

TIPS FOR AVOIDING COMPUTER CRIME

- Cyber Crime P.S., CID, A.P.

Introduction

These suggestions are like installing high-security deadbolt locks on doors of an office or home. There is no warranty that following these suggestions will prevent one from being a victim of computer crime, but at least one can make it a little harder for a criminal, and maybe the criminal will find an easier target.

This essay contains only opinions on the general problem of computer security, and is not intended as advice on your specific problem. You should hire a competent expert in computer security to review your situation and then advise you.

1. Password

To access an online computer service or Internet service provider (ISP) one needs both a user name and password. ISPs typically select a user name that is the same as the last name of the subscriber. This means that user names are easy to guess, therefore one must be especially careful with the password.

Select a good password:

- Make the length of your password at least eight characters. It is too easy for automatic programs to sequentially try all combinations of characters in a password of only 1, 2, 3, or 4 characters.
- A five-character password composed of only random lower-case letters has about 8×10^6 possible combinations,

but a eight-character password composed of lower-case letters and the ten digits, all chosen randomly, has about 8×10^9 possible combinations, i.e., about one thousand times harder to guess.

- To make a long password, use a concatenation of two words, each with at least five characters, perhaps separated by one digit (e.g., african65safari).

Avoid obvious passwords (e.g.)

- your name,
- anyone's first name (especially bad are your spouse's first name, your child's first name, your dog's or cat's name)
- your nickname (e.g., "Chinni" or "Buzzi"),
- your home telephone number,
- your date of birth,
- your astrological sign,
- your mother's maiden name,
- your wife's maiden name,
- license plate number of your car,
- exact sequences of letters on a keyboard (e.g., QWERTY or ASDFGH)
- sequences from the alphabet (e.g., ABCDEFG or ABCABC)
- or any other publicly available information.

Also avoid any of the above spelled backwards, and any of the above either preceded or followed by a single digit.

There are about 8×10^6 possible combinations of a string of five lower-case letters that are chosen randomly. In comparison, there are only about 0.15×10^6 entries in an English dictionary for college students' desks. Therefore, it would make sense for a hacker to use a word list from a spelling checker, instead of generating permutations of characters. In response, you should make the hacker work harder by choosing a password that is not in the dictionary of your local language.

For a given number of characters, the strongest password is a random sequence of lower- and upper-case letters and digits. However, such a password can be difficult to remember. My suggestion is to choose a unusual foreign word that does not appear in the dictionary of your local language. Of course, you don't need to limit yourself to official languages. <grin> You can invent your own words, e.g., pagal49diwane. Such words are much easier to remember than unpronounceable clusters of characters. When you get a new computer account, it will come with an initial password, which password was probably randomly chosen. Follow the instructions from the system administrator for choosing your own password, and change the password. The initial password may have been seen by someone who gave or mailed it to you. Having chosen a good password, do not write it down, and do not tell anyone what

it is. (Get a separate account for your spouse, each of your children, each of your co-workers, so that no one shares.) Use a different password at each website, service provider, or computer account.

Changing your password every few weeks is standard advice from computer security experts. However, changing your password every few weeks also makes it easier for you to forget your password. You need to decide if it is worth the bother of changing passwords every few weeks. If you do forget your password, you will need to contact a system administrator, prove that you really are the official user, and get a new initial password assigned.

Many users store their user name and password in a logon script on their hard disk in various programs: e-mail (e.g., Eudora), webbrowser (e.g., Netscape), terminal emulator (e.g., Procomm), and modem control programs (e.g., Trumpet Winsock). This storage of user name and password is convenient, as it automates the logon process. However, if you store your user name and passwords in logon script(s), then:

- You should definitely enable the password setting in the BIOS of your computer, so that a password is required every time the machine is switched on. You might also enable a password setting in Windows98 or other operating system, to give an additional layer of protection against unauthorized use of your computer.
- If other people have access to your computer when your machine is

running and you are away from your desk, you should install screen saver software that requires a password to return to the operating system or applications software.

