

What you should know about the dangers of the internet.

Computers have become very useful tools for communications, banking, shopping, entertainment, staying in touch with friends and family and learning about any number of interesting topics. However, the internet has a dark side, and most people are completely unaware of the pitfalls which come with this relatively new and fascinating online world.

Among the malicious intentions of those who would compromise your computer are those to gain access to your personal data for identity theft, to use your computer to send spam or be used to attack other computers on the network, to use your computer to “hack” other computers or simply as the act of juvenile mischief to wreak havoc. What ever the intent, you owe it to yourself to understand the dangers and learn how to protect yourself, as it may save you countless headaches, and in some cases, a substantial amount of money.

LET THE WEB SURFER BEWARE!!

1. The most common dangers

2. Likely ways to get malware infections such as spyware and viruses

3. Security at your IU South Bend workstation

4. Securing your home computer and laptops

1. The most common dangers

There are several forms of malicious software infections, (malware), which may compromise your computer system. Unlike viruses in the old days, most malicious software operates in the background without the computer user even knowing that they are there. Among them are:

Adbots – Adbots are used to deliver unwanted advertisements to your computer, usually in the form of pop up windows. While these are not that harmful in and of themselves, they do indicate that your computer is not adequately protected and is probably infected with other malware.

Backdoor – A backdoor is a way in to your computer, bypassing the normal authentication procedures. Backdoors allow hackers to utilize your computer for any reason in which they can conceive.

DDoS Zombie – One type of virus you might have on your computer creates a backdoor in to your system for which a hacker can “call up” your computer to be used as a Distributed Denial of Service tool. Basically, your computer is used along with thousands

of other infected computers to send mass amounts of network traffic to a target machine, (usually a web service for which the owner is being attacked for not giving in to extortion). Again, especially with computers connected to high speed internet connections such as DSL, the owner of the computer is likely to not even know that their computer is being used as a tool to carry out malicious internet attacks. A computer which is infected in such a way is said to be a “zombie” computer.

Dialers – Have you ever had your computer modem dial the network by itself, as if it had a mind of its own? If so, you probably had a Dialer infection on your computer. Besides being used as a tool to automatically connect to sites to download even more malware to your computer, a Dialer can call 900 numbers which can run up your phone bill. Dialers take advantage of the fact that many users save the user and password pair for their dialup connection out of convenience. As it turns out, it’s convenient for hackers as well.

Downloaders – This is malware which is used by someone to download files from your computer to their computer. For example, they might be interested in files with extensions common to spreadsheets, database files or income tax files, to name a few.

Hijackers - Hijackers take control of various parts of your web browser, including your home page, search pages, and search bar. They may also redirect you to certain sites should you mistype an address or prevent you from going to a website they would rather you not, such as sites that provide software updates. Hijackers most frequently target Internet Explorer.

Keyloggers – Anyone who has ever had their identity stolen and suffered financial loss would tell you to pay close attention to the following information. Keyloggers are malware which can capture the keystrokes from your keyboard and save them to a file to be transmitted to a hacker later on. Usually, Keyloggers are awakened when you invoke a secure session, such as SSH or ordering products online through a “secure” order form, (so much for ‘secure’ network ordering). A hacker can gather useful information such as user/password pairs, PIN #'s, account #'s, credit card information and other personal information about you which could be used to steal your identity for the purposes of their financial gain in your name and your liability.

Spybots – Not to be confused with the anti-spyware software by the same name, spybots send information from your computer back to interested parties about your activities, (such as what websites you visit), for the purpose of gathering information about you.

Spyware – Spyware is a generic term for malicious software which ends up on your computer, and is used to gather information about you and other files on your computer. This information includes what sites you visit, or in worse cases, personal information used for identity theft.

Trojans – Simply put, these are backdoors in to your computer in which access is gained by hackers on the internet to either gather information from your computer or to use your

computer as a tool for malicious activity such as internet extortion schemes, sending spam from your computer or using your computer to hack in to other systems.

Viruses – In the old days, the fact that you had a virus on your computer would usually become immediately obvious as they would do malicious damage to your computer. These days, the creators of viruses have other intentions in mind. A virus has become a generic term for many types of malicious software installed on your computer. The most common type today are Trojans, which like the name implies, create backdoor entry points in to your computer. Especially with high speed connections like DSL, your computer may be compromised and not give any signs of infection.

Worms – Worms can replicate themselves from one machine to another without the need of downloading them from the internet. They often send themselves as attachments in emails they generate from their infected host computer. Worms can be used as Trojans to open doorways to your computer or to send out spam. You know all that spam you get that is annoying beyond belief? Chances are, most of it is coming from computers on the network which are compromised by worms that remain undetected.

