



Computing Security
@
Carnegie Mellon University

Allison MacFarlan
Information Security
Engineer

&

Wiam Younes
Training and Awareness
Coordinator

Five Computing Security Tips

Carnegie Mellon®



- Patching
- Antivirus and anti-malware software
- Strong passwords
- Back up your data
- Be aware of Theft – your computer, your account
- Read our Policies and Guidelines
- Take advantage of our tools: Identity Finder, Anti-Phishing Phil

What's infecting the Campus now

Carnegie Mellon®

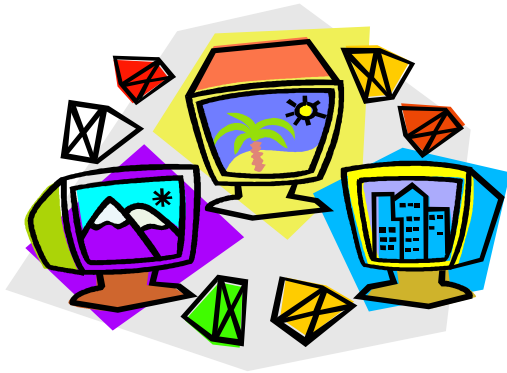
- Zeus – acquired from phish messages, causes spamming, steals banking credentials.
- Gozi – Russian mafia, sets up proxy, connects to botnet, banking.
- Torpig – identity stealer, reboots the computer, lodges in the MBR, hidden.



Why are computers getting compromised?

Carnegie Mellon®

- Unpatched Adobe products and java.
- Facebook involved 50% of the time.
- Downloading exploits with P2P.
- Clicking on e-mail objects.
- 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 Tepper students participating in a phish study fell for phishing attempts on day one (IDtheft study, 4/2009).

- Bring your computer to the bathroom. It will be stolen from the Library.
- Register your computer and bike with the CMU Police

<http://www.cmu.edu/police/programsandservices/crime-prevention.html>

- **BACK YOUR DATA UP REGULARLY.**



- Big network: 10 GB core, via PSC/3ROX and two Commodity Feeds.
- Two public Class Bs plus a few misc. slivers for .org and remote sites. SEI walled off.
- Five kerberos realms, seven AFS cells.
- Depending on the day, between 45,000 and 60,000 devices.

- Signatures, flows, logs.
- Only the most egregious stuff, and not all of it.
- What people report to us.
- We pay much more attention to administrative systems.

- Take advantage of the antivirus/anti-malware software on Computing Services's site

<http://www.cmu.edu/computing/software/all/index.html>

- Act like you're going to graduate school at a Hacker conference.





Information Security Office (ISO)

iso@andrew.cmu.edu

www.cmu.edu/iso

412-268-4357