A presentation by Albert Wang
Systems Administrator Lead
SHASS Dean's Office
4/9/2013

Safe Computing @MIT

What everyone needs to know

Email

- Important: MIT will *NEVER* ask you for your password, nor will MIT send you email requesting your password or other confidential information.
  Please delete all email messages that request such information. They are social engineering scams designed to steal your information.
- These social engineering scams are called “PHISHing”.
- The above applies to telephone calls as well.
  (telemarketing, Nigerian 419, phishing, 809 scam, etc)

Spam

- **Spam** is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media.
- MIT Anti-Spam Resources: http://ist.mit.edu/spam
- Exchange users get Spam Quarantine: https://mailsec-cc.mit.edu/brightmail/
- Authenticate with your kerberos username and password.

Attachments

- Never open attachments from people you don't know.
- Never open attachments from people you do know but weren't expecting an attachment from.
- Attachments (some examples: pdf, doc, jpg, exe, zip, gzip) are used as Trojan horses by bad people to deliver bad stuff like viruses, malware, and root kits.
- If in doubt, email the sender to verify the attachment is legit.

Bad Stuff

- Viruses- A computer virus is a computer program that can replicate itself and spread from one computer to another.
- Malware- Short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
- Rootkit- A stealthy type of software, often malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Free software

- Everybody loves the idea of free software.
- The only problem is the bad guys know this.
- The guise of free software is another common delivery device for bad stuff (malware, viruses, and rootkits).
- Free software is the most common delivery vehicle for Mac bad stuff. So if your Mac asks you if you want to open or install any application you aren't sure about, always say no.

Safe ‘free’ software

- Legitimate shareware and freeware do exist, but Google them if you’re not familiar to verify their authenticity. See what people are talking about.
- Anything published on CNET.com and available for download is safe.
- Some very good anti-malware and anti-virus programs are free and safe.
- When in doubt, ask either Dan or myself.

Anti-Bad Stuff software

- Have one or two that you use. Even if it's McAfee.
- Great free options. (Spybot S&D, Super AntiSpyware, Malwarebytes, AVG for PC) (ClamXAV, Avast!, Sophos Anti-Virus for Mac)
- Update it. Use it once in a while.
- IS&T has replaced McAfee with Sophos. Everyone should remove McAfee and download and install Sophos.

Passwords

- According to the password management company SplashData, here are the 25 most common passwords of 2012, along with the change in rank from last year.

- 1. **password** (Unchanged) 2. **123456** (Unchanged) 3. **12345678** (Unchanged) 4. **abc123** (Up 1) 5. **qwerty** (Down 1) 6. **monkey** (Unchanged) 7. **letmein** (Up 1) 8. **dragon** (Up 2) 9. **111111** (Up 3) 10. **baseball** (Up 1) 11. **iloveyou** (Up 2) 12. **trustno1** (Down 3) 13. **1234567** (Down 6) 14. **sunshine** (Up 1) 15. **master** (Down 1) 16. **123123** (Up 4) 17. **welcome** (New) 18. **shadow** (Up 1) 19. **ashley** (Down 3) 20. **football** (Up 5) 21. **jesus** (New) 22. **michael** (Up 2) 23. **ninja** (New) 24. **mustang** (New) 25. **password1** (New)

What is a good password?

- Eight characters or longer.
- Mixed case (lower and upper case letters), with a number, and a symbol.
- Something you'll easily remember.
- Ideally no words that can be found in a dictionary.
- Eg. M@rv1nth3m@rt1an, D@44ydvck!, Tru3B100d, G@m3ofThr0n3s

Storing passwords

- Never send or store passwords in email.
- Many of us have more than 1, 2 or even 3 passwords for different accounts in our daily lives.
- If you have a lot of passwords, you can store the passwords in an encrypted file or use a management system like LastPass, 1Password, KeePass.
- Don't keep passwords under your keyboard or written down on a piece of paper in your office.

Software Updates

- General rule is to do your Windows or Mac OS X operating system updates a week or two after they come out. This gives the company time to work out any bugs.
- If you use MITSIS here at MIT be careful not to do any JAVA updates. Otherwise, do the JAVA updates.
- Office Updates are generally always safe. It's ok to do those when they come out.
- Always do Flash and Adobe Reader PDF updates.

Sensitive Data

- Massachusetts state law requires MIT safeguard all sensitive data. (Names, social security numbers, addresses, date of birth, credit card info, etc)
- If you use a laptop to access or store sensitive data, the laptop needs to be encrypted.
- We must securely erase all machines that have handled or stored sensitive data once the area is done using it.
- Identity Finder is available from the IS&T website.

Knowledge

- Knowledge is power.
- The more you learn from talking to us, your web searches, and personal investigations, the better you will be able to discern what is legit and what isn't and protect yourself against bad people and criminals.
- Don't be afraid to ask questions. There are no dumb questions.

Protect your stuff

- Your data is the most important thing on your computer.
- Have backups. All Mac users should be using Time Machine. PC Users should be using Windows Backup. Both of these programs require an external HD to work.
- Remember, only you can prevent data loss.