2010 Guide for Home Computer Security

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

DISCLAIMER

This Guide for Home Computer Security by Bob Mahan is brought to you by the Unclassified Computer Security Program at the Pacific Northwest National Laboratory (www.pnl.gov). For questions or comments, contact us via e-mail at ucs@pnl.gov.

For additional copies of this guide, see:
http://www.pnl.gov/main/links.html#computer.

CONTENTS

Overview iii

Internet Connections 1

Risks 1

Risk Reduction 2

Resources 11

Glossary 13

Levels of Computer Protection 17

OVERVIEW

Note: Glossary terms are indicated by **copper, bolded font** and can be found at the end of the guide.

This guide provides information to help you protect your home computer from attacks and other events that can harm your system or the information stored on it.

If you use a computer at home, have access to the Internet, and haven't been living under a rock, you are likely aware of the threat posed by **viruses**, **worms**, and **hackers**. However, being aware of the threat isn't much help if you can't take action to neutralize it. Take heart: there are steps you can take to reduce the probability that an attack will be successful.

Four conditions are required to carry out a successful attack, whether it comes from a virus, worm, or hacker:

1. First, there must be a threat. We already know that threats are real. Viruses, worms, and hackers are all threats we have read about or experienced.
2. Second, your computer must be vulnerable to the threat. As it turns out, all computer systems contain vulnerabilities. One of the most significant vulnerabilities is the user. Every time you download and execute software or open an e-mail attachment, you are taking the risk of downloading a malicious program. Vulnerabilities are also software flaws in your computer that weaken its security.

3. Third, there must be an attempt to **exploit** the vulnerability. An *exploit* is an attack that uses the vulnerability to enter and compromise your system. Exploits can be simple or complex. An example of a simple exploit is sending a virus attached to an e-mail message. If you open the attachment, your computer might be infected.
4. Finally, your computer must be targeted and an attempt made to exploit the vulnerability in order to compromise your computer. This is typically a matter of probabilities. The longer your computer is exposed to the Internet, the greater the probability that someone or something (e.g., a virus) will target your computer and attempt to exploit it.

The bad news is you cannot completely eliminate the risk of your computer being compromised. There is no such thing as perfect computer security. The good news is you can significantly reduce the probability that your system will be compromised.

INTERNET CONNECTIONS

Internet connections provide the principal conduit for attacks to reach your computer. Internet connections are available in two main classes, low-speed dial-up and highspeed access. Many home computer users connect to the Internet using a **modem** that calls a server over your home telephone line. The **server** is provided by an Internet Service Provider (ISP) such as One-World Telecommunications or America Online. Once connected, you use the server's capabilities to browse the Internet.

Currently, high-speed access is common in many areas. High-speed access includes:

» Cable modem access from a local cable television service provider

» **Digital subscriber lines** (DSL) from a telephone company

» Wireless access from a wireless service provider

» Satellite

These high-speed services are often referred to as *always-on connections* because they are available all the time. High-speed access offers several benefits:

» Web pages load and display faster, typically 5-25 times faster. This is very apparent when downloading software updates, images, or other large files.

» Except when the service is down for maintenance, the connection is always available. There are no telephone numbers to dial and no busy signals.

» The connection doesn't block your telephone. Cable, satellite, and wireless connections are separate from your telephone. DSL shares your telephone line between voice calls and Internet service without conflict.

Risks

Anytime you are online, your system can be infected by a **virus** or **worm**, unknowingly exposed to a malicious web site, or directly attacked by a **hacker**. Viruses are typically acquired by some action you take such as loading an infected floppy disk or CD or opening an e-mail attachment that has been infected. Worms are more insidious. Worms do not require you to take any action. They can propagate over a network without assistance, arriving silently and infecting your system. Both worms and hackers target your system by using your system's Internet address.

When you connect to the Internet, you are identified by an Internet address, a string of numbers that uniquely identify your connection.

For dial-up connections, a different assignment is made every time you log on to your ISP. Because your address is only valid while you are online, the risk of being attacked by a hacker is small but not zero (that is, as long as you are online, you could be attacked).