- If your computer is stolen, it is possible for the thief to logon to all of your accounts. Therefore, it is essential that you logon to each of your online accounts and change the password for each account immediately after the theft of the computer is discovered.

This remediation includes changing your passwords at online stores (e.g., amazon.com). The information stored on your computer in the cookies.txt file that your web browser accesses identifies you to each online store, and could make it possible for a thief to impersonate you and to charge items to your credit card. Nearly everyone has private data (e.g., medical and financial data on a home computer; business secrets on a computer in the office) on their machine. The same suggestions about a password in BIOS and a password in a screen saver apply if you have confidential or proprietary information on your computer. However, unlike changing online account passwords, there is no easy way to destroy the value of confidential data in files on a stolen computer. Users with very sensitive data (e.g., military secrets, major trade secrets) should encrypt all of their data files.

2. Anti-Virus Software

In the 1980s, computer viruses were generally passed from one user to another user via floppy disks. Hence, users in the 1980s did not need anti-virus software if they both (1) only purchased software from reputable sources and (2) never copied programs from floppy disks provided by their friends and colleagues.

Three developments in the 1990s made anti-virus software essential for all computer users:

1. It became common to distribute software and updates via downloads from the Internet,
2. hackers developed viruses that were delivered inside macros for Microsoft Word, which malicious macros could be hidden inside a document sent by e-mail, and
3. hackers developed malicious computer programs that were commonly distributed as attachments to e-mail: clicking on the attachment executed the malicious computer program and infected the victim's computer.

Since everyone uses e-mail and nearly everyone will download executable software from the Internet, everyone should have a good anti-virus program running on their machine.

Because an anti-virus program will likely object to the installation of any new software, the user should disable anti-virus program before installing new software. Of course, before temporarily

disabling the anti-virus program, use the anti-virus program to scan the distribution files (e.g., CD-ROM, floppy disk, or *.exe file downloaded from the Internet) for viruses. Do not forget to enable the anti-virus software after you install new software.

It is not adequate to purchase anti-virus software with a new computer, install the anti-virus software, and forget about that software. The virus definition file for the anti-virus software should be updated periodically, because new viruses are discovered every day. How often you should update your virus definition file is a complicated question: the answer depends upon your tolerance for risk, how you use your computer (i.e., receiving e-mail or downloading software from bulletin boards is risky), and which operating system you use.

1. If your computer runs a 32-bit Microsoft Windows operating system (e.g., Windows 95 or later), then we suggest that you update your virus definition files at least once a week.
2. If your computer runs an Apple operating system or Linux, then we suggest that you update your virus definition files at least once every two months.

Of course, when there is an epidemic of a new virus reported in the news media (particularly a virus spread by attachments in e-mail), it would be wise to update your virus definition files as soon as the developer of your anti-virus software revises their virus definition files

to recognize the new virus, and daily thereafter until variants (copycats) of the new virus stop appearing.

Attachments in e-mail

As a virus, worm, or other malicious program can be transmitted via an attachment to e-mail, one should rigorously follow three rules:

1. Never open an executable attachment (e.g., an attachment with a file name ending in .exe or .vbs, amongst many other types) in e-mail without first knowing the contents and source of this file. There is no harm done in waiting a few hours or a few days to contact the person who sent the e-mail and learn the contents and source of the attachment. The Melissa and ILOVEYOU incidents, on March 1999 and May 2000, emphasize that you can receive malicious programs from a person who you know and trust, since that person could be a victim of a malicious program that automatically sent e-mail in his/her name.
2. Never open any attachment from an unknown source. Simply reply to the e-mail and request that the sender send the attachment as plain ASCII text in the body of the e-mail. Or, if the e-mail is obviously junk, delete both the e-mail and the attachment.
3. Be cautious of any attachment that has a double file extension, especially when the rightmost file

