STATUS: ARCHIVED (Depreciated)

A very old but still very relevant article that outlines the threats that we all face online. Understanding the risks and their sources will go farther in protecting you then any anti-virus available. This should be standard reading in every school.

David Bowen, Department of Interdisciplinary Studies, College of Urban, Labor and Metropolitan Affairs, Wayne State University

Last updated: October 13, 2003

Life online is getting less secure. It's you against the hackers, and there are more of them, and they seem to have a lot more time. Here is a brief guide to the dangers you face today, and suggestions about protecting your computer and your Internet connection.

1. **Sources - where do online threats come from?**
    - Free programs, unauthorized copies, etc.
    - Scripts in email attachments, word processing documents, spreadsheets, etc.
    - Internet downloads, may be silent (cookies, web bugs)
2. **Types**
    - **Harmful**
        - Virus. A program (*.exe, *.com etc) that gets into your computer, is executed, and does harm there, such as erasing or corrupting files, or changing the way your programs work. It also seeks to copy itself and distribute copies using floppy diskettes, a Local Area Network, email or a general Internet connection. NOTE: your computer may not be configured to show file extensions, or it may be reconfigured by a script. I always recommend seeing the extensions.
        - Worm. An executable part of an email message or a word processing document that may damage files on your computer, but mainly is directed towards clogging up resources on your computer, slowing it down or seeming to disable it, and which also emails copies of itself to other computers using a list of email addresses.
        - Trojan horse. A back door that sits on your computer and allows others to download and execute files, or take other actions. Can be used in Denial of Service attacks.
        - Monitoring software. Software that employers put on employees' computers to check that employees are doing useful things and not breaking company

regulations. May include a keyboard logger, a feature that records all of your keystrokes and reports them.

- Spyware. Software that reports computer usage to another computer, often used to report personal information such as credit card numbers or social security numbers. May include a keyboard logger (see "Monitoring software" above). Some people use "spyware" to refer to what I call "monitoring software" above. The results are often the same - information about your computer usage gets reported to someone else. If the category here is not called spyware, it may instead be called "snoopware."

- Operating system vulnerabilities. For example, Telnet and FTP are two features of many operating systems. Telnet allows an external user to use the command line on your computer. FTP allows an external user to download files to your computer, and execute them. If the passwords for these are left at some default, or your passwords can be easily guessed, your computer is vulnerable. Other vulnerabilities or exploits use malicious messages to overflow data areas, allowing the user to download and execute code. In this case, the underlying software on your computer has been badly written. Many such examples are found and reported on a regular basis.

- Denial Of Service (DOS) attacks. This is an attack on a server that causes it to be unavailable to legitimate users. The targeted server is bombarded with so many requests for information and services that it spends virtually all of its time on these fake requests, and has no time for legitimate users. The server has not been hacked into, has not been compromised, but still its services are not available. In addition, the network is slowed down for everybody. The attack is often mounted from hundreds of other computers that have been taken over by hackers who have previously installed trojan horses to target that particular server.

- Warez (not "jaurez" but wares with a z). This is where hackers put software on your computer to distribute files over the Internet, often illegal files, which they also download to your computer. The purpose is to use your computer as a sales platform for distributing these files. Orders may be taken and money collected on a separate computers, then customers directed to you for delivery. This software can also use your computer as a platform for taking over other computers for the same purpose.

- Web jacking. Intercepting traffic to a legitimate web site, and convincing the unsuspecting that they are supplying a trusted site with their identification. Web jacking can also be done for the purpose of downloading spyware or warez.

- Typo site. A web site that closely matches the URL for a legitimate site, but is misspelled. People entering this particular misspelling will go to the typo site, where they may be subject to many of the ills above.

- Stealthware. Growing, especially since about March 2003. If you visit certain web sites using Internet Explorer (IE) , these sites exploit a weakness in IE called the Browser Help Object (BHO), to download themselves to pop up streams of ads on your PC, even when you are no longer on the Internet. Listed as most often coming from free web-hosting sites, porno sites and typo sites (PC World, October 2003).

- Identity theft. Can occur through spyware, intercepting Internet traffic (rare, especially with secure communication), hacking into the merchant's server or (most common) through authorized employees.

- **Privacy**

  - Cookie. A web server can leave a cookie on your computer, a small file or part of a file, which is meant to enable a dialog with the web server (the web server that "set" the cookie can read it when you come back, and recognize you). The cookie can record information such as the web site, the time and date, and what page you were on. Cookies are pretty standard, but malicious companies and hackers can can look at your cookies, and perhaps tell something about you from where you have been, and report back. Both Netscape and current versions of Internet Explorer allow cookie control.

  - Web bug. A tiny web graphic that is used to tell another web site what file you are looking at now. For example, an online store might arrange for a web bug from a company that personalizes ads for the store. Not everyone agrees that you should be worried about web bugs; no personal information is reported.

- **Annoying**

  - Virus hoax. A false warning that a certain email message or link contains a virus that is often the most terrible virus ever, certified as such by IBM or AOL or Symantec. Usually you are asked to forward the warning to everyone one you know. These things can circulate for years after they are exposed (indeed, a former WSU VP for Technology frequently circulated messages like this).

  - Spam - widely distributed often anonymous email that clogs up mailboxes and the Internet. Sending mass emails is so cheap that even if 99.9% of people trash it without reading, you can still make a very nice living off of that remaining tenth of a percent.

