**ADMINISTRATIVE COMPUTING SERVICES CENTER**

If you have any comments, suggestions

or questions, please contact the

Administrative Computing Services Center at

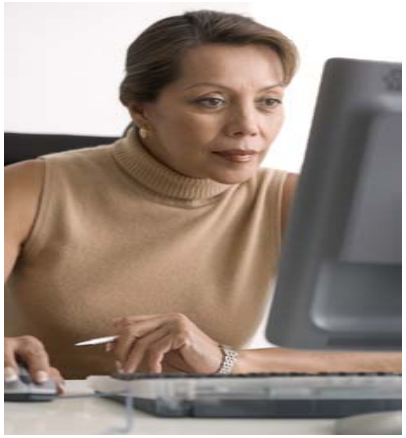
helpit@mec.cuny.edu or call **(718) 270-6262**

*"Creating Success, One Student At A Time."*

MEDGAR EVERS IS CUNY

# A GUIDE TO PROTECTING YOUR COMPUTER & YOUR IDENTITY

# @ MEDGAR EVERS



**Administrative Computing Services Center**

# A Guide to Protecting

# Your Computer & Your Identity

## Safeguarding Medgar Evers Computers and Networks

## Is Everyone's Responsibility!

### WHAT ALL MEDGAR EVERS FACULTY, STUDENTS AND STAFF NEED TO KNOW

The Department of Information Technology is responsible for safeguarding the Medgar Evers computers and networks from any security breach. However, hackers can attack any computer system at the College through the Internet or other means. As an end-user, you also share the responsibility of keeping our systems safe.

### WHY WORRY ABOUT COMPUTER SECURITY?

No computer is safe once it is connected to a network or the Internet.

Internet Security Officers at the College and CUNY continually scan our network for compromised or infected computer systems. If your computer becomes infected or compromised, you are likely to lose access to the College network.

This is done to minimize the damage to the infected computer and also to protect the rest of the College computers and networks. To regain access, your computer will have to be totally cleaned and reinstalled with the latest updates and patches.

Therefore, please take the time to learn about computer security risks and take these measures to protect your computer.

**Remember awareness is the best defense against**

**system vulnerabilities!!**

## CUNY INFORMATION SECURITY OFFICE

CUNY's Office of Information Security is continually working better to protect your computer and your identity.

Please visit:http://security.cuny.edu for updated information on a regular basis.

## OTHER HELPFUL COMPUTER SECURITY SITES

**CERT Coordination Center- Home Computer Security**

www.cert.org/homeusers/HomeComputerSecurity/

**National Cyber Security Alliance Beginners Guide**

www.staysafeonline.info/beginner.adp

**Security Tips**

www.staysafeonline.info/sectips.adp

**Cyber Security Test**

www.staysafeonline.info/selftest.adp

## PROTECT AGAINST VIRUSES

1. **Make sure your computer has the most recent Anti Virus software installed.**

- If you do not currently have Anti-Virus software, please download it free from CUNY Portal eMall (http://portal.cuny.edu) and install it on your computer immediately. Using the remote updated version of this software will ensure that it is kept current.

2. **Make sure your computer's operating system updates are installed.**

- If you are using 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/

3. **Exercise Caution when opening your e-mail attachments.**

- 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 the attachment if you have not been expecting it, even if the email "appears" to have come from someone you know. Just delete these messages.

- If the email comes from someone you know, call that person or send a NEW email to determine if this person sent you the attachment to ensure it is not a virus. More information can be found at:

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

## MINIMIZE UNAUTHORIZED ACCESS TO YOUR ACCOUNTS OR COMPUTER

**1. Never share your login IDs and/or passwords**

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

**2. 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 discovered, such as your address, birthday or hobbies.

- Use 8 to 16 characters including at least one number and one special character.

**3. 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.

## PROTECT YOURSELF FROM IDENTITY THEFT

Identity theft is one of the nation's fastest growing crimes. Being a student does not safeguard you against identity theft.

Identify thieves don't steal your money; they steal your name and reputation and use them for their own financial data.

As a student, you may even be more vulnerable to identify theft because of the way many students handle their personal data.

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

**Office of Inspector General**

www.ed.go/about/offices/list/oig/misused/idtheft.html

**Federal Trade Commission- Identity Theft**

www.consumer.gov/idtheft/

**U.S. Department of Justice- Identity Theft & Fraud**

www.usdoj.gov/criminal/fraud/idtheft.html

**Identity Theft Prevention and Survival**

www.identifytheft.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/online/pubs/credit/idtheft.htm

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

**Spybot Search and Destroy**

http://www.safer-networking.org/en/download/index.html

**Adware (download)**

http://www.lavasoft.com

## PROTECT YOUR PRIVACY ONLINE

When sitting at your computer "surfing the net," sending email messages, and participating in online forums, it is 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 on the risks as well as the measures you need to 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/

**EEF's- Top 12 Ways to Protect Your Online Privacy**

www.eff.org/Privacy/eff_privacy_top_12.html

**CDT's – Top 10 Ways to Protect Privacy Online**

www.cdt.org/privacy/guide/basic/topten.html

**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/

**4. 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.

**5. Prevent sharing of your hard drive**

- Believe it or not, your hard drive may be wide open to those who would like to use it as a server. Do not share any files or place files on your hard drives that are accessible by the Internet. Windows actually makes it easy to share hard drives and printers over a network. While it is an convenience and is efficient for those who need it, this compromises your computer's safety.

**6. Limit the use of administrative privileges on your computer**

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

## 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 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:
www.microsoft.com/athome/security/spyware