HOW TO PROTECT AGAINST SPY-WARE

Spyware is software that collects personal information without your knowledge or permission. You might be the target of spyware if you download music from file-sharing programs, free games from sites you know nothing about, or other software from an unknown source. If your computer suddenly begins to display hundreds of pop-up ads or if your start page changes without your knowledge, you may be the victim of spyware.
For general information on what it is, how it works and what you can do to prevent or get rid of it go to
microsoft.com/athome/security/spyware

The following free tools are useful for finding and eliminating spyware:
Spybot Search and Destroy - *http://www.safer-networking.org/en/download/index.html*
Ad-aware (download) - *http://www.lavasoft.com*

PROTECTING YOUR PRIVACY ONLINE

When sitting at your computer "surfing the net", sending electronic mail messages, and participating in online forums, it's easy to be lulled into thinking that your activities are private. Be aware that at any step along the way your online messages can be intercepted and your activities monitored — in the vast untamed world of cyberspace. Educate yourself on the risks as well as the measures you can take to protect yourself online.

Visit the following web pages to learn more about protecting your privacy online.

Microsoft – Maintain Your Privacy
www.microsoft.com/athome/security/privacy/

EFF's - Top 12 Ways to Protect Your Online Privacy
www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy

CDT's – Top 10 Ways to Protect Privacy Online
www.cdt.org/privacy/guide/

BBB Online (Better Business Bureau) - Privacy Tips
www.bbbonline.org/UnderstandingPrivacy/toolbox/tips.asp

Microsoft – Chat and Messaging Safety
www.microsoft.com/athome/security/chat/

PROTECT YOURSELF FROM IDENTITY THEFT

Being a student does not safeguard you against identity theft, one of the fastest growing consumer crimes in the nation. Identity thieves don't steal your money; they steal your name and reputation and use them for their own financial gain. They attempt to steal your future! Identity theft literally steals who you are, and it can seriously jeopardize your financial future.

In fact as a student, you may even be more vulnerable to identity theft because of the availability of your personal data and the way many students handle this data.

Visit the following web pages to learn more about identity theft and how to protect yourself from it.

Office of Inspector General
www.ed.gov/about/offices/list/oig/misused/idtheft.html

Federal Trade Commission – Identity Theft
www.consumer.gov/idtheft/

US Department of Justice – Identity Theft & Fraud
www.usdoj.gov/criminal/fraud/websites/idtheft.html

Identity Theft Prevention and Survival
www.identitytheft.org/

Privacy Rights Clearinghouse - Identity Theft Resources
www.privacyrights.org/identity.htm

FTC -When Bad Things Happen to Your Good Name
http://www.ftc.gov/bcp/menus/consumers/data/idt.shtm

OTHER HELPFUL COMPUTER SECURITY SITES

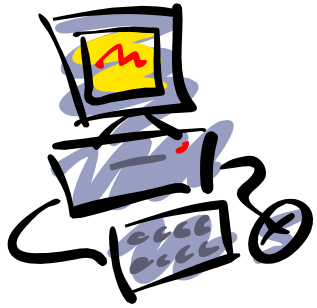
CERT Coordination Center – Home Computer Security
www.cert.org/homeusers/HomeComputerSecurity/

National Cyber Security Alliance Guide
www.staysafeonline.org/for-higher-education

Security Tools & Resources and Free Security Check Ups
www.staysafeonline.org/toold-resources

All comments, suggestions or questions should be sent to the
Department of Information Technology
helpdesk@jjay.cuny.edu
Phone (212) 237-8200
http://www.jjay.cuny.edu/doit

Be Safe Than Sorry!



A Guide to Protecting Your Computer and Your Identity

► How we can empower you?

Department of Information Technology
Office of Finance and Administration

JOHN JAY COLLEGE OF CRIMINAL JUSTICE

INFORMATION FOR JOHN JAY STUDENTS, FACULTY AND STAFF

Keeping our computers and networks safe from attack should not only be the responsibility of DoIT but also be the responsibility of all at John Jay. Similar to every computer-centric facility connected to the Internet, our college is continuously being scanned by hackers from all over the world looking for computers that are vulnerable to intrusion from outside. Once inside our system, these hackers can damage or steal private data, take control of the your system, use it to launch virus attacks, or simply harass you for fun.