More Info - For more information on Malware, do a websearch with the key words “types of malware”.

2. Likely ways to get malware infections such as spyware and viruses

First and foremost understand three things:

- A. Trust no message sent to your computer from anyone.
- B. Free is not free.
- C. Visiting websites which are unknown to you is dangerous.

The three most common ways computers become infected is from opening email attachments which contain malware, downloading files off of the internet or visiting a malicious website.

Many worms use email to send spam and to spread themselves to other computers. They use email addresses that are found in email address books on the infected computer, so that the email appears to come from people you know. These emails are disguised as something official or useful, such as security updates for your computer or official business from a bank or IT department. Never trust emails with links to security updates. Be aware that emails which appear to come from people you know, may contain harm links. These links are usually disguised as innocent web locations.

Another very common way of catching a virus is from downloading things from the internet. The most common websites are those that offer free downloads such as screensavers, background images, pornography, music files or any other free download you can imagine. Internet scoundrels have even figured out a way to put viruses in pictures that you can download and save to your computer. Another very common way of getting malware infections is use of P2P software such as Kazaa, Morpheus, ...etc.. Again, free is not free.

The third most common way to end up with an infected computer is by simply visiting websites setup to lure visitor with the intent of tricking the user in to clicking on a link which will download malicious software. You may be offered free software or images, or a pop up window may appear which will download malware whether you click 'OK' or 'Cancel' or 'Exit' or any other button, or you may be tricked in to clicking on a link to a page which actually downloads malware. Internet Explorer is the most targeted web browser, which is why IU South Bend IT recommends alternative web browsers such as Firefox from mozilla.org.

Now for a fact which may be quite surprising to you. You can turn on your computer, have it attached to the network, not be reading email, not surfing the web, not downloading anything, and be vulnerable, simply by being attached to the network. It has been documented that an unprotected, unpatched computer attached to the network will be compromised in as little as 8 minutes.

To learn how to protect yourself, follow the links on security at IU South Bend and protecting your computer at home.

3. Security at your IU SOUTH BEND workstation

- At IU South Bend, each workstation setup by IT has Norton Antivirus software installed. This software should be centrally updated, however, some viruses actually disable the update and protective features of antivirus software. Ensure that Norton anti-virus is being kept up to date via Live Update and is performing regularly scheduled scans. – [<http://kb.iu.edu/data/agzb.html>]. When you initially start Symantec Antivirus, the date of the Virus Definition File should rarely be more than a week old.
- Lock your workstation when it's not in use, ("Windows Key – L"), or log out. Never leave your workstation unattended while logged in.
- Update Spybot, [<http://kb.iu.edu/data/anfq.html>], and scan your office computer at least once a week, [<http://kb.iu.edu/data/angd.html>].
- Update Adaware, [<http://kb.iu.edu/data/anfa.html>], and scan your office computer at least once a week, [<http://kb.iu.edu/data/alrm.html>].
- Never keep a database or list of individual's personal information on computers other than those designated by IT as database servers.
- Inform IT if you bring up a server on campus and follow the IT [Server Security Guideline].
- **Never share your password with anyone at any time.** This includes use of your IU password to authenticate to IU systems from home.
- It is ILLEGAL to share music and other media files if you do not have appropriate permission to distribute the files. Check the options you have set in file-sharing programs like Morpheus, KaZaA, Aimster, and Gnutella. To read more about Indiana University's policy on file sharing, see [[File Sharing @ IU](#)]. For details on specific programs, see: [[Disabling Peer to Peer File Sharing](#)].
- Never give out personal information (such as your Social Security #) via e-mail or on an insecure web page, or if you are concerned that your information might be intercepted and used illegally.
- Clear your web browsers cache periodically, or set the cache to expire at regular intervals. For details, visit [<http://kb.iu.edu/data/abts.html>]

4. Securing your home computer and laptops

So you just bought a computer brand new, took it out of the box, set it up and have begun surfing the web. You may be thinking that since the computer is new, it should have all the software and safety precautions built in already. Well, you're probably wrong.

Whether you have an older computer or a brand new one, there are steps you need to take to ensure the security of your system. IU South Bend IT does not support users home equipment or personal equipment brought on campus. However, we strongly recommend you take a few precautions to protect yourself. The information provided in this section is simply a guide and is provided for your benefit.

The first thing that you need to know is that Windows 95/98 and Windows ME are not secure operating systems when connected to the internet. IU South Bend IT strongly recommends that if you are on the internet with a Windows based computer, that you use Windows XP with Service Pack 2, (SP2), and that you keep the software updated.

While it is true that Mac OS or Linux based computers are not as frequently targeted by viruses and hackers, there are vulnerabilities and viruses written specifically for those operating systems as well, and it is important to keep these operating systems patched with the same vigilance as a Windows based user.

