Carnegie Mellon

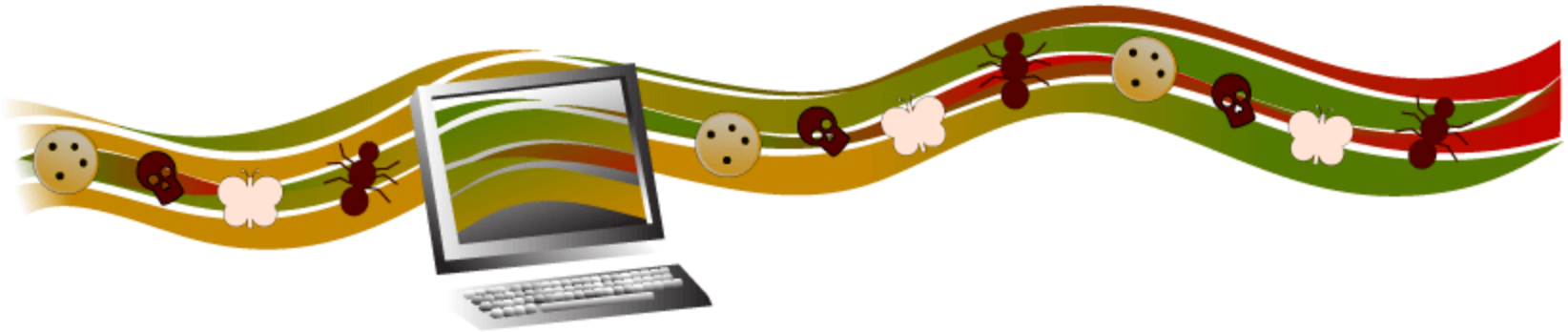
Cyber Security 101

Wiam Younes
Information Security Office
Computing Services
Carnegie Mellon University

What is Cyber Security?

Carnegie Mellon

Cyber Security is a set of principles and practices designed to safeguard your computing assets and online information against threats.



Why worry?

Carnegie Mellon

My role in cybersecurity!

Carnegie Mellon

End-users are the last line of defense. As an end-user, you;

1. Create and maintain password and passphrase
2. Manage your account and password
3. Secure your computer
4. Protect the data you are handling
5. Assess risky behavior online
6. Equip yourself with the knowledge of security guidelines, policies, and procedures

Security Threats

Carnegie Mellon

Intrusion – Unauthorized individuals trying to gain access to computer systems in order to steal information

Virus, Worm, Trojan Horse (Malware) – programs that infect your machine and carry malicious codes to destroy the data on your machine or allow an intruder to take control over your machine

Phishing – The practice of using email or fake website to lure the recipient in providing personal information

Spyware – software that sends information from your computer to a third party without your consent

Spam – programs designed to send a message to multiple users, mailing lists or email groups

Security risks

Carnegie Mellon

- Compromised Personally Identifiable Information (PII); *PII data refers to name, SSN, D. Licenses, bank accounts*
- Identity Theft- computer intruders intent on stealing your personal information to commit fraud or theft
- The use of unsecure settings of Peer to Peer File Sharing applications.
- Compromised computer; A computer experiencing unexpected and unexplainable
  - Disk activities
  - Performance degradation
  - Repeated login failure or connections to unfamiliar services
  - Third party complaint of a suspicious activity

Or a stolen or lost computer

Compromised machine or data?

Carnegie Mellon

Responding to a Compromised/Stolen Computer
http://www.cmu.edu/iso/governance/procedures/compromised-computer.html

Compromised - Reasonable suspicion of unauthorized interactive access

1. Disconnect From Network
2. Do NOT Turn Off
3. Do NOT Use/Modify
4. Contact ISO & Dept Admin
5. Preserve External Backups/Logs
6. Produce Backups/Logs/Machine ASAP For Investigation

Also report stolen computers

Security Measures

Carnegie Mellon

1. Safely mange your password
2. Safely manage your email account
3. Secure your computer
4. Protect the data you are handling
5. Avoid risky behavior online
6. Be aware of security guidelines, policies, and procedures

Safely manage your password

Carnegie Mellon

- Create and maintain a strong password
- Consider using a passphrase
- Avoid sharing your password with any one
- Avoid reusing the same password for multiple accounts
- Avoid storing your password where others can see it, or storing it electronically in an unencrypted format (e.g. a clear text file)
- Avoid reusing a password when changing an account password
- Do not use automatic logon functionality

Please refer to Carnegie Mellon guidelines for password management
http://www.cmu.edu/iso/governance/guidelines/password-management.html