The situation is different for high-speed access. Your Internet address is unchanged over a longer period of time (days or weeks) rather than changing with every access. Also, your computer is always connected to the Internet unless you turn it off or disconnect the access device (e.g., the cable **modem**). If the computer is on and connected, then it can be exposed to an attack because **hackers** continually scan the Internet for addresses to attack. Hackers also tend to prefer breaking into computers that have a highspeed Internet connection. For example, a Pacific Northwest National Laboratory staff member with a new high-speed service installed a BlackICE **firewall** on his home computer and left it powered up overnight. Over 50 attempts an hour were made to access and exploit his computer. This level of activity is not unusual for a system using high-speed access. Fortunately, none of the attacks were successful.

Risk Reduction

You can take several actions to significantly reduce the risk of acquiring malicious code or having your system compromised if it is attacked.

1. **Use anti-virus and anti-malware software**. Anti-virus (AV) software scans for the presence of worms and viruses. It can scan system memory and disk files and be configured to automatically scan any file your system attempts to open. This is particularly useful for e-mail attachments. If a virus is detected, the AV software either quarantines or removes the offending program. AV software uses a database of known virus signatures to detect offending software. Be sure to configure the AV software to examine all files before they are opened. Popular AV programs include Symantec's Norton AntiVirus [http://www.symantec.com/] and McAfee [http://www.mcafee.com/]. Many antivirus programs include

malware removal software, but not all. Make sure your antivirus software checks for spyware, adware and rootkit. If it does not then consider getting malware removal software.

2. **Regularly update AV signatures**. Because new virus strains are continually being developed and released, the signature (also called *definitions*) file must be kept up to date. Most AV signatures can be updated online from the vendor's web site. You should set your antivirus software to automatically update **virus signatures** (preferred) or visit the site regularly to obtain the latest signature file.
3. **Install and use a firewall**. A **firewall** restricts access to your system from the Internet. It can be used to restrict in-bound access, out-bound access, or both. It allows you to specify what is and isn't permissible. Firewalls can be implemented in software or hardware. Software firewalls are installed on your computer. Newer operating systems include an embedded firewall, and inexpensive software firewalls (e.g., BlackICE [blackice.iss.net/] and ZoneAlarm [www.zonelabs.com]) are available for older operating systems. Hardware firewalls are connected between your computer's network access port and the high-speed access modem (e.g., cable or DSL modem). Hardware firewalls are available from several vendors for under $100. Typically, these devices also serve as **routers** that allow you to connect multiple home computers to the Internet.
4. **Protect wireless connections**. You need to take special care to protect wireless connections to keep outsiders from hijacking your Internet connection or invading your system. Carefully read and follow the security instructions that came with your wireless **access point** configuration guide. The following steps are highly recommended:
   - » For access points with **firewall** capabilities, enable the firewall.
   - » Many people believe that disabling broadcast of the SSID can increase security. The opposite is actually true. Disabling broadcast of the SSID requires the access point to keep in constant contact with the clients and send the SSID info on a regular basis. This opens the access point to more easily cracking of the encryption key. Besides making your network less secure it

also makes it more difficult to add computers and keep them connected.

- Change the default password used to manage the access point. The password is widely known, and anyone who gains access to the wireless network could then change the configuration of the access points and any firewall capability it has.
- Do not bother with MAC address filtering. MAC address filtering is completely ineffective as a security measure. Anyone can download freely available MAC addressing spoofing software and even some commercially available access points or NICs come with spoofing software for non-nefarious reasons.
- Enable **encryption** for the wireless link. Older access points will support **WEP** encryption only this is not an effective solution and updating your access point should be a priority. Newer devices will support **WPA and WPA2**. If only WEP is available, set it for 128-bit encryption. WPA is the minimum preferred method and WPA2 is the most desirable. In each case, you will enter a key or a **passphrase** in the access point and each computer that uses the wireless connection. Use complex values that are as long as permitted. Write them down on paper and store them in a secure location. Keep in mind that all access points will support WEP, but not all support TKIP and/or AES. If you are purchasing an access point, take care to ensure it supports WPA and WPA2.
- Change the default name for your wireless network. Do not use personally identifiable information in your network name.
- Disable remote management of your access point if enabled.
- Change the SSID and key values/passphrases on a regular schedule such as every few months. It is a good idea to write yourself instructions on how to do this as you are likely to forget the steps between changes.

