2001 CERT Tech Tip: Home Network Security

Original publication date: June 22, 2001

This document gives home users an overview of the security risks and countermeasures associated with Internet connectivity, especially in the context of always-on or broadband access services (such as cable modems and DSL). However, much of the content is also relevant to traditional dial-up users (users who connect to the Internet using a modem).

---

1. Computer security
    a. What is computer security?

        Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

    a. Why should I care about computer security?

We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs. Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer (such as financial statements).

a. Who would want to break into my computer at home?

   Intruders (also referred to as hackers, attackers, or crackers) may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.

   Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems. Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target.

   Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.

a. How easy is it to break into my computer?

   Unfortunately, intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

   When holes are discovered, computer vendors will usually develop patches to address the problem(s). However, it is up to you, the user, to obtain and install the patches, or correctly configure the software to operate more securely. Most of the incident reports of computer break-ins received at the CERT/CC could have been prevented if system administrators and users kept their computers up-to-date with patches and security fixes.

   Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure. Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

1. Technology

   This section provides a basic introduction to the technologies that underlie the Internet. It was written with the novice end-user in mind and is not intended to be a comprehensive survey of all Internet-based technologies. Subsections provide a short overview of each topic. This section is a basic primer on the relevant technologies. For those who desire a deeper understanding of the concepts covered here, we include links to additional information.

   a. What does broadband mean?

      "Broadband" is the general term used to refer to high-speed network connections. In this context, Internet connections via cable modem and Digital Subscriber Line (DSL) are frequently referred to as broadband Internet connections. "Bandwidth" is the term used to describe the relative speed of a network connection -- for example, most current dial-up modems can support a bandwidth of 56 kbps (thousand bits per second). There is no set bandwidth threshold required for a connection to be referred to as "broadband", but it is typical for connections in excess of 1 Megabit per second (Mbps) to be so named.

   a. What is cable modem access?

      A cable modem allows a single computer (or network of computers) to connect to the Internet via the cable TV network. The cable modem usually has an Ethernet LAN (Local Area Network) connection to the computer, and is capable of speeds in excess of 5 Mbps.

      Typical speeds tend to be lower than the maximum, however, since cable providers turn entire neighborhoods into LANs which share the same bandwidth. Because of this "shared-medium" topology, cable modem users may experience somewhat slower network access during periods of peak demand, and may be more susceptible to risks such as packet sniffing and unprotected windows shares than users with other types of connectivity. (See the "Computer security risks to home users" section of this document.)

   a. What is DSL access?

      Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. Also, the "dedicated bandwidth" is only dedicated between your home and the DSL provider's central office -- the providers offer little or no guarantee of bandwidth all the way across the Internet.

      DSL access is not as susceptible to packet sniffing as cable modem access, but many of the other security risks we'll cover apply to both DSL and cable modem access. (See the "Computer security risks to home users" section of this document.)

   a. How are broadband services different from traditional dial-up services?

      Traditional dial-up Internet services are sometimes referred to as "dial-on-demand" services. That is, your computer only connects to the Internet when it has something to send, such as email or a request to load a web page. Once there is no more data to be sent, or after a certain amount of idle time, the computer disconnects the call. Also, in most cases each call connects to a pool of modems at the ISP, and since the modem IP addresses are dynamically assigned, your computer is usually assigned a different IP address on each call. As a result, it is more difficult (not impossible, just difficult) for an attacker to take advantage of vulnerable network services to take control of your computer.

      Broadband services are referred to as "always-on" services because there is no call setup when your computer has something to send. The computer is always on the network, ready to send or receive data through its network interface card (NIC). Since the connection is always up, your computers IP address will change less frequently (if at all), thus making it more of a fixed target for attack.

Whats more, many broadband service providers use well-known IP addresses for home users. So while an attacker may not be able to single out your specific computer as belonging to you, they may at least be able to know that your service providers broadband customers are within a certain address range, thereby making your computer a more likely target than it might have been otherwise.

The table below shows a brief comparison of traditional dial-up and broadband services.

	Dial-up	**Broadband**
Connection type	Dial on demand	Always on
IP address	Changes on each call	Static or infrequently changing
Relative connection speed	Low	High
Remote control potential	Computer must be dialed in to control remotely	Computer is always connected, so remote control can occur anytime
ISP-provided security	Little or none	Little or none

Table 1: Comparison of Dial-up and Broadband Services

a. How is broadband access different from the network I use at work?

