GLOSSARY OF INFORMATION CYBER THREATS

Computer • device for storing and processing data according to instructions given to it in a program (e.g. laptop, desktop, mobile phone, game console, tablet, etc.).

Artificial intelligence (AI) • machine simulations of human intelligence that are programmed to think and act like humans, which can leverage all the following threats.

Bot • an automated software application that performs repetitive tasks over a network, many are designed with malicious intent.

Deep fake • using artificial intelligence to create fake but convincing audio or video of celebrities, political figures, and familiar people

Hacking • using a computer to gain unauthorized control of a computer or access to data often for fraudulent purposes.

Identity theft • the fraudulent acquisition and use of another person's private identifying information, usually for financial gain.

Keylogger • software that records every keystroke typed, sending it to a covert, remote listening agent; a stealthy way to steal userids and passwords.

Malware • a general term used to describe ***mal***icious soft***ware*** designed to trick a computer user or infiltrate a computer, stealthily transmitted by many vectors, including email, websites, social media, USB drives, texts, WiFi, advertising, browser plug-ins, and games.

Meta data • information collected from digital files and exchanged between computer systems that track user details, habits, and behavior that can be used to compromise privacy.

Pharming • an attack intended to redirect a website's traffic to fraudulent site, often used to mimic legitimate and authoritative sites (e.g. banks, anti-virus software, invoices).

Phishing • deceptive attempt to acquire sensitive information (i.e. usernames, passwords, and credit card details) by someone masquerading as a trustworthy entity; threat include email, instant messaging, web sites, social media, and telephone calls.

Ransomware • malicious software designed encode a user's documents using encryption and then demand a ransom to have those files restored.

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.

Software vulnerability • a flaw in software programming exploitable by malware and hacking; meticulous software management (including patches, updates, removal) reduces risk.

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.

Worm • self-replicating malware that can move from computer to computer. Unlike a virus, it does not need to attach itself to an existing document or application.

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.

Vishing scam • voice phishing uses a phone call to trick a victim into giving money or revealing personal information. The caller may pretend to represent a family member, legitimate company, government agency, or other trusted institution

The City College of New York

HOW TO ELUDE CYBERSECURITY THREATS @ CCNY

FOR STUDENTS

This guide highlights the importance of learning to protect your sensitive information and vulnerable technology from cyber threats in the workplace and the home using five cybersecurity principles to E.L.U.D.E. cyber threats:

- **E**nvironmental Awareness
- **L**ogins, Passwords, & Authentication
- **U**pdates & Upgrades (Hardware, Software, Security)
- **D**ata & Information Management
- **E**ncryption (Storage and Transmission)

Today a pandemic of cyber threats, augmented by the prowess of artificial intelligence, is constantly probing all our technology devices, social networks, and commercial services to exploit porous vulnerabilities.

By vigilantly adopting all the following common sense cybersecurity best practices – in combination with the layers of cybersecurity measures provided by the college and university – together you can help us protect our community from exploitation and fraud.

Office of Information Technology

August 2025

IT Security Office
Email: ITsecurity@ccny.cuny.edu
Phone: (212) 650-6565

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

PROTECTING YOUR INFORMATION AND YOUR FAMILY

As the internet and mobile devices proliferate, maintaining information security has become a vital part of all our lives. Of particular concern is guarding personally identifiable information (PII), which includes:

- Social Security numbers and birthdates
- Debit and credit card numbers
- Userids with passwords
- Student records (i.e. GPAs, transcripts, grades, test results)
- Financial records (i.e. tax information, bills, insurance records, payroll information)
- Health records
- Drivers Licenses or other government-issued identification
- Citizenship status

ADDITIONAL INFORMATION SECURITY RESOURCES

SANS Ouch! Information Security Newsletters and Podcast Free monthly security awareness resources produced by information security experts for a wide audience. Subscribe today!
https://www.sans.org/security-resources

CUNY Cybersecurity Awareness Training - This interactive program provides an overview of information security threats with best practices developed to keep your cyber-safe and secure. It takes approximately 45 minutes. **Login to CUNY Blackboard > select Organization**

CCNY Password Reset - reset your CCNY password for applications maintained by OIT, including CityMail student email, City Central Student Portal, CCNY Wifi network, library databases, and Tech Center resources. If you ever suspect your CCNY account has been compromised, use this utility to immediately reset your password! https://reset.ccny.cuny.edu

INSTALL AND UPDATE FREE ANTI-MALWARE SOFTWARE

A good way to defend against cyber threats is to install trusted anti malware software. Use the internet to search for and research trustworthy anti-malware products. **Reevaluate it annually!**

HOW DO I GUARD MYSELF FROM IDENTITY THEFT?