If these instructions sound intimidating, it is because they are. The good news is that most wireless device manufacturers provide explicit instructions on how to perform each of these actions. It may be helpful for you to visit the web sites for devices you are considering and read their instruction manuals as most are available online.

5. **Practice safe e-mail and web surfing habits**. Most, but not all, **virus** infections are transmitted by e-mail. A virus often arrives as an attachment forwarded by a friend or acquaintance, but it could come from any source. Don't depend completely on

your AV software. New virus and **worm** programs are developed and released all the time. Your AV signature file might not have a signature for a new viral strain. If you receive suspicious e-mail, even from someone you know, do not open it—delete it immediately.

Phishing (pronounced fishing) is a scam where a perpetrator sends you an e-mail request appearing to come from an Internet site you trust or do business with, like AOL, your bank, PayPal, eBay, etc. The phisher may use any number of several **social engineering**, e-mail and web site **spoofing** ploys to trick you into revealing private information. You may be asked to update your account information and be provided a link to a web site. When you click the link, you go to a site that, for example, appears to be the eBay site. The bogus site then takes you through an update process where you enter your private information such as passwords, account numbers, credit card numbers, etc. Trouble is, the site does not belong to eBay. It is a clever duplicate operated for the sole purpose of obtaining your information so your real account can be ransacked or your identity stolen. To be safe, do not respond to these kinds of inquiries by following a link provided in an e-mail or chat session. Do not disclose private information unless you initiated the connection yourself.

Also, as you surf the web, it is possible for a web **server** to silently download malicious code to your computer. For example, web servers often deliver web pages with hidden code that is executed when you download the page. In most instances, the code provides a useful function (e.g., an animated display). However, the hidden code in some pages is malicious and could be used to compromise your system. While you cannot always know whether a web site is the host for malicious activity, you should be careful in selecting sites to visit.

6. **Regularly install updates and patches**. All software has vulnerabilities that can be exploited. As vulnerabilities are discovered, exploits are written and often published on the Internet for anyone to use. Manufacturers regularly issue software updates so your system cannot be exploited by a particular vulnerability. These updates are made available for distribution to users free of charge. In some cases, automated

tools such as Windows Update are available to notify users of the availability of updates for downloading and automatic installation. In other cases, you need to locate and visit the vendor's web site to acquire the updates.

Keeping your operating system, applications, and your **virus signatures** or definitions updated is by far the most effective way you have of defending against attacks and infections. Well over 90% of all successful break-ins are the result of exploiting well-known vulnerabilities that could have been fixed with a simple update.

In the past, updating a system was not for the faint of heart or less than expert user. It was difficult enough just to find updates much less understand whether you needed one or know how to install it. As indicated above, newer operating systems are becoming much more effective at making this process relatively easy for the average user. It is highly recommended that you use this capability even if it means upgrading your operating system. You can find updates to Microsoft Windows and other Microsoft products at **http://update.microsoft.com** or, for Apple Macintosh systems, run the Software Update Apple menu item.

7. **Create and Use Passwords Wisely**. You probably will construct various passwords to access your home computer and various sites you visit (e.g., your bank, credit union, investment plans, etc.). When you construct these passwords, make them difficult to guess and/or break—the more complex the better. Contrary to what you may have been told, writing down your password can be a good idea. When you know you have a written copy to verify against you are more likely to make a complex and long password. Just make sure you store your password in a safe place, preferable in a different room (not under the keyboard).

8. **Back Up Your Computer**. At a minimum, you should make regular **backup** copies of any important information you store on your computer. There are many ways to do backups, including using **CD-RW** drives. With the cost of large disk storage coming down, you may want to consider a second hard drive large enough to back up your entire system or just the important files. USB removable **flash drives** are another option. Also, if you haven't created an **emergency disk** for your system, do it immediately. This disk can get you out of a scrape if your system will not boot up—it is an essential part of your toolkit.

9. **Turn Off Features You Don't Need**. Computers are delivered with so-called default settings. There are various settings from display colors to

security protection. In the past, most computers were delivered with a default security setting of "NONE" and with services like printer-sharing turned on. At least part of the reason for this was to make setting up the computer as easy as possible for the user and to provide all the services a user would likely ever need. Some of these services are inviting to **hackers** and used in common **exploits**. Turn off, for example, file- and print-sharing unless you know what you are doing or are behind a **firewall**. Fortunately, vendors are now setting defaults to stronger security and building systems with better protection. This is another reason to upgrade your operating system.