        - Pop-up ads / pop-unders. Windows that pop themselves up on top when you go to a regular web site. Some may be popped by the site you are going to, but others are popped by a separate site. Some can be very aggressive, for example making it difficult to shut the pop-up down by hiding the close button or putting it off the screen. A pop-under sits underneath your Browser window and appears after you thought you had closed your Bowser.

3. **Why do they do it? What motivates people who do this? Does it matter?**
    - Exploits. Some people just get a kick out of showing that they can harm or take over your computer.
    - Malice. Malice tends to be directed against larger systems, such as Google, etc. Eastern European countries, for example, have skilled programmers with no jobs after the fall of the communism.
    - Greed. Some computer exploits take over your computer as a server for computer information such as pirated videos, pornography, and so on, with payment being made before the customer is sent to your web site. Or stolen information can be bundled and sold.
    - Bottom line: you may feel that you are too insignificant to be a target. If this is your attitude, times have changed and you /are/ a target..
4. **Protection:**
    - **Passwords**
        - Passwords can be strong, weak, or in between. To be secure, you should use strong passwords. Here are some guidelines for passwords (many taken from the C&IT web site). Examples of weak passwords:
            - A dictionary word. Hackers can back up an electronic dictionary to your login and run through all of the possibilities very quickly.
            - A dictionary word spelled backwards.
            - Your name, your user name, names of your spouse, children or other relatives. Does not matter if they are spelled backwards.
        - Computers used by hackers can guess passwords randomly and try them. Here are some ways to frustrate this approach:
            - Use a minimum of six characters so there is more guessing to be done.
            - Use a wide variety of characters so there is more guessing to be done. If you use only lower-case letters (this is common), that is only 26 guesses

to make per character. Put in some uppercase, numbers and special characters such as !, @, and #, and you are up to about 75 guesses per character. For our six-character password, we have gone from three hundred million possible passwords to nearly two hundred billion passwords, or nearly six hundred times more passwords to guess.

        - Today we all have several if not many passwords. Do not use the same password everywhere. Use a variety of passwords. Make the hackers work harder.

- Some ways to construct strong passwords:

    - Use the first or last letters of a phrase, such as mhall from the first letters of Mary Had a Little Lamb, or ydaeb from the last letters, although this one does not have the minimum of six letters.

    - Run two dictionary words together that are not often associated. For example, you could combine base and ball to make baseball but this is a common word itself. On the other hand, combining base and bat to make basebat is an unusual combination, and is therefore better.

    - Make an arbitrary combination of upper case, lower case and special characters, such as aEQ!y&23.

    - If learning a separate and distinct password for every location is too much, you can make an easily remembered customized password for each place you go by taking a password from any of the above methods and adding, either at the beginning or the end, either the first two three letters, or the last two or three, of the place you are going to log into. For example if we take the last two letters of the location, and your base password is ydaeb, your password for WSU would be ydaebSU and for Amazon would be ydaebon.

    - Do not let your computer memorize your passwords. This is always good advice, but particularly for a lab or public situation, where anyone could walk up to the computer and log in as you.

    - Make sure to log out of any system you can, when you are done using it. Otherwise the next person using the computer could use your account, at least before your logout times out from inactivity.

- **Be cautious:**

    - Do not open an email attachment if you do not know the person who sent it. Possibly you need to expect it.

        - Pay attention to the URL for all sites you are visiting. Watch for webjacking.
        - Be slow to give out personal information. Watch out for requests for your mother's maiden name.
    - **Antivirus program.** Looks for matches to known viruses. Used to be the standard for protection, but most likely is now not enough.
        - Virus definition files. Must be updated frequently, something like two weeks. Most new antivirus programs can be set to update themselves in the background whenever you are connected to the Internet.
        - Scan engine. The program that searches for the viruses. Each time a new "road in" is discovered, an update is necessary so that the engine will scan that road in, certainly every three or four years. Often requires paying an upgrade fee.
        - Should now protect against all files brought in to your computer through the Internet, on floppy diskettes or zip disks, etc.
    - **Firewall.** Hardware or software that allows only trusted sites and programs to use network connections, including the Internet. Also blocks and restricts access to "ports."
    - Many of the attacks listed above have specialized software, often free, to protect against them. For example, Ad-Aware, free from Lavasoft (this is not an endorsement) is advertised as protecting against attempts to track and report your computer usage.
    - **Internet Security Suite.** Combines antivirus and firewall, with other security features such as spyware blocking. MacAfee and Symantec (Norton) have products.
    - **Operating system updates.** Particularly for Windows ME, 2000, XP. Microsoft seems to be more vulnerable right now, for three reasons:
        - So much software is Microsoft that a hacker gets a bigger bang hacking their stuff.
        - Recent Microsoft software (particularly Windows and Internet Explorer) has many features that allow a remote connection (a point of attack).
        - Often the code for these new features is poorly written from an Internet security standpoint, probably due to a rush to get features "out the door." Bad Microsoft!
    - **Reducing the time during which your computer is open to attack**
        - If you have a high-speed, "always on" connection, turn your computer off whenever you are not using it. If your computer is off, it cannot be attacked.

- If you have a modem connection, close your Internet connection when you are done with it, even if you might need it again. If your computer is offline, it cannot be attacked over the Internet.