Computing Security
@ Carnegie Mellon University

John K. Lerchey
Information Security Office
lerchey@andrew.cmu.edu
Start with the Basics

• Patching
• Antivirus and anti-malware software
• Strong passwords
• Be aware of Theft
  – (Computer, Account)
• Back up your data
• Read our Policies and Guidelines
• Take advantage of our tools:
  – Identity Finder, Anti-Phishing Phil, Anti-Phishing Phyllis, ISO Patch-Check
What’s infecting the Campus now

- **Fake A/V** – fake antivirus that ties up the system with pop-ups, sometimes installs backdoors or other malware.
- **Zbot/Zeus** - acquired from phish messages, causes spamming, steals banking credentials.
- **Torpig** – identity stealer, reboots the computer, lodges in the MBR, hidden.
Why are computers getting compromised?

- Unpatched Java, Adobe Reader and Adobe Flash.
- Rotating web-ads are often involved.
- Downloading exploits with P2P.
- Clicking on e-mail objects.
- Clicking on pop-up windows
- Passing around infected USBs.
• CMU is a big target (reputation).
• People **inside** are always trying out new hacker tools on this network.
• People from other countries want your credentials to get Library/other resources.
• 51% of students participating in a phish study fell for phishing attempts on day one (IDtheft study, 4/2009).
A Few Words About Phishing…

• Computing Services will NEVER ask for your password
• Notices from Computing Services will always come from a valid Carnegie Mellon email address
• General announcements can be verified at:
  http:www.cmu.edu/computing/news
What ISO Sees

• Signatures, flows, logs.
• Only the most egregious stuff, and not all of it.
• Events and incidents reported to us.
• We pay much more attention to administrative systems.
What you can do

• Take advantage of the antivirus/anti-malware software on Computing Services’s site:
  http://www.cmu.edu/computing/software/all/index.html

• Take advantage of the ISO Patch-Check tool
  https://www.cmu.edu/iso/patch-check/

• Follow the polices and guidelines

• Be careful with “course software” and projects

• Register your computer with the CMU Police
  http://www.cmu.edu/police/programsandservices/crime-prevention.html
Questions?

Information Security Office (ISO)
iso@andrew.cmu.edu
www.cmu.edu/iso
Computing Services Help Center: 412-268-4357