

# **A GUIDE TO PROTECTING YOUR COMPUTER & PERSONAL INFORMATION**

## **WHAT YOU NEED TO KNOW?**

The Department of Information Technology (DoIT) is responsible for safeguarding John Jay computers and networks from security breaches. We at DoIT are proactive in protecting the college's computing assets with regular systems upgrades, software patches, anti-virus software, etc. However, if you install spurious software or applications such as games, music or videos either from an untrusted source on the Internet or from infected media such as a flash drive or CD your computer can get infected and become compromised.

Hackers who gain control of on campus computers then use them to further attack other computers or the entire network system of the College. In most cases the focus of these hackers is to extract confidential data they can use for financial gain. It is important that as a technology user at John Jay you understand the responsibility you share with DoIT to protect against this ever present threat.

## **SECURITY STARTS WITH YOU! DO YOUR PART!**

The most important component of good computer security for the John Jay Community is not a firewall or some network security device but your understanding of what risks exist and what you can do to safeguard yourself and others against them.

## **AWARENESS IS YOUR BEST DEFENSE! EDUCATE YOURSELF AND EDUCATE OTHERS!**

[WHY WORRY ABOUT COMPUTER SECURITY?](#)

[PROTECT AGAINST VIRUSES](#)

[MINIMIZE UNAUTHORIZED ACCESS TO YOUR ACCOUNTS OR COMPUTER](#)

[PROTECT AGAINST SPYWARE](#)

[PROTECT YOURS AND OTHER'S PRIVACY ONLINE](#)

[PROTECT YOURSELF AND OTHERS FROM IDENTITY THEFT](#)

[DATA SECURITY AT JOHN JAY](#)

[WHAT TO DO IF SECURITY PROBLEMS OCCUR?](#)

[CUNY INFORMATION SECURITY OFFICE](#)

[OTHER HELPFUL COMPUTER SECURITY SITES](#)

## **WHY WORRY ABOUT COMPUTER SECURITY?**

No computer is safe once it is connected to a network or the Internet. Unfortunately security risks to you and your computer can happen anytime - day or night, often time without your knowledge. When this occurs College and CUNY Internet Security Officers who continually watch our network for compromised computer systems and suspicious traffic are charged with removing the computers involved from the network.

This is done to minimize the risk to you and to protect the rest of the College community, computers and networks. When this happens before you can regain access to the network, your computer will be examined to ensure that confidential data was not compromised. Once this is done your computer will be scanned, cleaned, reinstalled and updated with virus definitions and patches. Only after all of this is done will you regain access to network based resources.

It goes without saying that incidents of this type and others not only lead to a considerable disruption in your access to technology services but may also result in a data breach and identity theft. The good news is that these situations are often avoidable if you take the time to learn about computer security risks and understand how to protect yourself and others.

## **PROTECT AGAINST VIRUSES**

- Ensure your computer has the most recent Anti-virus software installed:  
If you are on campus and do not believe you have Anti-Virus Software installed contact the helpdesk at (212) 237-8200 or [helpdesk@jjay.cuny.edu](mailto:helpdesk@jjay.cuny.edu). If you do not currently have Anti-Virus software at home the university provides a free copy to all faculty, staff and students. Anti-Virus Software can be downloaded from the CUNY Portal e-Mall (<http://portal.cuny.edu/>). Once installed be sure to update the definitions files and version of this software to ensure you are protected against the latest threats.
- Make sure your computer's operating system updates are installed:  
Updates fix new security holes found in a computer's operating system (i.e. Windows, Mac OSX, etc...) since it was installed. If you are using a Windows operating system, please make sure that auto update is turned on. You can find instructions on how to do this by clicking on "Keep Your Operating System Up-to-Date" under "Protect Your Computer" on the following web page. [www.microsoft.com/athome/security/protect/](http://www.microsoft.com/athome/security/protect/)
- Exercise Caution when opening your e-mail attachments:  
The most common way to spread a worm or a virus is through e-mail attachments. When you receive an e-mail with an attachment, do not automatically open it. If you have not been expecting this message and the content of the email seems suspicious even if the e-mail "appears" to have come from someone you know delete it immediately. More information related to email security can be found at: <http://www.f-secure.com/virus-info/tips.shtml>

## **MINIMIZE UNAUTHORIZED ACCESS TO YOUR ACCOUNTS OR COMPUTER**

- Never share your login ID:  
You are responsible for any activities associated with your login ID.
- 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. Always change the password provided by a vendor or other system provider, 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.

- Use strong passwords:  
Be creative. Make up your own word. 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. Use 8 to 16 characters including at least one number, one special character and combination of lower and upper case letters.
- Enable screen saver password protection:  
If you're concerned about others accessing your computer while you are away from your desk, you should enable a password protected screen saver. For Windows machines you can also hit control-alt-delete and lock your computer.
- Do not share your hard drive:  
Your hard drive can be configured to allow anyone on the network to have access to it as a server. Do not do this or allow others to do it. Do not share any files directly from your computer through Windows file sharing or make files directly accessible by the Internet via a sharing program. While Windows makes it easy to share files and printers over a network it compromises your computer's safety.

## PROTECT AGAINST SPYWARE

Spyware is software that collects personal information without your knowledge or permission. You might be the target of spyware if you download music or videos from file-sharing programs, free games from untrusted sites 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 more information on what it is, how it works and what you can do to prevent or get rid of it visit [microsoft.com/athome/security/spyware](http://microsoft.com/athome/security/spyware)

The following free tools are useful for finding and eliminating spyware:

1. **Spybot Search and Destroy**  
<http://www.safer-networking.org/en/download/index.html>
2. **Ad-aware (download)**  
<http://www.lavasoft.com/>

## PROTECT YOURS AND OTHER'S PRIVACY ONLINE:

When sitting at your computer "surfing the net", sending e-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. Educate yourself and others on the risks as well as the measures can be taken to protect online.

