How to… use your computer securely.

Top Ten Tips for Safer Computing

1. Install OS and 3rd party patches

It is critical to keep your software up-to-date

- Operating system
- Anti-virus and anti-spyware
- Applications including browsers, Adobe Acrobat, Java, Flash

Newest versions contain fixes for discovered vulnerabilities

Enable automatic update features in OS and application software

- Windows – Control Panel
- Mac OSX – System Preferences

2. Use current anti-virus, anti-spyware and firewall software

Anti-virus software

- "Used to identify and remove computer viruses, as well as many other types of harmful computer software, collectively referred to as malware" Wikipedia
- Offers ongoing protection, daily scans, daily updates

Anti-spyware software

- Protects your computer from malicious spyware.
    - Spyware may monitor your online activities and collect personal information while you surf the web.
- Periodically scans your computer for spyware.

Firewall Software

- Firewall software and/or hardware monitors the communications between your computer and the outside world (the Internet).
- Firewalls prevent unauthorized access to or from a private "network" (i.e., your home computer).
- You can implement a firewall in either hardware or software form, or a combination of both.

At Home – install Internet Security Packages

- Some commercial internet security packages include anti-virus, anti-software and firewall software.
- Norton, Trend Micro, McAfee, EEye, ESET, AVG
- To be effective virus definitions **must** be updated routinely.

3. Use strong, complex passwords

- At least one alphabetic, one numeric and one special character
- At least 7 characters long
- Mixed case
- Not similar to other passwords or your name
- Not found in the dictionary
- Choose a password that is difficult to guess
- Protect your password and do not share it

4. Lock your computer

- Lock your computer or handheld device while unattended and use a screen saver that is password protected.
- Windows XP Professional and Windows Vista, press **Ctrl+Alt+Delete**, and then click **Lock Computer**.

5. Backup important files

Maintain regular backups

- Use the TCU network drives assigned to you
- Keep your documents in a standard location
- Always be prepared to have your machine reformatted

Backup Data at Home

- Be prepared for the worst by backing up critical data and keeping backups in a separate, secure location.
    - Use supplemental hard drives, CDs/DVDs or flash drives
    - Backup data, files, pictures

6. Be aware of email security

Phishing

- Greet emails seeking personal information with skepticism.
- Be leery of alarming statements that urge you to respond immediately.
- Do not reply to phishing emails.
- Do not click on links in emails.

Spam

- Spam is anonymous, unsolicited junk email sent indiscriminately to huge numbers of recipients.
- Do not open email that is obviously spam.
- If you do open spam, do not click on any links.

Attachments

- Computer viruses and other malicious software are often spread through email attachments.
- If a file attached to an email contains a virus, it is often launched when you open (or double-click) the attachment.
- Don't open unexpected email attachments.

Links

- Approach links in an email with caution.
- They might look genuine, but they could be forged.
- Copy and paste the link to your web browser.
- Type in the address yourself.
- Or even Google the company and go to their website from the search results.

7. Don't install unknown or unsolicited programs on your computer

Cute games, utilities and other fun stuff are often used to disguise spyware/malware

- Spyware – software hidden inside more harmless software that at its most benign records information such as web sites visited or at its worse can do keystroke logging in order to steal your information.
- Malware – *malicious software* designed to infiltrate or damage a computer without the owners awareness or consent

8. Protect your private information

- Do not send sensitive personal information through email unencrypted.
- Make sure any web site that requests personal information uses SSL to encrypt your data
  - Look for https and lock displayed on web browser
- Watch out for Phishing emails that ask for personal or financial information

9. Maintain physical security of your computer

- Be aware of your surroundings
- Do not leave phones, laptops, handheld devices etc. unattended
- Lock your office when you leave
- Do not allow others to use your computer

10. Stay up-to-date and involved

Resources

- TCU Information Security Services web site:
  - https://security.tcu.edu
  - Alerts and Advisories
  - Digital Self Defense
  - Information on Digital Copyright
  - Policies and Procedures
  - All the tools and knowledge you need to use the Internet safely and protect yourself and others from online threats.
- US-CERT web site http://www.us-cert.gov

Help

- TCU Computer Help Desk
  - 817-257-6855
  - Help@tcu.edu
  - http://Help.tcu.edu
  - Location: Mary Couts Burnett Library, first floor
- Information Security Services
  - https://Security.tcu.edu
  - Security@tcu.edu