Guide for Home Computer Security

By Bob Mahan

This guide 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.

Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

unclassified CS

December 2003

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

Overview

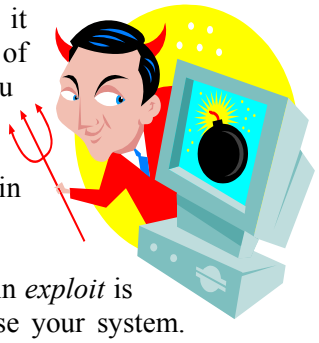
This guide provides information to help you protect your home computer from attacks and other events that can harm your system or the information stored on it.

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.

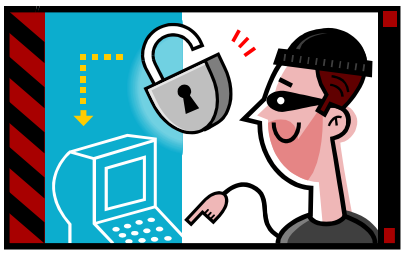
2. Second, your computer must be vulnerable to the threat. As it turns out, all computer systems contain vulnerabilities. One of the most significant vulnerabilities is the user. Every time you download and execute software or open an e-mail attachment, you are taking the risk of downloading a malicious 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 high-speed 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.

More recently, high-speed access has become available in many areas, including the Tri-Cities. 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:

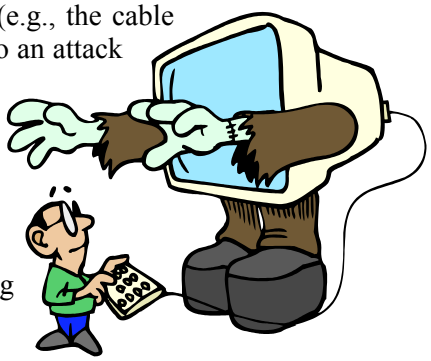
- Web pages load and display faster. This is very apparent when downloading software updates, images, or other large files.
- Except when the service is down for maintenance, the connection is always available. There are no telephone numbers to dial and no busy signals.
- The connection doesn't block 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 disk 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 high-speed 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 software.** Anti-virus (AV) software scans for the presence of malicious software. 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 McAffee [http://www.mcaffee.com/].

2. **Regularly update AV signatures**. Because new virus strains are continually being developed and released, the signature file must be kept up to date. Most AV signatures can be updated online from the vendor's web site. You should set your anti-virus software to automatically update virus signatures (preferred) or visit the site regularly to obtain the latest signature file.

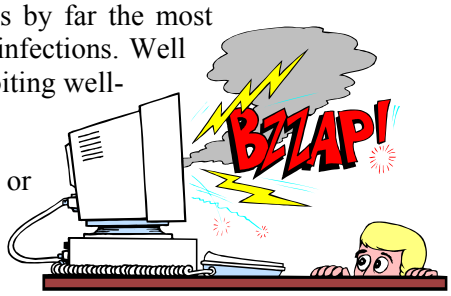
3. **Install and use a firewall**. A firewall restricts access to your system from the Internet. It can be used to restrict in-bound access, out-bound access, or both. It allows you to specify what is and isn't permissible. Firewalls can be implemented in software or hardware. Software firewalls are installed on your computer. Newer operating systems include an imbedded 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. **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.

   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.

5. **Regularly update 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 patches so your system cannot be exploited by a particular vulnerability. These patches are made available for distribution to users free of charge. In some cases, automated tools are available to notify users of the availability of patches for downloading and automatic installation. In other cases, you need to locate and visit the vendor's web site to acquire the patches.

   Keeping the patches and your virus signatures 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 patched.



   In the past, patching a system was not for the faint of heart or less than expert user. It was difficult enough just to find patches 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.

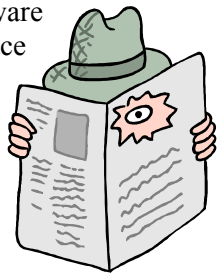
6. **Create and Use Passwords Wisely**. You probably will construct various passwords to access your home computer and various sites you visit (e.g., your bank, credit union, investment plans, etc.). When you construct these passwords, make them difficult to guess and/or break—the more complex the better. Trouble is, you won't be able to remember them very well if they are too complex. Consequently, you will be tempted to write them down or store them on your computer or have the remote system remember them so they don't have to be re-entered. None of these practices is a good idea, especially when you are protecting private information that can result in unacceptable damage to you socially or financially if the information is disclosed. Therefore, passwords must be protected.