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

1. **Microsoft – Maintain Your Privacy**  
[www.microsoft.com/athome/security/privacy/](http://www.microsoft.com/athome/security/privacy/)

2. **EFF's - Top 12 Ways to Protect Your Online Privacy**  
[www.eff.org/Privacy/eff\\_privacy\\_top\\_12.html](http://www.eff.org/Privacy/eff_privacy_top_12.html)
3. **CDT's – Top 10 Ways to Protect Privacy Online**  
[www.cdt.org/issue/consumer-privacy](http://www.cdt.org/issue/consumer-privacy)
4. **BBB Online (Better Business Bureau) - Privacy Tips**  
[www.bbbonline.org/UnderstandingPrivacy/toolbox/tips.asp](http://www.bbbonline.org/UnderstandingPrivacy/toolbox/tips.asp)
5. **Microsoft – Chat and Messaging Safety**  
[www.microsoft.com/athome/security/chat/](http://www.microsoft.com/athome/security/chat/)

## PROTECT YOURSELF AND OTHERS FROM IDENTITY THEFT

Identity theft is one of the nation's fastest growing crimes. Only awareness safeguards you against identity theft. Identity thieves don't steal your money; they steal your name and reputation and use them for their own financial gain.

Visit the following web pages to learn more about identity theft and how to protect you, your friends and colleagues from it.

1. **Office of Inspector General**  
[www.ed.gov/about/offices/list/oig/misused/idtheft.html](http://www.ed.gov/about/offices/list/oig/misused/idtheft.html)
2. **Federal Trade Commission – Identity Theft**  
[www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/)
3. **U.S. Department of Justice – Identity Theft & Fraud**  
[www.stopfraud.gov](http://www.stopfraud.gov)
4. **Identity Theft Prevention and Survival**  
[www.identitytheft.org/](http://www.identitytheft.org/)
5. **Privacy Rights Clearinghouse - Identity Theft Resources**  
[www.privacyrights.org/identity.htm](http://www.privacyrights.org/identity.htm)
6. **FTC -When Bad Things Happen to Your Good Name**  
[www.ftc.gov/bcp/menus/consumer/data.shtm](http://www.ftc.gov/bcp/menus/consumer/data.shtm)

## DATA SECURITY AT JOHN JAY

1. Non-public University information such as SS#, grades, etc. must not be sent in email text, email attachments, and be left unencrypted on devices subject to theft or loss.
2. Encrypt all sensitive data on your computer using encryption software such as PGP.
3. Maintain access on a strict need to know basis and store non-public University information on a secure server rather than on end point devices such as desktop, laptop or flash drives.
4. Reports produced containing full social security numbers except where required for regulatory compliance requirements should be modified to include only the last four digits.
5. Strictly controlling access to SSNs, cleaning out old data, storing data with SSNs on secure file servers and using encryption where full SSN access is absolutely necessary also helps to reduce risk of public disclosure.
6. Lock your computer every time you leave your desk. Set up a screen saver with preset time out and password protection.

7. Backup your data regularly.
8. Be cautious when you print or copy sensitive non-public information — do not leave it in an open area and shred it when not in use.
9. Strictly follow CUNY security policies, procedures and advisories (<http://security.cuny.edu>), and report violations and issues when they occur to the IT department.
10. Don't give out your social security number to any college department unless it is absolutely necessary.

## WHAT TO DO IF SECURITY PROBLEMS OCCUR?

1. When using e-mail or other web services, you may encounter spam, phishing scams, obscene material, aggressive behavior or theft of your account or identity. When this occurs:
  - o Report immediately to the service (e.g. look for *Report Abuse* link or email *abuse@domain.edu*, etc.)
  - o Report immediately to John Jay IT department (DoIT)
2. If any sensitive non-public data has been compromised because of theft or loss of a computer or a laptop, portable device, breach of network security or through any other means try your best to minimize the damage and:
  - o Report it immediately to John Jay IT department (DoIT)
  - o Change all passwords immediately for network accesses and devices after they have been found
  - o For smartphones and PDAs, contact the service provider for help in wiping the data from the device. For college owned devices contact DoIT.

## CUNY INFORMATION SECURITY OFFICE

CUNY's Office of Information Security is continually working to better protect your computer and your identity. Please visit [security.cuny.edu/](http://security.cuny.edu) site for updated information on a regular basis. We highly recommend the security awareness course which is free for all CUNY faculty, staff and students.

## OTHER HELPFUL COMPUTER SECURITY SITES

1. **CERT Coordination Center – Home Computer Security**  
[www.cert.org/homeusers/HomeComputerSecurity/](http://www.cert.org/homeusers/HomeComputerSecurity/)
2. **National Cyber Security Alliance Beginners Guide**  
[www.staysafeonline.org/for-higher-education](http://www.staysafeonline.org/for-higher-education)
3. **Security Tips**  
[www.staysafeonline.org](http://www.staysafeonline.org)
4. **Cyber Security Test**  
[www.staysafeonline.org/tools-resources/free-security-check-ups](http://www.staysafeonline.org/tools-resources/free-security-check-ups)

If you have any comments, suggestions or questions, please contact the Department of Information Technology at [helpdesk@jjay.cuny.edu](mailto:helpdesk@jjay.cuny.edu) or call (212) 237-8200. Thank you!