfers."**
 - Make sure that when you are filling out forms or inputting passwords that no one is looking over your shoulder.
- **Place a fraud alert on your credit.**



- This is the first line of defense if feel that you have had any of your personal information stolen. Contact each of the bureaus for assistance.