Safely manage your email account

Carnegie Mellon

- All “university business” correspondence should be sent from an official CMU email address
- Avoid using personal accounts for business workflow
- Save personal messages in a designated folder
- Organize your email and files by project or work type
- Request additional file storage for projects with large number of files
- Avoid opening attachments from an untrusted source
- Avoid clicking on links in an email from an untrusted source
- Avoid providing your user ID and password or other confidential information in an email or in a response to an email
- Save copies of important outgoing email
- Be wary of email phishing scams

For more information on email account management, please visit Carnegie Mellon Computing Services, Accounts www.cmu.edu/computing/accounts

Secure your computer

Carnegie Mellon

- Lock your computer when not attended
- Log off or shutdown when going home
- Disconnect your computer from the wireless network when using a wired network
- Patch and update your operating system
- Install and update your anti-virus and anti-malware with the latest security definitions
- Create a unique user ID when sharing a computer with others
- Enable pop-up blocker on your browser
- Make an informed and rational decision prior to installing or downloading software on your computer
- Lock your office when you leave

Protect the data you are handling - 1

Carnegie Mellon

- Understand the type of data stored on your machine.
- Avoid storing personally identifiable information (PII) on local storage devices, e.g. laptop, USB, hand-held computers

  - Use Identity Finder to review, remove or redact PII data

  - Keep any PII data that you need for work process on a centrally managed, secure file system.
- Pay attention to the following when you have to email sensitive data:

  - Encrypt the data

  http://www.cmu.edu/computing/doc/security/encrypt/

  - Set password controls

  - Send the document password in a separate email

  - Ensure that the recipient has a need for the sensitive data

Protect the data you are handling - 2

Carnegie Mellon

- Back up your data regularly
- Be cautious when disposing data

  http://www.cmu.edu/iso/governance/guidelines/data-sanitization.html

  http://www.cmu.edu/iso/tools/data-sanitization-tools.html
- Segregate your personal files from your business files
- Organize your files by project or work type
- Make sure to securely delete data from systems before disposal when replacing or upgrading your computer.

To do so, please follow the ISO guidelines for Data Sanitization & Disposal at www.cmu.edu/iso/governance/guidelines/data-sanitization.html

Avoid risky behavior online

Carnegie Mellon

- Be wary of phishing scams
- Be cautious when handling attachments and links in email, chatrooms or instant messages (IM)
- Avoid responding to questions via pop-up windows, or click on links in a pop-up window
- Be cautious when using Peer to Peer File Sharing applications.

  www.cmu.edu/computing/doc/security/faqpeer.html

  www.cmu.edu/iso/aware/P2P/
- Be cautious when browsing the web. One spelling mistake can direct you to undesired websites

Guidelines

Carnegie Mellon

- Guidelines for Appropriate Use of Administrator Access
- Guidelines for Bulk Email Distribution
- Guidelines for Copyright Violations
- Guidelines for Data Sanitization and Disposal
- Guidelines for Instant Messaging Security and Usage
- Guidelines for Mobile Device Security and Usage
- Guidelines for Password Management
- Guidelines for Windows Administrator Accounts

http://www.cmu.edu/iso/governance/guidelines/index.html

Policies and Procedures

Carnegie Mellon

Please review the following polices and procedures:

- Information Security Policy
  http://www.cmu.edu/iso/governance/policies/information-security.html
- Carnegie Mellon Computing Policy
  http://www.cmu.edu/policies/documents/Computing.htm
- Procedure for Responding to a compromised computer
  http://www.cmu.edu/iso/governance/procedures/compromised-computer.html
- Procedure for Employee Separation
  http://www.cmu.edu/iso/governance/procedures/employee-separation.html
- Procedure for Requesting Access to Network Data and Research
  http://www.cmu.edu/iso/governance/procedures/net-data.html

Discussion

Carnegie Mellon

After reviewing the security measures for protecting the technology you use, revisit the questions presented at the beginning of the presentation:

1. How would you know whether an email sent to you with an attachment is free from viruses?
2. How do you secure sensitive data you send via email?
3. What steps would you take to secure your computer from malware?
4. What does the phrase“ safely manage your password” mean to you?

Questions?

Carnegie Mellon

Recourses

Carnegie Mellon

The Information Security Office; Training and Awareness

www.cmu.edu/iso/aware

- Guidelines for Data Classification
  www.cmu.edu/iso/governance/guidelines/data-classification
- Guidelines for Data Protection
  www.cmu.edu/iso/governance/guidelines/data-protection
- File Sharing and Digital Copyright
  http://www.cmu.edu/iso/aware/P2P/index.html
- Carnegie Mellon University Computing Services
  www.cmu.edu/computing
- Identity Finder
  www.cmu.edu/computing/software/all/identity
- Anti-Virus software
  www.cmu.edu/computing/software/all/symantec
- Operating Systems Support
  www.cmu.edu/computing/doc/os/terms.html
- Securing Your Web Browser
  http://www.us-cert.gov/reading_room/securing_browser/