Corporate and government networks are typically protected by many layers of security, ranging from network firewalls to encryption. In addition, they usually have support staff who maintain the security and availability of these network connections.

Although your ISP is responsible for maintaining the services they provide to you, you probably wont have dedicated staff on hand to manage and operate your home network. You are ultimately responsible for your own computers. As a result, it is up to you to take reasonable precautions to secure your computers from accidental or intentional misuse.

a. What is a protocol?

A protocol is a well-defined specification that allows computers to communicate across a network. In a way, protocols define the "grammar" that computers can use to "talk" to each other.

a. What is IP?

IP stands for "Internet Protocol". It can be thought of as the common language of computers on the Internet. There are a number of detailed descriptions of IP given elsewhere, so we won't cover it in detail in this document. However, it is important to know a few things about IP in order to understand how to secure your computer. Here well cover IP addresses, static vs. dynamic addressing, NAT, and TCP and UDP Ports.

An overview of TCP/IP can be found in the TCP/IP Frequently Asked Questions (FAQ) at

http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/

and

http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part2/

a. What is an IP address?

IP addresses are analogous to telephone numbers when you want to call someone on the telephone, you must first know their telephone number. Similarly, when a computer on the Internet needs to send data to another computer, it must first know its IP address. IP addresses are typically shown as four numbers separated by decimal points, or dots. For example, 10.24.254.3 and 192.168.62.231 are IP addresses.

If you need to make a telephone call but you only know the persons name, you can look them up in the telephone directory (or call directory services) to get their telephone number. On the Internet, that directory is called the Domain Name System, or DNS for short. If you know the name of a server, say www.cert.org, and you type this into your web browser, your computer will then go ask its DNS server what the numeric IP address is that is associated with that name.

Every computer on the Internet has an IP address associated with it that uniquely identifies it. However, that address may change over time, especially if the computer is

- dialing into an Internet Service Provider (ISP)
- connected behind a network firewall
- connected to a broadband service using dynamic IP addressing.

a. What are static and dynamic addressing?

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time. However, if a static address is assigned but not in use, it is effectively wasted. Since ISPs have a limited number of addresses allocated to them, they sometimes need to make more efficient use of their addresses.

Dynamic IP addressing allows the ISP to efficiently utilize their address space. Using dynamic IP addressing, the IP addresses of individual user computers may change over time. If a dynamic address is not in use, it can be automatically reassigned to another computer as needed.

a. What is NAT?

Network Address Translation (NAT) provides a way to hide the IP addresses of a private network from the Internet while still allowing computers on that network to access the Internet. NAT can be used in many different ways, but one method frequently used by home users is called "masquerading".

Using NAT masquerading, one or more devices on a LAN can be made to appear as a single IP address to the outside Internet. This allows for multiple computers in a home network to use a single cable modem or DSL connection without requiring the ISP to provide more than one IP address to the user. Using this method, the ISP-assigned IP address can be either static or dynamic. Most network firewalls support NAT masquerading.

a. What are TCP and UDP Ports?

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both protocols that use IP. Whereas IP allows two computers to talk to each other across the Internet, TCP and UDP allow individual applications (also known as "services") on those computers to talk to each other.

In the same way that a telephone number or physical mail box might be associated with more than one person, a computer might have multiple applications (e.g. email, file services, web services) running on the same IP address. Ports allow a computer to differentiate services such as email data from web data. A port is simply a number associated with each application that uniquely identifies that service on that computer. Both TCP and UDP use ports to identify services. Some common port numbers are 80 for web (HTTP), 25 for email (SMTP), and 53 for Dmain Name System (DNS).

a. What is a firewall?

The Firewalls FAQ (http://www.faqs.org/faqs/firewalls-faq/) defines a firewall as "a system or group of systems that enforces an access control policy between two networks." In the context of home networks, a firewall typically takes one of two forms:

- *Software firewall* - specialized software running on an individual computer, or
- *Network firewall* - a dedicated device designed to protect one or more computers.

Both types of firewall allow the user to define access policies for inbound connections to the computers they are protecting. Many also provide the ability to control what services (ports) the protected computers are able to access on the Internet (outbound access). Most firewalls intended for home use come with pre-configured security policies from which the user chooses, and some allow the user to customize these policies for their specific needs.

More information on firewalls can be found in the Additional resources section of this document.

a. What does antivirus software do?

There are a variety of antivirus software packages that operate in many different ways, depending on how the vendor chose to implement their software. What they have in common, though, is that they all look for patterns in the files or memory of your computer that indicate the possible presence of a known virus. Antivirus packages know what to look for through the use of virus profiles (sometimes called "signatures") provided by the vendor.