[A. Security related software.](#)

[B. A few words about DSL & Cable Modems](#)

[C. A few words about home wireless access points.](#)

A. Security related software.

Many of the software titles listed below are available to IU students, faculty and staff for free. It is available on the IUWare CD, [<http://kb.iu.edu/data/agze.html>], which can be obtained in the bookstore or as a free download from [IUWare.iu.edu].

The great news is that there is all kinds of free security software available to home users, whether associated with IU or not. So for a small investment of only your time, you can significantly decrease the likely hood of becoming a victim of internet crime.

Virus Protection

IU students, faculty and staff can install and use Norton Symantec Antivirus software on their home computer for free. This software should be configured to automatically receive updates via Live Update and to perform regularly scheduled scans of your computer, however, some viruses actually disable the update and protective features of antivirus software. Ensure that Norton anti-virus is being kept up to date via Live Update

and is performing regularly scheduled scans. – [<http://kb.iu.edu/data/agzb.html>]. When you initially start Symantec Antivirus, the date of the Virus Definition File should rarely be more than a week old.

As an alternative or even as an additional anti-virus program, Grisoft.com offers AVG antivirus, which can be downloaded for free, or an enhanced version can be purchased online.

Anti-spyware

Spybot can be installed for free. Update Spybot, [<http://kb.iu.edu/data/anfq.html>], and scan your home computer at least once a week, [<http://kb.iu.edu/data/angd.html>].

Adaware can be installed for free. Update Adaware, [<http://kb.iu.edu/data/anfa.html>], and scan your home computer at least once a week, [<http://kb.iu.edu/data/alrm.html>].

Firewall Software

Microsoft XP SP2 comes with a basic firewall built in. However, it lacks the protection that other software firewalls can provide. IU South Bend IT can not recommend any one package as being the best suited for all concerned.

This website gives detailed information on firewalls [<http://grc.com/su-firewalls.htm>].

Some good firewalls can be found here, (*including some free versions):

- Zone Alarm* [http://www.zonelabs.com/store/content/company/zap_za_grid.jsp]
- Symantec [http://www.symantec.com/sabu/nis/nis_pe/]
- McAfee
[http://us.mcafee.com/root/package.asp?pkgid=101&WWW_URL=www.mcafee.com/myapps/firewall/]

Updates

Security updates are patches supplied by the developing software company when they discover a vulnerability to their software package and wish to provide updates to you, the consumer, to protect your computer system. While Microsoft is by far the best known for providing updates, [<http://kb.iu.edu/data/ajco.html>], any software company may provide end users with updates.

For example, the secure web browser by Mozilla.com, known as Firefox, has a method of finding and downloading updates. We encourage you to discover for yourself those update packages available for the software you have installed on your home computer.

B. DSL & Cable Modems

High speed access to the internet is desirable by the person using the computer. However, it also makes your computer a more desirable target by hackers and malware.

By virtue of the fact that the computer is “always on” the network and has greater speed capacities, it is more vulnerable to being cracked and exploited. Depending on the type of DSL or Cable Modem, the computer may actually have more vulnerabilities to exploit. IU South Bend IT does not provide support for these types of connections; however, we do strongly recommend the use of firewall products.

Further information can be viewed here.

[<http://infosecurymag.techtarget.com/articles/january00/features1.shtml>]

C. A few words about home wireless access points

While internet connections become backdoor entry points to your computer from the internet, wireless access points connected to your computer system can be doorways to your computer AND internet access for unintended users through your network connection.

Wireless Pitfalls

- It is a doorway in to your computer.
- It is a doorway for unauthorized use of your internet access.
- Without encryption, your data can be intercepted and viewed.

Common Mistakes

The two most common mistakes made by people who setup wireless access points are not properly configuring the access point itself and not configuring their computer and internet access to prevent unauthorized use of your connections.

Protection Methods

IUSB IT strongly recommend that you protect your system with firewalls, wireless authentication models such as MAC address limitations, use of encryption and configuring the access point appropriately. Information on most of these items can be found here [<http://www.microsoft.com/athome/security/online/homewireless.msp>].

Initial Configuration

When you first install a new access point, it is a good idea to change the default SID, (the name that your wireless access point shows on your computer as), the administrator's password and change the channel, (which is usually set by default to channel 6). If the access point has the option, set the channel to “Auto”, to help avoid conflict with neighboring access points.

Security Keys

WEP is a security scheme presented in the early days of wireless access. It is virtually useless as a security tool, as it can be easily defeated. Today, WPA comes on most wireless access points and is much more secure.

Other Resources

For more information on securing your home computer, visit IU ITSO's webpage

http://itso.iu.edu/Guides_for_Everyone