7. **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-R/W drives and tapes. With the cost of large disk storage coming down, you may want to consider a second hard drive large enough to backup your entire system or just the important files. USB ThumbDrives® are another option. 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.

8. **Turn Off Features You Don't Need.** Computers are delivered with so-called default settings. These are various settings for everything 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 machine 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.

9. **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 www.lavasoftusa.com and downloading the free software package called Ad-aware. It will scan your system for the presence of Adware and Spyware and report it to you. It will offer to remove the offending software from your system.



   Instant messaging is often misused because it opens up your system to the person you are talking to. It should either be disabled or you should be careful that you only use it to communicate with people you know and trust.

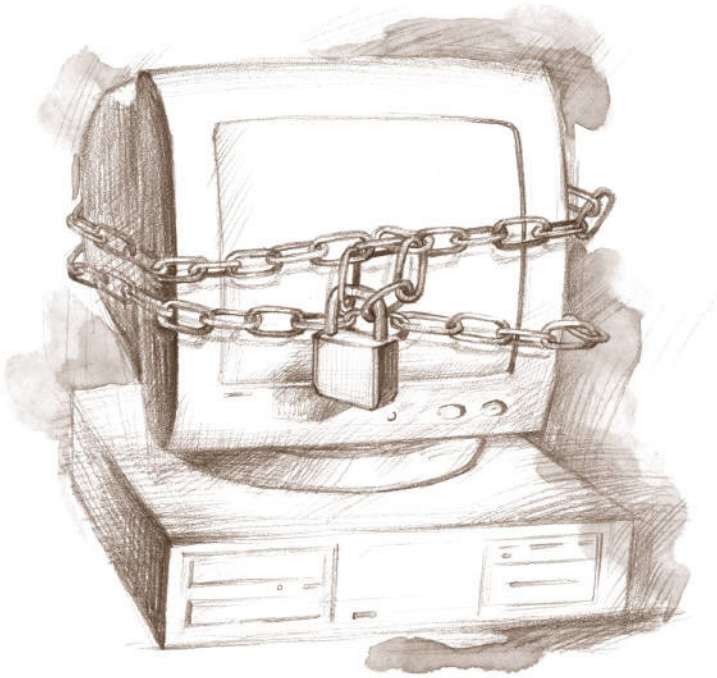
   Both instant messaging and many of the popular music services are a form of software called peer-to-peer software. There are many file download services, including KaZaA, Morpheus, and BearShare. In each case, you download and install a program on your computer. If you download the software, be sure 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.

10. **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 the system.

    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 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.



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.

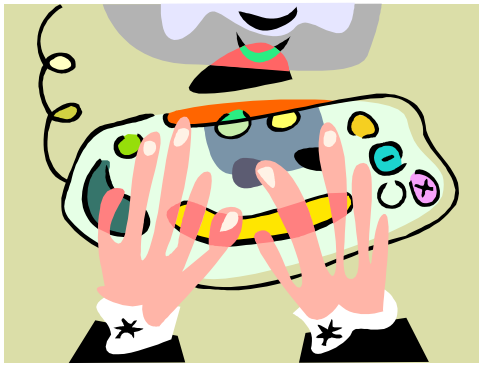
Macintosh Security
www.securemac.com. This site contains lots of security tips and tools for Macintosh computers.

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:

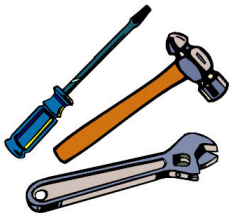
- **Symantec Antivirus:** www.symantec.com
- **McAffee Antivirus:** www.mcaffee.com
- **Ad-aware:** http://www.lavasoftusa.com/
- **Zone Alarm:** http://www.zonelabs.com/
- **BlackIce:** http://www.blackice.iss.net/

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



Levels of Computer Protection

1. Operating System Updates

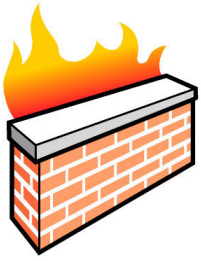


Check

2. Anti-virus Software

Check

3. Firewall



Check

To the Internet

Do on a Regular Schedule

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

Guide for Home Computer Security Developed at
Pacific Northwest National Laboratory