What is Cyber Security?

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

Information Security Office (ISO)
Carnegie Mellon University
So, what does it mean?
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
<table>
<thead>
<tr>
<th>Security Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intrusion</strong> – Unauthorized individuals trying to gain access to computer systems in order to steal information</td>
</tr>
<tr>
<td><strong>Virus, Worm, Trojan Horse (Malware)</strong> – 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</td>
</tr>
<tr>
<td><strong>Phishing</strong> – The practice of using email or fake website to lure the recipient in providing personal information</td>
</tr>
<tr>
<td><strong>Spyware</strong> – software that sends information from your computer to a third party without your consent</td>
</tr>
<tr>
<td><strong>Spam</strong> – programs designed to send a message to multiple users, mailing lists or email groups</td>
</tr>
</tbody>
</table>
Security risks

• 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

Information Security Office (ISO)
Carnegie Mellon University
Impact on work

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

• 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

- 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

Information Security Office (ISO)
Carnegie Mellon University
Secure your computer

• 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

Information Security Office (ISO)
Carnegie Mellon University
Protect the data you are handling - 1

- 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
  - 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

- Back up your data regularly
- Be cautious when disposing data
- 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](http://www.cmu.edu/iso/governance/guidelines/data-sanitization.html)
Avoid risky behavior online

- 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

- Guidelines for Appropriate Use of Administrator Access
- Guidelines for Bulk Email Distribution
- Guidelines for Copyright Violations
- Guidelines for Data Sanitization and Disposal
- Guidelines for Data Protection
- Guidelines for Mobile Device Security and Usage
- Guidelines for Password Management
- Guidelines for E-Discovery and Litigation Hold

http://www.cmu.edu/iso/governance/guidelines/index.html
Please review the following policies 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
Identity Theft
Identity Theft is a crime in which an impostor obtains key pieces of personal identifying information (PII) such as Social Security Numbers and driver’s license numbers and uses them for their own personal gain.
PII – “Personally Identifiable Information”
How does it happen?

- Stolen wallet
  - Driver license ID
  - Credit cards
  - Debit cards
  - Bank accounts checks; last withdrawal banking statement
  - Health insurance
  - Auto registration and insurance card
  - Frequent flyer card
- Pilfered mail
- Computer virus
- Phishing and Social Engineering
  - Links to fraudulent web sites
  - Email
  - Phone call
  - Mail
- Social Networking account
- License plate
- Health records
- Financial Data

Information Security Office (ISO)
www.cmu.edu/iso
Identity Theft related crimes include

- Check fraud
- Credit card fraud
- Financial Identity Theft
- Criminal identity theft
- Governmental identity theft
- License plate number identity theft
- Mortgage fraud

Information Security Office (ISO)
www.cmu.edu/iso
Good and bad news

US Adult Identity Fraud
2003: 10.1 m
2007: 8.4 m

One year fraud amount
2006: 55.7 b
2007: 49.3 b

The mean per fraud victim
2006: 6,278
2007: 5,720

The mean for the resolution time per victim
2006: 40 hr
2007: 25 hr

Information Security Office (ISO)
www.cmu.edu/iso
The threat of identity theft hits close to home

This is my street. 1 out of every 33 people means someone on my street will have their identity stolen this year.
Protect yourself from Identity Theft

Protecting Yourself from Identity Theft
The following tips can help you lower your risk of becoming a victim:

1. Protect your Social Security number
2. Fight phishing - do not take the bait
3. Keep your identity from getting trashed
4. Control your personal financial information
5. Shield your computer from viruses and spyware
6. Click with caution
7. Check your bills and bank statements
8. Stop pre-approved credit offers
9. Ask questions
10. Check your credit reports - for free

*** - Adapted from the California Office of Privacy Protection - Top 10 Tips for Identity Theft Protection.

1. Protect your Social Security number

   Do not carry your Social Security card in your wallet.
   If your health plan (other than Medicare) or another card uses your Social Security number, ask the company for a different number.

   For more information, visit the Social Security website and read Identity Theft and Your Social Security Number.

2. Fight phishing - do not take the bait

   Scam artists phish for victims by pretending to be banks, stores or government agencies. They do this over the phone, in emails and through regular mail. Do not give out your personal information - unless you made the contact.