10. **Avoid Inherently Unsafe Software and Services**. Certain software and services are very appealing to the home user. **Freeware**, instant messaging, and music download software come to mind as products or services that are widely used on home computers.

    Freeware sometimes is great software and sometimes it isn't. Some freeware comes bundled with **Adware** or **Spyware** that tracks the user through cyberspace and reports back to an Internet site all of your surfing habits. You can determine whether your system has any of this software, typically loaded without your knowledge, by visiting http://www.lavasoftusa.com and downloading the free

software package called Ad-aware. A similar product, SpyBot Search & Destroy, is also freely available at http://www.safer-networking.org. Both packages will scan your system for the presence of Adware and Spyware and report it to you. They will offer to remove or mark the offending software so it does not affect your system.

Instant messaging is often misused because it may open up your system to the person you are talking to. Either you should disable it or you should be careful that you only use it to communicate with people you know and trust.

Both instant messaging and many of the popular music services are a form of software called **peer-to-peer** software. There are many file download services, including KaZaA, Morpheus, and BearShare. In each case, you download and install a program on your computer. If you download the software, be sure you understand that you have little or no control over what it does. One of these packages has been widely verified to include another software package that can take over

the operation of your computer and use it for other purposes. This means that it is a **Trojan horse** program: a program that appears to perform a legitimate function but may also perform undesirable functions unknown to the user.

One other caveat. **Distributed file services**, like KaZaA, cause your computer to become a **server** and permit access from the Internet to your computer by other participants in that file-sharing network. Depending on the service, you may be able to opt out of becoming a server. If you are not given the choice or you do not opt out, you may be providing access to your system from the Internet and assuming all the associated risk. You can also end up violating music copyrights without realizing it.

Peer-to-peer software is a very appealing technology and has great potential for useful and productive applications. However, in its current state of development, it is dangerous, because of the lack of any protection on your system. Most peer-to-peer technology has no security protection and requires no authentication to identify peers in a way that can keep out the bad guys. As we have indicated, you need to be careful and prudent if and when you use this type of software.

11. **Don't store critical information on your computer**. If your computer is compromised, the entire contents of the system are exposed to the attacker. It is then easy to search for and harvest passwords, encryption keys, credit card numbers, social security numbers, or other private information. The best bet is to never store critical information on your computer.

    If you keep financial records or other personal information on your home computer, you should store the files either offline (e.g., on a **CD-RW** or **removable flash drive**) or online in encrypted form. Recent operating systems generally are delivered with strong encryption capabilities so you can protect important files. This capability provides yet another reason to upgrade.

12. **Use caution when shopping on the Internet**. Online shopping is becoming increasingly popular, but it carries its own risks as well because you need to provide credit card information to complete a transaction. To keep this out of the wrong hands, you should ensure that your browser is enabled to check certificates and notify you if a certificate is invalid. A certificate is a document

that contains the identity of the merchant and an encryption key that can be used to secure your transaction. The certificate is issued by a third party and is presented to your browser by the merchant. Your browser contacts the third party to request validation. The third party replies with a valid or invalid message. If you have set your browser to notify you of invalid results (see the browser help file for how to do this), you can either accept the certificate (not recommended) or stop shopping (recommended). In addition, many sites will offer to remember your credit card information. It is your call, but if you accept, it will be stored on a server operated by, or on behalf of, the merchant. If that server is compromised, your credit card number could be revealed.

13. **Treat social networking sites like you would email**. Social networking sites like Facebook can open you to many of the same risks that email does. Never click on links sent to you through these sights. Social networking sites also open you to other risks you may not even consider. Recently, a popular social networking site changed its EULA to give it indefite rights to anything you upload to it. Furthermore, they did it without having to notify users because the initial EULA stated it could change the EULA at any time without notice. A watchdog group discovered this change and blew the whistle on the site. There was such an outcry that site owners changed the EULA back.