extension is an executable file type. (A file extension is a three-letter code at the end of a filename [e.g., .htm, .doc, .exe, .txt, etc.], that indicates the type of file.) Examples of dangerous double file extensions are:

filename.jpg.vbs
filename.doc.exe
filename.zip.com
filename.gif.bat
filename.txt.pif
filename.mp3.scr
filename.htm.lnk

where "filename" can be any sequence of letters and numbers. Files with such dangerous double file extensions are executable programs (perhaps malicious programs) that are pretending to be a picture, a document, text, or a webpage. This list of dangerous double file extensions is not complete, because there are many different permutations of a non executable file extension on the left with an executable file extension on the right, and because there are more than sixty executable file extensions in Microsoft Windows.

3. Firewall

It is good practice to erect a "firewall" between parts of a computer system that an external user can access (e.g., via modem or Internet or voice mail) and parts that are supposedly accessible only by a local user. Many hackers run programs that randomly search the

Internet and probe ports on computers that are connected to the Internet. If the hacker finds a port that is "open", the hacker might be able to access that computer and view/alter/delete files on that computer. Worse, hackers may also hijack the victim's computer and use it to launch their illegal attacks on other computers.

Some hackers randomly search the Internet, probing ports controlled by a malicious program called SubSeven. When the hacker finds a computer that contains SubSeven and is not protected by a firewall, the hacker can access the victim's computer through the backdoor provided by SubSeven. The SubSeven program was first detected in June 1999, and there are many similar programs in existence, for example, the Back Orifice program that was first detected in August 1998.

In February 2002, there was an average of approximately 1½ attempts/hour to probe a port on a computer. In March 2004, there was an average of 60 attempts/hour to probe a port on a computer. This dramatic increase in the number of attempts per hour to access a computer shows that the Internet is becoming a more dangerous place and that firewall software is necessary for a secure computer.

Separate machines

Now that computers are relatively inexpensive (e.g., less than RS 30000), I believe that it also makes sense to have totally separate and isolated machines for external access. The cost of having a

separate computer that is dedicated solely to receiving incoming modem connections and requests from the Internet (i.e., e-mail and web browser software) is offset by the increase in security with minimum inconvenience to authorized users inside the building. When a secure computer and a computer for external access are in the same building, communications between them should be via floppy disk or rewritable compact disk, not via wire or cable.

Here are some hints about how to make a computer secure from incoming commands:

- Set terminal emulator software so that the modem either
 - a. never answers an incoming telephone call or
 - b. answers on the 99th ring and also connect a telephone answering machine to the modem's line to pick up on the fourth ring, so there is never a 99th ring.
- Do not install any software that allows even an authorized user to access the computer remotely, via a modem.

More important to have firewall on computers with wideband Internet connection

During the 1990s, communications between computers in different places were made by an analog modem that connected to an ordinary voice-grade telephone line. The state-of-the-art

analog modem in 1998 (i.e., using the V.90 standard) could download data at 56000 bits/second and upload data at 36000 bits/second. With compression (i.e., using the V.42bis standard), effective download data rates of more than 120000 bits/second were possible on an ordinary voice-grade telephone line. Each time the user wanted to connect to the Internet, the user would need to have the computer's modem dial the local access number of the Internet Service Provider (ISP) and establish a connection, a process that takes about 30 seconds. The ISP then assigns the user a numeric IP address for that one Internet session. This IP address is known as a "dynamic IP address", because it is different for each session. If the user does not send/receive some data over the Internet during some period of time (e.g., ten minutes), the ISP will automatically disconnect from the telephone line and sever the user's connection to the Internet.

Beginning in the 2000s, it became common to connect computers to the Internet via cable television lines or on DSL telephone service, which have a much higher download data rate, so-called "wideband" service. The cable or DSL service is always connected to the Internet, unlike the modem on an ordinary voice-grade telephone line. Specifically, the ISP assigns the user an IP address that is constant, a so-called "static IP address".

