CSCC Information Security

Session II: Safe Computing

Topics Covered

- Anti-Virus and Spyware
- Spam/Phishing
- Protection methods
- Patching
- Encryption
- Software demonstrations
- Where to learn more

Anti-Virus and Spyware

- Spyware
  - Collects information without the user's knowledge
  - Attempts to hide from the user
  - Does not usually self-replicate
- Most infections come from unpatched software and web-based infection methods. Avoid using Internet Explorer if you can.
- Beware of fake security and other dialog boxes when web browsing
  - Most glaring, attention grabbing pop-ups that say your computer is infected are malware

Anti-Virus and Spyware continued

- Be very cautious about installing freeware and software from unknown companies. If in doubt, ask Assist.
- Use reputable sites like download.com
- Keep Windows firewall active
- Avoid add-on toolbars in your web browser
  - Google and Yahoo toolbars are safe, but aren't generally necessary
  - Other tool bars may be collecting information about your browsing habits
- Google poisoning
  - Common with breaking news stories (Haiti, Samoan earthquakes)
- Use common sense

Spam

- Be suspicious of email attachments
  - Only open attachments that you're expecting
  - Use common sense when evaluating whether an attachment is legitimate
  - If in doubt, call or email the sender and confirm they sent the attachment
- Use cautions with links in emails, IMs, etc.
  - Look carefully at links and hover over them to ensure you know where they're going
  - If in doubt, type the link into your browser manually or use a bookmarked link to the site
  - http://www.unc.edu

Phishing

- Common features:
  - Forged From: address
  - Content looks legitimate
  - Usually accompanied by a threat or urgent warning
  - Attempt to have the user click on a link or send sensitive information via email or IM
- Spear Phishing
- Whaling
- Vishing

Phishing continued

- We will NEVER ask for account information
- Never click on links in emails requesting personal information
- Never click on links you receive in unsolicited email. Copy and paste them into your browser
- If in doubt, ask an Assist staff member
- Pay attention to scam alerts in browsers and email clients
- Be wary of greeting card scams around the holidays

Social Networking

- Facebook
  - Increasing numbers of scammers are migrating to Facebook
  - Beware when giving applications access to your information
  - Know the privacy settings of Facebook and don’t give up too much information
- Twitter
  - Shortened URLs can hide malicious links

Signs of Spyware

- You are subjected to endless pop-up windows
- You are redirected to web sites other than the one you typed into your browser
- New, unexpected toolbars appear in your web browser
- New, unexpected icons appear in the task tray at the bottom of your screen

Signs of Spyware continued

- Your browser's home page suddenly changed
- The search engine your browser opens when you click "search" has been changed
- Certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form)
- Random Windows error messages begin to appear
- Your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.)

Software (free!)

- Spybot Search & Destroy
  - http://www.safer-networking.org/en/download/
  - Does not scan automatically
- MalwareBytes
  - http://www.malwarebytes.org/mbam-download.php
  - Does not scan automatically

Patching

- Make sure Windows automatic updates are turned on
  - Assist has enabled it on all our workstations
  - Restart as soon as possible when patches are applied
- Always say yes when applications (Adobe, Java, iTunes) ask to apply updates.
- Set applications to check for updates and apply them automatically
- Keep your Symantec anti-virus client updated!

Encryption

- Locknote
  - simple, but sending .exe files over email is problematic.
  - http://www.steganos.com/us/products/for-free/locknote/overview/
- KeePass
  - Version 1.x and 2.x available. We're using 1.x; 2.x may be better for home use
  - http://keepass.info/
- Winzip
  - Strong (AES) encryption added in version 9.0
  - http://www.winzip.com
- 7-Zip
  - Free alternative to Winzip with AES encryption support
  - http://7-zip.org/

Encryption continued

- PGP Whole Disk Encryption
  - Available to the CSCC from ITS
  - Will be deployed on all checkout laptops
  - Will be installed on laptops “storing, accessing, processing” sensitive information.
    - storing/processing comes first
  - No plans for desktop deployment at this time
    - licenses are limited
    - desktops should not have sensitive information

More information

- UNC Security FAQ:
  - http://its.unc.edu/InfoSecurity/faq/index.htm
- UNC Quick Tips:
  - http://help.unc.edu/6404
- US-CERT Cyber Security Tips:
  - http://www.us-cert.gov/cas/tips/