How to…
Protect Your Computer @ Home

Critical Patches

- Keep 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

Anti-Virus Software

- Anti-virus software is “used to identify and remove computer viruses, as well as many other types of harmful computer software, collectively referred to as malware” Wikipedia
- Anti-virus software offers ongoing protection, daily scans, daily updates.
- To be effective virus definitions must be updated routinely.
- Norton, Trend Micro, McAfee, AVG, eEye, also included in internet security packages.

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.
- Must also be kept up-to-date
- Ad-Adware, Spybot, also included in internet security packages

Internet Firewall

- Anti-virus and anti-spyware products inspect files on your computer, in incoming and outgoing email, and on removable media.
- 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.
- Hardware Firewall
  - Router (wired or wireless), i.e., Linksys
  - DSL Modem, Gateway
- Software Firewall
  - Built-in Windows Firewall
  - Only stops inbound traffic, does not check outbound
  - Mac OSX 10.2 and later also has an built-in firewall
  - Part of an internet security package

Internet Security Packages

- Some commercial internet security packages include anti-virus, anti-spyware and firewall software.
- Norton, Trend Micro, McAfee, EEye, ESET, AVG

Email Security

Phishing

- Phishing is an illegal activity that uses social engineering techniques to manipulate people into giving out personal information and sending money.
- A highly targeted version of a phishing scam is "spear phishing."
- Characteristics of phishing emails
    - Unsolicited request for personal information
        - Username, userid, email id, email identity
        - Password
        - Social security number
        - Birthdate
    - Generic greetings
    - Contains an ultimatum
    - Grammatical errors
    - Content appears genuine
- Protect yourself from phishing
    - Watch out for links in emails.
        - Do not click on them
        - Type the link directly into web browser
    - Learn to spot non-legitimate web sites
    - Look at the address between the // and the first / - it should end with the company you expect
        - Fake: http://**www.1025.ru**/js/mail.tcu.edu
        - Real: https://**mobile.tcu.edu**/owa/auth/logon.aspx…
    - Is it secure?
        - https in the address
        - Yellow lock icon
    - Greet emails seeking personal information or money with skepticism.
    - Be leery of alarming statements that urge you to respond immediately.
    - Do not reply to phishing emails.
    - TCU Technology Resources, including the computer help desk and information security services will NEVER ask you for your password via email, the phone or in person.
    - When TCU upgrades its computer or email systems we will NEVER send a link inside an email which will go to a website requesting that you login or enter your username and password.

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.

Backup Your Computer

- 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

Use Strong Passwords

- Strong 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
- Test your passwords: http://www.passwordmeter.com/

Wireless Security

- Change the administrator username and password on your wireless hardware.
- Use WPA2 encryption to secure communication between your computer and your wireless access point.
- Change the Default SSID (default name of the your wireless network – i.e., Linksys devices are normally "linksys")
- Run setup wizard that comes with wireless router.

Etcetera

- Rename Administrator account and set a complex password and use a non-administrative account for normal day-to-day work.
- Supervise Children
    - Teach computer security
    - Use monitoring software
- Turn off computer when not using it
    - Warning – if off for weeks it won't get updates. Force updates when you turn it back on.
- Use Firefox instead of Internet Explorer
    - Turn on Master Password
- Beware of freeware or shareware – it may be spyware

- If you need to access the TCU network from home, use VPN with Remote Desktop (Windows) or Screensharing (Mac)
- When getting rid of an old computer, even if the hard drive is broken, drill holes through it.
- Beware of public computer access
    - Wireless hotspots – not secure, don't require encryption.
        - You may want to use TCU VPN.
    - Kiosks or public computers – not secure, key logging software may be installed.

Resources

TCU Computer Help Desk – 817-257-6855
Help@tcu.edu – http://help.tcu.edu

Information Security Services
Security@tcu.edu - https://security.tcu.edu