New viruses are discovered daily. The effectiveness of antivirus software is dependent on having the latest virus profiles installed on your computer so that it can look for recently discovered viruses. It is important to keep these profiles up to date.

1. Computer security risks to home users

a. What is at risk?

Information security is concerned with three main areas:

- Confidentiality - information should be available only to those who rightfully have access to it
- Integrity -- information should be modified only by those who are authorized to do so
- Availability -- information should be accessible to those who need it when they need it

These concepts apply to home Internet users just as much as they would to any corporate or government network. You probably wouldn't let a stranger look through your important documents. In the same way, you may want to keep the tasks you perform on your computer confidential, whether it's tracking your investments or sending email messages to family and friends. Also, you should have some assurance that the information you enter into your computer remains intact and is available when you need it.

Some security risks arise from the possibility of intentional misuse of your computer by intruders via the Internet. Others are risks that you would face even if you weren't connected to the Internet (e.g. hard disk failures, theft, power outages). The bad news is that you probably cannot plan for every possible risk. The good news is that you can take some simple steps to reduce the chance that you'll be affected by the most common threats -- and some of those steps help with both the intentional and accidental risks you're likely to face.

Before we get to what you can do to protect your computer or home network, lets take a closer look at some of these risks.

a. Intentional misuse of your computer

The most common methods used by intruders to gain control of home computers are briefly described below. More detailed information is available by reviewing the URLs listed in the References section below.

i. Trojan horse programs
ii. Back door and remote administration programs
iii. Denial of service
iv. Being an intermediary for another attack
v. Unprotected Windows shares
vi. Mobile code (Java, JavaScript, and ActiveX)

vii. Cross-site scripting
viii. Email spoofing
ix. Email-borne viruses
x. Hidden file extensions
xi. Chat clients
xii. Packet sniffing

i. Trojan horse programs

Trojan horse programs are a common way for intruders to trick you (sometimes referred to as "social engineering") into installing "back door" programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus. More information about Trojan horses can be found in the following document.

http://www.cert.org/advisories/CA-1999-02.html

i. Back door and remote administration programs

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are BackOrifice, Netbus, and SubSeven. These back door or remote administration programs, once installed, allow other people to access and control your computer.

i. Denial of service

Another form of attack is called a denial-of-service (DoS) attack. This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. In most cases, the latest patches will prevent the attack. The following documents describe denial-of-service attacks in greater detail.

http://www.cert.org/advisories/CA-2000-01.html
http://www.cert.org/archive/pdf/DoS_trends.pdf

It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

i. Being an intermediary for another attack

Intruders will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service (DDoS) tools are used. The intruders install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not your own computer, but someone elses -- your computer is just a convenient tool in a larger attack.

i. Unprotected Windows shares

Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking shares combined with distributed attack tools such as those described in

http://www.cert.org/incident_notes/IN-2000-01.html

Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate. One such example is the 911 worm described in

http://www.cert.org/incident_notes/IN-2000-03.html

There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

i. Mobile code (Java/JavaScript/ActiveX)

There have been reports of problems with "mobile code" (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by your web browser. Although the code is generally useful, it can be used by intruders to gather information (such as which web sites you visit) or to run malicious code on your computer. It is possible to disable Java, JavaScript, and ActiveX in your web browser. We recommend that you do so if you are browsing web sites that you are not familiar with or do not trust.

Also be aware of the risks involved in the use of mobile code within email programs. Many email programs use the same code as web browsers to display HTML. Thus, vulnerabilities that affect Java, JavaScript, and ActiveX are often applicable to email as well as web pages.

More information on ActiveX security is available in http://www.cert.org/archive/pdf/activeX_report.pdf

i. Cross-site scripting

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

You can potentially expose your web browser to malicious scripts by

- following links in web pages, email messages, or newsgroup postings without knowing what they link to
- using interactive forms on an untrustworthy site
- viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags

More information regarding the risks posed by malicious code in web links can be found in CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.

i. Email spoofing

Email spoofing is when an email message appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofed email can range from harmless pranks to social engineering ploys. Examples of the latter include

- email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply
- email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

Note that while service providers may occasionally request that you change your password, they usually will **not** specify what you should change it to. Also, most legitimate service providers would **never** ask you to send them any password information via email. If you suspect that you may have received a spoofed email from someone with malicious intent, you should contact your service provider's support personnel immediately.

i. Email borne viruses

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 mail originated from an address you recognize. The Melissa virus (see References) spread precisely because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs.