14. **When all else fails**. If you suspect you have been the victim of an online scam, you should contact the Internet Fraud Complaint Center (IFCC) immediately and file an online complaint at http://www.ifccfbi.gov/, and/or forward the suspicious e-mail to the Federal Trade Commission (FTC) at uce@ftc.gov, or call the FTC help line at 1-877-382-4357.

RESOURCES

We hope you found this guide useful and will put all or at least some of the recommendations into practice. If you need more information, some excellent sources on the web are listed below:

Cable Modem/DSL Tuning Guide

cable-dsl.home.att.net/#security. Sponsored by AT&T, this site provides step-by-step advice on securely configuring Windows and Macintosh systems for safe computing. It also discusses home firewalls, Internet privacy, content filtering for children, tuning your system for high-performance Internet access, and a host of other technical and non-technical subjects. The site is highly recommended reading for anyone who accesses the Internet from home.

Home Network Security

www.cert.org/tech_tips/home_networks.html. This site belongs to the Computer Emergency Response Team (CERT) at Carnegie-Mellon University. It is a somewhat more comprehensive guide than the one above on protecting your home computer.

Macintosh Security

www.securemac.com. This site contains lots of security tips and tools for Macintosh computers.

Microsoft Security

www.microsoft.com/security/. This site contains the latest security advisories and patches for Windows and other Microsoft products.

Resources in This Guide

- **Symantec Antivirus**: http://www.symantec.com/
- **McAfee Antivirus**: http://www.mcafee.com/
- **Ad-aware**: http://www.lavasoftusa.com/
- **SpyBot Search & Destroy**: http://www.safer-networking.org
- **Zone Alarm**: http://www.zonelabs.com/
- **BlackIce**: http://www.blackice.iss.net/
- **Internet Fraud Complaint Center**: http://www.ifccfbi.gov/
- **Windows Updates**: http://windowsupdate.microsoft.com

GLOSSARY

Access Point A hardware device that acts as a communication hub for users of a wireless device to connect to a wired local area network.

Adware Software that collects information about a user in order to display advertisements in the user's browser based on the user's web browsing habits. It is a type of **Spyware**.

AES Advanced Encryption Standard is the latest in the standards and supports 128, 192 and 256-bit keys and encryption blocks and may be extended in multiples of 32 bits. See **WEP** and **TKIP**.

Backup A copy of files on a second medium (such as disk or tape) in case the first medium (e.g., the computer hard drive) fails, becomes corrupt, or is destroyed. Many experts recommend making two or even three backups and keeping one backup in a different location from the others.

CD-RW Short for ***CD-ReWritable disk***, a type of compact disk that enables you to write onto it in multiple sessions. One problem with CD-R disks is that you can only write to them once. With CD-RW drives and disks, you can treat them just like a floppy or hard disk, writing data onto it multiple times.

Certificate An attachment to an electronic message used for security purposes. The most common use of a certificate is to verify that a user sending a message is who he or she claims to be and to provide the receiver with the means to encode a reply.

Digital Subscriber Line A generic name for digital lines that are provided by telephone companies to their local subscribers and that carry data at high speeds.

Distributed file service An application that allows users to access and process data stored on a server as if it were on their own computer.

Emergency disk Also called **Rescue disk**. This disk contains a backup of your computer's essential files so that you can recover from a virus attack or other computer failure. When you install anti-virus software, you are usually prompted to create this disk and are taken through the steps to do so.

Encryption The process of changing data and text to scrambled (encoded) data and text, and vice versa.

Exploit An attack that takes advantage of a computer vulnerability to enter and compromise the computer system.

Firewall A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

Flash drive A small, removable data storage device. It is also known by numerous other terms, such as a keydrive, keychain drive, pen drive, jump drive, and thumb drive.

Freeware Copyrighted software given away for free by the author. The author retains the copyright, which means that you cannot do anything with the software that is not expressly allowed by the author.

Hacker A slang term for a computer expert. Although the term can be complimentary or derogatory, the derogatory sense (meaning someone who illegally accesses computer systems) has become more common.

MAC address A media access control (MAC) address identifies a unique computer and is provided by a network interface card (NIC), the component that allows a computer to connect to a network.

Media Tapes or disks used to store backup files.

Modem A device that enables a computer to transmit data, usually over a telephone or cable line.