Your computer is a popular target for these bad people. There are several reasons for this. They are looking for what is stored in there. They are looking for credit card numbers, bank account information, and anything else they can find. After stealing such information, intruders can use your money to buy stuff for themselves. Intruders are also looking for resources of your computer, e.g. your hard drive space, your speedy processor, and your network connection. They launch attacks onto other computers on the Internet using these resources. In fact, the more computers an intruder uses, the more difficult it is for law enforcement people to discover where the attack is really emanating. If intruders can not be located they can not be caught and prosecuted.

WHAT IS COMPUTER SECURITY?

It is important to know that even a brand new computer purchased today installed with a Windows Operating System can get infected or compromised within 30 seconds to 5 minutes of connecting to a network like ours.

The College's and CUNY's Internet Security Officers continually scans our network for compromised or infected computer systems. Any system identified as infected or compromised will immediately be taken off-line and lose access to the College's network. This is done not only to minimize the damage to the infected computer but also to protect the rest of the computers and network hardware on the network. Unless and until the system is clean and current with all critical updates and patches, access will not be given for such system.

Don't allow your computer to be infected or compromised and lose access to the College's network. You should make yourself aware of computer security risks and use protective measures to guard against them. Please try to be a good cyber citizen and do your part in securing your system. Make every effort to educate yourself on this issue. Remember awareness is the best defense against system vulnerabilities.

HOW TO PROTECT AGAINST VIRUSES?

Anti Virus Software is installed with latest updates: If you do not currently have Anti-Virus software please download it free from CUNY Portal e-Mall (http://portal.cuny.edu) and install it on your computer immediately. Using the remote update version of this software will ensure that it is kept up to date.

Operating system updates are installed: If you are using Windows operating system ensure that auto update is turned on. You can find instructions on how to do this under step 2 "Get Computer Updates" on the following page.

www.microsoft.com/athome/security/protect/

Open your e-mail attachments with utmost care: The most common way to spread a worm or a virus is through email attachments. When you receive an email with an attachment do not open any attachment you have not been expecting even if the email "appears" to have come from your acquaintance.
Just delete these messages. If it does come from one of your acquaintances, you should contact that person by calling or sending an email (by composing a new email, not replying to the email in question) to confirm that he/she really did indeed send you an attachment and it is not a virus. More information can be found at:

http://www.f-secure.com/virus-info/tips.shtml

MINIMIZE UNATHORIZED ACCESS TO YOUR ACCOUNTS OR COMPUTER

Never share your login ids and/or passwords

Remember you are responsible for any activities associated with your login ID and password.

Use strong passwords

1. Be creative

Do not use simple, obvious or predictable passwords such as names or nicknames of people, pets, places, or personal information that can be easily found out, such as your address, birthday or hobbies.

Do not use any word found in any dictionary

Use 8 to 16 characters – a minimum of 8 is best – that include at least one number and one special character

2. Protect your security codes and passwords

Do not share your passwords with anyone

Do not write down your passwords or store them on your computer

3. Always change the password provided by a vendor or other system provider

4. Change your password frequently —At least once every 90 days

If you think your password has been compromised, change it immediately

Don't reuse your previous passwords

Enable screen saver password protection

If you're concerned about others accessing your computer while you are away from your desk, you should enable your password protected screen saver.

Prevent sharing of hard disk

Believe it or not, your hard disk may very likely be wide open to those who'd like to use it as a server — sharing any files there or placing files on it to be accessible over the Internet. Windows actually makes it easy to share hard drives and printers over a network, a convenience and efficiency for those who need it.

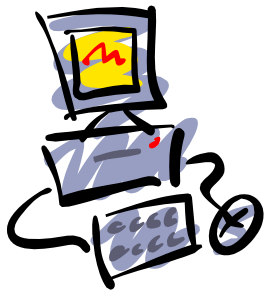
Limit the use of Administrative privileges on you computer

Do not allow your network administrator to map drive connections to other computers

CUNY INFORMATION SECURITY OFFICE

CUNY's Office of Information Security has made significant efforts in compiling additional information to protect your computer and your identity. Please visit http://security.cuny.edu site for this information.

Please see the back of the pamphlet for other helpful web pages related to computer security.



Be Safe Than Sorry!