Many recent viruses use these social engineering techniques to spread. Examples include

- W32/Sircam -- http://www.cert.org/advisories/CA-2001-22.html
- W32/Goner -- http://www.cert.org/incident_notes/IN-2001-15.html

Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

i. Hidden file extensions

Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but a user may choose to disable this option in order to have file extensions displayed by Windows. Multiple email-borne viruses are known to exploit hidden file extensions. The first major attack that took advantage of a hidden file extension was the VBS/LoveLetter worm which contained an email attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs". Other malicious programs have since incorporated similar naming schemes. Examples include

- Downloader (MySis.avi.exe or QuickFlick.mpg.exe)
- VBS/Timofonica (TIMOFONICA.TXT.vbs)
- VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)
- VBS/OnTheFly (AnnaKournikova.jpg.vbs)

The files attached to the email messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example).

i. Chat clients

Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type.

Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients. As with email clients, care should be taken to limit the chat clients ability to execute downloaded files. As always, you should be wary of exchanging files with unknown parties.

i. Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access.

Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers since entire neighborhoods of cable modem users are effectively part of the same LAN. A packet sniffer installed on any cable modem user's computer in a neighborhood may be able to capture data transmitted by any other cable modem in the same neighborhood.

a. Accidents and other risks

In addition to the risks associated with connecting your computer to the Internet, there are a number of risks that apply even if the computer has no network connections at all. Most of these risks are well-known, so we wont go into much detail in this document, but it is important to note that the common practices associated with reducing these risks may also help reduce susceptibility to the network-based risks discussed above.

i. Disk failure

Recall that availability is one of the three key elements of information security. Although all stored data can become unavailable -- if the media its stored on is physically damaged, destroyed, or lost -- data stored on hard disks is at higher risk due to the mechanical nature of the device. Hard disk crashes are a common cause of data loss on personal computers. Regular system backups are the only effective remedy.

i. Power failure and surges

Power problems (surges, blackouts, and brown-outs) can cause physical damage to a computer, inducing a hard disk crash or otherwise harming the electronic components of the computer. Common mitigation methods include using surge suppressors and uninterruptible power supplies (UPS).

i. Physical Theft

Physical theft of a computer, of course, results in the loss of confidentiality and availability, and (assuming the computer is ever recovered) makes the integrity of the data stored on the disk suspect. Regular system backups (with the backups stored somewhere away from the computer) allow for recovery of the data, but backups alone cannot address confidentiality. Cryptographic tools are available that can encrypt data stored on a computers hard disk. The CERT/CC encourages the use of these tools if the computer contains sensitive data or is at high risk of theft (e.g. laptops or other portable computers).

1. Actions home users can take to protect their computer systems

The CERT/CC recommends the following practices to home users:

a. Consult your system support personnel if you work from home
b. Use virus protection software
c. Use a firewall
d. Dont open unknown email attachments
e. Dont run programs of unknown origin
f. Disable hidden filename extensions
g. Keep all applications (including your operating system) patched
h. Turn off your computer or disconnect from the network when not in use
i. Disable Java, JavaScript, and ActiveX if possible
j. Disable scripting features in email programs
k. Make regular backups of critical data
l. Make a boot disk in case your computer is damaged or compromised

Further discussion on each of these points is given below.

Recommendations

a. Consult your system support personnel if you work from home

If you use your broadband access to connect to your employer's network via a Virtual Private Network (VPN) or other means, your employer may have policies or procedures relating to the security of your home network. Be sure to consult with your employer's support personnel, as appropriate, before following any of the steps outlined in this document.

a. Use virus protection software

The CERT/CC recommends the use of anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date. Many anti-virus packages support automatic updates of virus definitions. We recommend the use of these automatic updates when available.

a. Use a firewall

We strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks. However, no firewall can detect or stop all attacks, so its not sufficient to install a firewall and then ignore all other security measures.

a. Don't open unknown email attachments

Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs.

If you must open an attachment before you can verify the source, we suggest the following procedure:

i. be sure your virus definitions are up-to-date (see "Use virus protection software" above)
ii. save the file to your hard disk
iii. scan the file using your antivirus software

iv. open the file

For additional protection, you can disconnect your computer's network connection before opening the file.

Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.

a. Don't run programs of unknown origin

Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

a. Disable hidden filename extensions

Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but you can disable this option in order to have file extensions displayed by Windows. After disabling this option, there are still some file extensions that, by default, will continue to remain hidden.

There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system. The "NeverShowExt" registry value is used to hide the extensions for basic Windows file types. For example, the ".LNK" extension associated with Windows shortcuts remains hidden even after a user has turned off the option to hide extensions.

Specific instructions for disabling hidden file name extensions are given in http://www.cert.org/incident_notes/IN-2000-07.html

a. Keep all applications, including your operating system, patched

Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check periodically for updates.

a. Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

a. Disable Java, JavaScript, and ActiveX if possible

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Turning off these options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some web sites.

Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites.

More information on ActiveX security, including recommendations for users who administer their own computers, is available in http://www.cert.org/archive/pdf/activeX_report.pdf

More information regarding the risks posed by malicious code in web links can be found in CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.

a. Disable scripting features in email programs

Because many email programs use the same code as web browsers to display HTML, vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to email as well as web pages. Therefore, in addition to disabling scripting features in web browsers (see "Disable Java, JavaScript, and ActiveX if possible", above), we recommend that users also disable these features in their email programs.

a. Make regular backups of critical data

Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store the backup disks somewhere away from the computer.

a. Make a boot disk in case your computer is damaged or compromised

To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk which will help when recovering a computer after such an event has occurred. Remember, however, you must create this disk **before** you have a security event.

Appendix

References and additional information

This section contains links to references and additional resources related to this document.

References

The following documents were used in compiling portions of this document:

- CERT Advisories
- CERT Incident Notes
- CERT Tech Tips
- Other CERT documents

CERT Advisories

CA-1999-02: Trojan Horses
http://www.cert.org/advisories/CA-1999-02.html

CA-1999-04: Melissa Macro Virus
http://www.cert.org/advisories/CA-1999-04.html

CA-2000-01: Denial-of-Service Developments
http://www.cert.org/advisories/CA-2000-01.html

CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests
http://www.cert.org/advisories/CA-2000-02.html

CA-2001-22: W32/Sircam Malicious Code
http://www.cert.org/advisories/CA-2001-22.html

CERT Incident Notes

IN-2000-01: Windows Based DDOS Agents
http://www.cert.org/incident_notes/IN-2000-01.html

IN-2000-02: Exploitation of Unprotected Windows Networking Shares
http://www.cert.org/incident_notes/IN-2000-02.html

IN-2000-03: 911 Worm
http://www.cert.org/incident_notes/IN-2000-03.html

IN-2000-07: Exploitation of Hidden File Extensions
http://www.cert.org/incident_notes/IN-2000-07.html

IN-2000-08: Chat Clients and Network Security
http://www.cert.org/incident_notes/IN-2000-08.html

IN-2001-15: W32/Goner Worm
http://www.cert.org/incident_notes/IN-2001-15.html

CERT Tech Tips

Spoofed/Forged Email
http://www.cert.org/tech_tips/email_spoofing.html

Other CERT documents

Results of the Security in ActiveX Workshop
http://www.cert.org/archive/pdf/activeX_report.pdf

Security of the Internet
http://www.cert.org/encyc_article/tocencyc.html#PackSnif

Trends in Denial of Service Attack Technology
http://www.cert.org/archive/pdf/DoS_trends.pdf

Additional resources

Additional information is available from the following sources.

TCP/IP Frequently Asked Questions
http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/
http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part2/
Computer Virus Frequently Asked Questions for New Users
http://www.faqs.org/faqs/computer-virus/new-users/

alt.comp.virus Frequently Asked Questions

http://www.faqs.org/faqs/computer-virus/alt-faq/part1/
http://www.faqs.org/faqs/computer-virus/alt-faq/part2/
http://www.faqs.org/faqs/computer-virus/alt-faq/part3/
http://www.faqs.org/faqs/computer-virus/alt-faq/part4/

VIRUS-L/comp.virus Frequently Asked Questions
http://www.faqs.org/faqs/computer-virus/faq/

Firewalls Frequently Asked Questions
http://www.faqs.org/faqs/firewalls-faq/

Revision History	
June 22, 2001	Initial Release
June 26, 2001	Added SubSeven to Remote Administration Programs section
August 6, 2001	Clarification of IP addressing for ISP dial-up modem pools
December 5, 2001	Fixed broken link to CA-1999-02, added links for Sircam, Goner, and DDoS Trends
February 27, 2006	Removed link to defunct directory that was on cert.org previously.