INFORMATION SECURITY THREATS

Identity theft • a form of stealing another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft can suffer adverse financial and criminal consequences if they are held accountable for the perpetrator's actions.

Keylogger • software that records everything you type while simultaneously sending it to a covert, remote listening agent.

Malware • a general term used to describe ***mal***icious soft***ware*** designed to trick a computer user or infiltrate or damage a computer.

Pharming • a hacker's attack aiming to redirect a website's traffic to fraudulent site, often used to mimic legitimate and authoritative sites (e.g. banking, anti-virus).

Phishing • deceptive attempt to acquire sensitive information (i. e. usernames, passwords, and credit card details) by an agent masquerading as a trustworthy entity in an email or instant message, or via a web site or telephone call.

Rootkit • a stealthy type of malicious software designed to hide the existence of certain processes or programs from normal methods of detection and enables continued privileged access to a computer, uses adaptive behavior to avoid detection and remediation.

Spam • the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. Basically junk email.

Spyware/ Adware • malware or marketing software whose principal aim is to surreptitiously collect information by "spying" on the user.

Trojan • disguised malware that appears to perform a benign or normal action but in fact performs a malicious action, such as transmitting a computer virus. Can appear to be a legitimate program or system resource.

Worm • self-replicating malware that can move from computer to computer on the network. Unlike a virus, it does not need to attach itself to an existing document or application. Worms almost always cause harm to the network, if only by consuming bandwidth.

Virus • self-replicating malware that attaches itself to a digital document or application, then spreads through copies of that document or application that are shared, frequently via email or USB drives. Viruses almost always corrupt or modify files.

FREE McAFEE ANTI-MALWARE SOFTWARE DOWNLOAD

http://www.cuny.edu/portal-login.html

Login to **CUNY Portal** > Click on **CUNY eMail** > **Software** > **McAfee Software** > **Start Shopping** > **More Software > McAfee VirusScan Enterprise** or **McAfee VirusScan for Mac**

The City College of New York

GUIDE TO PROTECTING YOUR COMPUTER & YOUR IDENTITY @ CCNY

FOR STUDENTS

Office of
Information Technology

September 2015

Email: ITSecurity@ccny.cuny.edu
Phone: Information Security x 5221

For more information visit the CCNY Information Security website:
https://www.ccny.cuny.edu/it/security

INFORMATION SECURITY • AN OVERVIEW

Network computing is an amazing phenomenon that is constantly redefining the way we interact with the world, whether at work or play, for collaboration or competition. Consider the many uses you make of your computer each day: sending and receiving email; browsing the Internet for work and leisure; using your bank card to make on-line, e-commerce purchases; social networking with colleagues, friends and family; filing confidential records (grades, financial records, medical claims).

If you're a typical network citizen, every day you use a small supercomputer to navigate mysterious internet "clouds" to exchange personal and professional information all the while leaving traces of every transaction on your computer, smart phone, flash drive and, very likely, hundreds of computers located throughout the world. All this data is vulnerable to malicious and opportunistic exploitation.

Information security has become part of all our lives. Each member of the City College community is responsible for the security and protection of electronic information resources over which he or she has control. This is especially true for social security numbers, drivers licenses or other government-issued identification, credit card numbers, userids with passwords, student records (i. e. GPAs, transcripts, grades, test results), and health records.

To minimize your risk of becoming a victim of identity theft, use the tips in this brochure as a guide to understanding threats and securing information on your computer and mobile devices.

Also, review the information we have prepared at the CCNY Information Security web site, which can be reached from the CCNY Web site, here:

https://www.ccny.cuny.edu/it/security

WHAT TO DO IF SECURITY PROBLEMS OCCUR?

If any sensitive non-public data has been compromised because of the theft or loss of a computer or a laptop, portable device, breach of network security or through any other means:

- Report it immediately to **ITSecurity@ccny.cuny.edu** or **x5221**
- Change all passwords immediately.

When using e-mail or other internet services, you may encounter spam, phishing scams, obscene material, aggressive behavior or theft of your account or identity. Learn how to detect vulnerabilities, avoid threats and safeguard your resources by taking CCNY's Information Security workshop offered throughout the academic year.

Be aware of other information security policies, procedures, and advisories that can be found on the CCNY IT Security web site:

https://www.ccny.cuny.edu/it/security_announcements

INFORMATION SECURITY TIPS TO E.L.U.D.E THREATS

Ⓔnvironmental Awareness

1. Physically secure your computer with security cables/plates; always lock building/office doors and windows when your workspace is unattended.
2. Never leave mobile devices unattended; thieves can steal your hardware & your identity.
3. Use discretion when logging onto and entering personal information into online resources: treat sensitive information like it could be there *permanently*, accessible to *everyone*.

Ⓛogins and Passwords

4. Use strong passwords that cannot be easily guessed or deciphered: at least eight characters including upper and lower case letters, numerals and symbols. Avoid using simple identifiers like common names, dictionary words, birthdates, and anniversaries. Never, ever share your password or login account!
5. Passwords are compromised all the time, so change your password at least every 90 days.
6. Always require a password to login to your computer, especially at start-up; use a screensaver to automatically password lock your unattended devices.
7. Use a generic user account for day-to-day tasks (browsing, email, working); only use administrative accounts for installing new software, updates and performing system maintenance.
8. Always log out of computer workstations, applications, social media and websites, even if you will only be away for moments.

Ⓤpdates and Upgrades

9. On all your devices, always check for and install updates and security patches before using software products—including operating systems, applications, browser plug-ins and add-ons; only use products that are currently maintained by their publisher.
10. Always use licensed and up-to-date malware protection to protect against attacks from malicious agents viruses, worms, zombies, and rootkits.
11. Obsolete programs contain security vulnerabilities; if you don't need it, delete it!

Ⓓata and Information Management

12. Exercise caution when opening unexpected or suspicious email messages or websites, which may contain malicious attachments or links that appear legitimate.
13. Classify and organize documents in order to minimize exposure of sensitive information (SSNs, financial records, credit card information, health records, etc.). If you don't need it, delete it!
14. Ensure critical backup files are encrypted and securely stored in safe, secure backup site. *Securely* delete unneeded data that contains confidential information, emptying the trash is not enough.

Ⓔncryption

1. Use file, folder and/or full disk encryption to protect all confidential data.
2. Before transmitting confidential data always ensure that data encryption protocols are in effect (e.g. HTTPS:// for websites and SSL/ TLS for file transfer).
3. Storage devices (hard disks, DVDs, USB drives, smart phones, network storage, etc.) containing confidential information (SSNs, financial, health, and academic records) must be securely overwritten or physically destroyed to prevent unauthorized disclosure.