Passphrase A Passphrase serves the same function as a password. It is generally longer than a password and may include words, letters, numbers, and special characters.

Patch A piece of software code that fixes an error or bug in an application or operating system.

Peer-to-Peer A type of network that allows a group of computer users with the same networking program to connect with each other and directly access files on one another's hard drives.

Phishing The act of sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to trick the user into providing private information. The e-mail provides a link to a phony web site that looks legitimate. The user is asked to update personal information, such as passwords and credit card, social security, and bank account numbers, which can then be used for identity theft.

Router A device that forwards information along networks.

Server A computer or device that manages network resources. A network server is one that manages network traffic.

Service Set Identifier (SSID) A sequence of characters that uniquely names a wireless local area network (WLAN). This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.

Social engineering The act of conning an individual into revealing secure information. Social engineering is successful because people want to trust other people and are naturally helpful. The victims do not realize the information will be used maliciously (e.g., to attack a computer network).

Spam Electronic junk mail.

Spoofing Forgery of an e-mail so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing to try to get recipients to open and respond to their solicitations.

Spyware Software that, unknown to the user, monitors a user's activity on the Internet and transmits that information to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

TKIP Temporal Key Integrity Protocol is a "wrapper" that goes around the existing **WEP** encryption. Although TKIP uses the same encryption engine and algorithm defined for WEP, the key used for encryption is 128 bits long, solving the problem of a too-short key length. Also see **AES**.

Trojan horse A destructive program that appears to be harmless. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One type of Trojan horse claims to rid your computer of viruses but actually infects your computer with viruses.

Virus signature A unique string of virus code. The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses. Anti-virus software uses the virus signature to scan for the presence of malicious code.

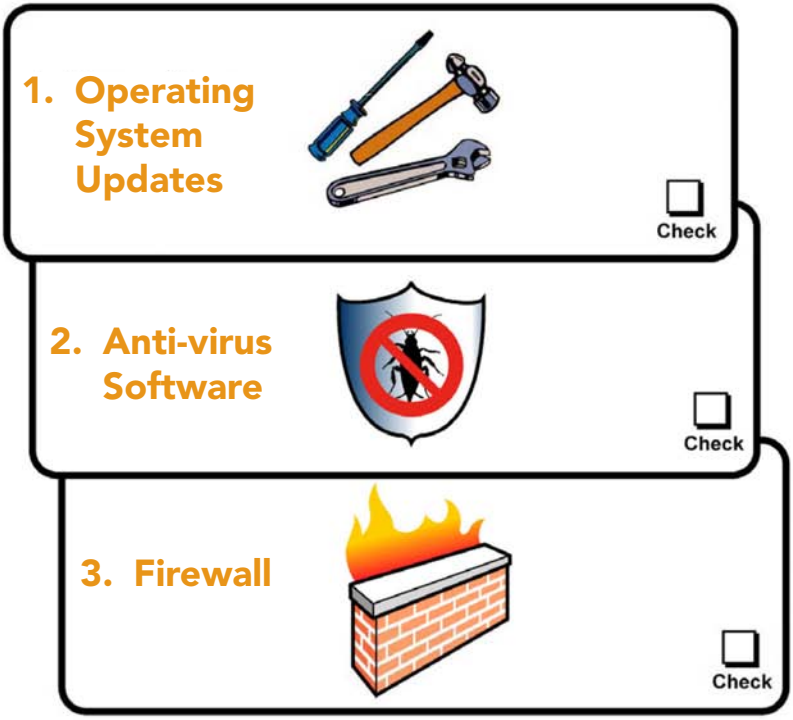
Virus A program that is loaded onto your computer without your knowledge and runs against your wishes. A simple virus can make a copy of itself over and over again. Even such a simple virus is dangerous because it will quickly use all available memory and bring the computer to a halt.

WEP Wired Equivalent Privacy is a security protocol for wireless local area networks. WEP is designed to provide the same level of security as that of a wired network.

Worm A program that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and shutting down the system.

The next page contains an overview of protection methods that you can post near your computer.

LEVELS OF COMPUTER PROTECTION



Do on Regular Schedule

- Update anti-virus & OS software often
- Back up data
- Store critical data offline
- Don't open suspicious e-mail
- Use good passwords

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*