   Do not believe the number displayed by your phone's Caller ID as they can be easily faked (often calledishing). Instead, ask for your case or ticket number and tell them you will call them back. Then call the publicly listed number for the bank, store or government agency and tell them you are calling in reference to the case or ticket number.

   Do not respond to a request to verify your account number or password - unless you made the contact. Legitimate companies do not request this kind of information in this way.

Information Security Office(ISO)
www.cmu.edu/iso
Stolen Identity

If you suspect that you are a victim of identity theft;
http://www.cmu.edu/iso/aware/idtheft/notify/index.html

1. Report identity theft to your local police department
2. Contact the fraud hotline at the Social Security Administration (SSA), if your social security was stolen
3. Contact the fraud department of the three major credit bureaus
   - Equifax
   - Experian
   - Trans Union
4. Contact your creditors or bank when suspecting that your credit card, debit card or bank account is compromised.
What About Everyone Else?

1. We can help keep others safe from identity theft!

2. What happens when we don’t?
   - PA Breach of Personal Information Notification Act
   - What To Do If You Suspect A Breach
   - ISO Breach Handling Process

3. Proper Handling of Sensitive Data – How To Avoid Breaches
Common CMU Sources of Identity Data

- Old Class and Grade rosters
- Old Salary files
- Any Excel export file from central systems (e.g. HRIS, SIS, etc.)
- Shadow systems (e.g. local financial aid, admission applications, etc.)
- Research datasets
- Locally stored email
- Old backups & media
• Effective June 20, 2006

• Triggered when computerized “Personal Information” is compromised

• Notification must be made “without unreasonable delay”
• “Personal Information” = First name (or first initial) and Last name linked with one or more of:
  – Social Security Number
  – Driver’s License Number
  – Financial Account Number or Credit or Debit Card Number with any required access code or password in un-encrypted or un-redacted form

• Or if encrypted and the encryption is breached/involves a person with access to the encryption key
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
ISO Breach Handling Process

The ISO:
1. Confirm compromise, notifiable data, and likelihood of data breach (stolen laptop = data breach)
2. If data breach – proceed to notification

The ISO, the organization, & General Counsel’s Office:
3. Identify population and locate current contact info via alumni records
4. Draft & send notification letter and interface w/ law enforcement and consumer reporting agencies as required
5. Operate call center and respond to legal action
1. Know what data is stored on your personal computer

Run


Training video and material on how to install and run Identity Finder is available at

http://www.cmu.edu/iso/aware/id-finder/index.html
2. Delete or redact what you don’t absolutely need.

Identity Finder for Windows (Commercial)

Tools Matrix for Windows, Mac Unix
http://www.cmu.edu/computing/security/secure/tools/data-sanitization-tools.html
3. Don’t store it on your personal computer especially not on your laptop or home computer.

If you must store sensitive data, check with your departmental computing administrator about options to store it on a secured file server, one with robust access control mechanisms and encrypted transfer services.
4. If you must store it on your personal computer
   A. Follow the “Securing your Computer guidelines”
      http://www.cmu.edu/computing/documentation/secure_general/secure_general.html
   B. Password protect the file if possible
   C. Encrypt the file (Identity Finder’s Secure Zip, Computing Services, PGP Desktop or TrueCrypt)
      http://www.cmu.edu/computing/doc/security/encrypt/overview.html
      http://www.truecrypt.org/
4. If you must store it on your personal computer (cont.)

D. Only transmit via encrypted protocols (NOT Telnet, FTP, or Windows File Shares – instead use SCP and SFTP)

E. Reformat and/or destroy your hard drive before disposal or giving your computer to someone else
   http://www.cmu.edu/iso/governance/guidelines/data-sanitization.html

F. Secure delete it as soon as feasible
   http://www.cmu.edu/computing/security/secure/tools/data-sanitization-tools.html

G. Secure your backups and media
Thank you, and stay safe!

Questions, Concerns, Feedback?
iso@andrew.cmu.edu

A copy of the presentation is available at
http://www.cmu.edu/iso/aware/presentation/sec101-idtheft.pdf

Identity Finder Training material and video are available at
http://www.cmu.edu/iso/aware/id-finder/index.html

Practice Safe Computing
http://www.cmu.edu/iso/aware/pledge/index.html
Recourses

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
  http://www.cmu.edu/iso/aware/id-finder/index.html

• 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/

Information Security Office (ISO)
Carnegie Mellon University