Cable or DSL makes a user more vulnerable to intrusions by hackers in two different ways:

1. The static IP address allows a hacker to return to the victim's computer, once the hacker has found that victim's computer has no firewall or an ineffective firewall.
2. If a computer is on all the time, hackers have continuous access to that computer, since cable or DSL is always connected to the Internet.

For these reasons, firewall software is more essential if one uses either cable television or DSL for an Internet connection.

4. Avoiding harassment

For casual on-line activities, you can establish a free e-mail account at Yahoo, Hotmail, or some other provider, and use an alias for that account. If someone harasses or stalks you, then you simply close that account and chose another alias. In other words, you adopt a disposable identity for your life in cyberspace.

Never give out your real name, address, city, telephone number, or other identifying information to a stranger in a chat room, computer bulletin board, or other public place.

Avoiding Phishing

The only connection between phishing and computers is that modern phishing uses e-mail and a bogus website to get a gullible person to disclose personal financial information to criminals. That

having been said, it is worthwhile to alert people to the existence of phishing.

People first encounter phishing when they receive a fraudulent e-mail that typically purports to be from a bank, credit card company, or other financial institution. The e-mail might mention something about your account is suspended until you "verify", "update", or "validate" some information. The e-mail invites you to click on a link in the e-mail. The link typically takes you to a web server located in a foreign country and operated by criminals, who display web pages with the logo and trademarks of a bank, credit card company, or government agency, which makes the webpage appear legitimate. The bogus webpage asks you to supply your account numbers, passwords, and other personal information (e.g., Social Security number, date of birth, mother's maiden name) that can be used to fraudulently access your financial accounts and perpetrate identity theft crimes.

Citibank has been a popular target for phishers. In response, Citibank posted a webpage on some specific phishing e-mails. The U.S. Federal Trade Commission (FTC) also has a consumer alert on the subject of phishing. There is also an industry antiphishing working group.

5. Backups

If a computer virus or an invading hacker deletes your files, or either one corrupts your files, the easiest way to restore your computer may be to reformat

the hard drive(s) and then copy files from a recent backup. Backups also offer protection from more common (and less exotic) threats such as accidental deletion of a file by an authorized user or failure of a hard disk drive.

Because making a backup is a chore that takes anywhere from a few minutes to more than an hour (depending on the amount of files copied to the backup medium and the speed of the backup device), and because backup copies are rarely needed, most users do not make backups as frequently as they should. The interval between backups should be determined by the amount of data files that you can afford to lose

Best policy is to make three kinds of backups:

1. A **full** backup of all files at least twice each year, and immediately after completing a major project.
2. An **incremental** backup of only those files that were changed since the previous incremental backup.
3. An **archival** backup: a full backup of all files to newly formatted media. Then activate the write-protect feature on this disk or tape cartridge and never write to it again.

If the only threat was a computer virus or attack by a hacker, it would be adequate to store all of the backup media in the same room as the computer. Because there are also threats of fire, tornado, etc., one should [also] make a

backup for offsite storage, such as in the safe deposit box at a bank. Archival backups are particularly well suited to offsite storage, since they are rarely needed.

The cost of backup media is so low compared to the value of the data, that it is reckless behavior not to make an archival backup at least once each year.

6. Other techniques:

Because Microsoft bundles an e-mail program, Microsoft Outlook Express, with their operating system, this e-mail program is commonly used. Hackers write malicious programs (e.g., the Melissa virus that struck on 26 March 1999) to use the victim's e-mail address book in Microsoft Outlook, knowing that such a malicious program will cause havoc on most personal computers, because of the popularity of Outlook. Similarly, hackers have written macro viruses that affect the Microsoft Word processing program. Use the latest version of e-mail and Internet browser software, operating system, and anti-virus software. Install the patches that are released between versions, to avoid security holes and other problems.