Identity theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain; victims can suffer adverse financial and criminal consequences. These resources provide information on understanding, avoiding, detecting, and reporting identity theft:

FTC Consumer Protection Information
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

FTC Identify Theft
https://identitytheft.gov/

To proactively prevent identity fraud (credit card, mobile phone accounts) request free annual credit reports from the following three credit reporting agencies. For a nominal fee you can also establish a "security freeze" for each of your family members. If you suspect identity theft, use these same agencies to request a free "fraud alert" or "extended fraud alert."

Equifax: http://www.equifax.com/CreditReportAssistance/ 1-888-766-0008
Experian: https://www.experian.com/fraud/center.html 1-888-397-3742
TransUnion: http://www.transunion.com/fraud-victim-resource/place-fraud-alert
1-800-680-7289

BEST PRACTICES TO E.L.U.D.E CYBERSECURITY THREATS

Ⓔ**nvironmental Awareness** of cyber threats, risks, and best practices is essential protection

1. Stay vigilant when using online resources (corporate accounts, email, social media, AI, etc.): treat sensitive information like it will be there *permanently*, accessible to *everyone*.
2. Disable online accounts and computer devices you no longer use.
3. When possible, physically secure your computer with security cables/plates; always lock building/office doors and windows when your devices are unattended.
4. Never leave mobile devices unattended; thieves can steal your hardware and identity.
5. Regularly check your accounts, billing statements, and credit reports for suspicious activity.

Ⓛ**ogins, Strong Passwords and Multifactor Authentication** should always be enabled

6. 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 words: common names, dictionary words, birthdates, and anniversaries. Use Password Managers!
7. Use a unique password with each account (with a password manager, if necessary).
8. Never, ever share your password or your account when logged in!
9. Passwords are compromised all the time, so change your password at least every 180 days
10. When available, configure your accounts to use two- or multi-factor authentication.
11. Always require a password to login to your computer, especially at computer start-up; use a screensaver to automatically password-lock your unattended devices.
12. Use a generic user account for daily tasks (browsing, email, working); only use administrative accounts for installing new software, updates and system maintenance.
13. Always log out of your computer workstations, applications, social media websites, even if you will only be away for moments.

Ⓤ**pdates and Upgrades** provide up-to-date protection against always evolving threats

14. On all your devices always check for and install critical 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 developer.
15. Always use up-to-date malware protection and firewalls to protect against cyberthreats.
16. Outdated programs contain security vulnerabilities; if you don't need it, delete it!

Ⓓ**ata and Information Management** organize and isolate sensitive information to avoid risk

17. Stay vigilant when opening unexpected or suspicious email messages or websites, which may contain malicious attachments or links that appear legitimate.
18. Classify and organize sensitive information to minimize exposure; never email or post it on public websites or email them. If you don't need it, delete it!
19. Backup critical data in scheduled intervals and store it in a safe, secure backup site.
20. Learn how to *securely* delete unneeded data that contains confidential information, emptying the trash is not enough.
21. Before disposing of storage devices containing sensitive information use a special program to securely delete data also consider physically destroying the hard drive/flash drive.

Ⓔ**ncryption** securely encodes data, scrambling it to make it resistant to hacks

22. Research how to use encryption tools (e.g. Microsoft Bitlocker, 7-Zip, Macintosh FileVault, OS X Disk Utility, VeraCrypt) to protect information stored on your devices.
23. Use layered file, folder, partition, and full disk encryption to protect confidential data.
24. Before transmitting confidential information always ensure data encryption protocols are in effect and secure (e.g. HTTPS:// for websites and SSL/ TLS for file transfer).