Before disposing of an old computer, by donation or sale:

1. delete all data and document files.
2. delete all application programs (to avoid software piracy).
3. run WIPEINFO, in Norton Utility for DOS version 8 (or the corresponding version for the Apple Macintosh), to overwrite all

of the free space on the hard disk, thus making it difficult to recover your data and document files.

WIPEINFO is necessary, because the delete command only changes the first character of the file name in the file allocation table (FAT) on the disk; the delete command does not remove the information in the file from the disk.

If you are tossing an old computer or hard disk drive in the trash, first disable the hard disk drive. You can use a hammer and chisel to remove some of the integrated circuits from the disk controller that is attached to the hard drive, or you can remove the hard drive from the computer and smash it with a hammer.

The design of a logon screen should include a notice that unauthorized use is prohibited by law. One might refer to the state (or federal) statute and mention the maximum penalties, in an attempt to deter people. On the other hand, making the notice too strong (i.e., reference to secret, proprietary, or private information inside the computer) may be a double-edged sword, in that it may entice a hacker by increasing the thrill.

Disabling Features in Microsoft Windows :

Some optional parts of the Microsoft Windows 95, and later, operating systems make a computer vulnerable to harm by malicious programs. For detailed instructions on how to disable some of these parts, see:

- The Computer Emergency Response Team (CERT) at Carnegie-Mellon University has links to their webpages on showing normally hidden file extensions, disabling JavaScript in web browsers, and disabling ActiveX.
- F-Secure, an anti-virus software company in Finland, has instructions for how to uninstall Windows Scripting Host in Windows 95, 98, 2000 and NT. This uninstall provides immunity from any malicious program that uses Microsoft Visual Basic Script, such as the ILOVEYOU worm. Symantec, who distributes Norton Anti-Virus software, has similar instructions: go to their search webpage, and enter the search query "uninstall Windows Scripting Host".

Wireless Networks

A local area network is popular in businesses, because it allows computers to share files without using a modem and because it allows multiple computers to use a single printer. Conventional local area networks in the 1980s required coaxial cable to be strung between computers and printers on the network. Recently, it has become popular to use a so-called "wireless network", in which computers and peripherals communicate via low-power radio transmissions.

However, wireless networks have an obvious security problem. Radio transmissions do not magically stop at the

exterior walls of the building. Anyone with an antenna and amplifier can intercept communications on a wireless network, which raises the possibility of both privacy violations and industrial espionage. It is easy to imagine someone sitting in a van in a parking lot with a high-gain Yagi antenna and a laptop computer, intercepting communications from a wireless network inside a nearby building.

If you want to use a wireless network, at least:

- enable encryption on all transmissions and
- locate the transmitters as far as possible from exterior walls, and especially far from windows.

Conclusion

When a criminal perpetrates a crime, his attorney is likely to say that the criminal did everyone a favor by calling attention to lapses in security of computers. It is a criminal defense attorney's job to put the best possible spin

on the client's horrible activities. However, recognize that "blaming the victim" for the crime is a cheap shot. Even if the victim behaved in an imprudent way, a victim never invites a crime.

It is to make clear that there are two completely separate issues:

- (1) prosecution of perpetrators of computer crimes and
- (2) steps that a computer user can take to avoid being a victim.

Most of the really effective steps that a computer user can take to avoid being a victim of crime make the user's computer less convenient to use. Each user must balance for himself/herself how much security is enough, especially when faced with daily inconvenience of high-level security measures vs. the rare occurrence of attacks. Further, the user must be aware that a determined and creative criminal can defeat nearly any security measure, so complete security is not possible.



Everybody gets so much information all day long that they lose their common sense.

- Gertrude Stein (1874-1946)

You will be glad to know that our "FARMER WELFARE CENTRE" is ready with Internet, debit card and e-banking.....

