Data Safety 101

Dean Halter

21 Mar 2001

Personal Data

Assets

Intellectual Property

Computers

Vulnerabilities

Safeguards

Hacker

Loss

Malicious Web Site

Threats

Theft

IT Compliance Regulations

- Family Educational Rights and Privacy Act (FERPA)
- The Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Higher Education Opportunity Act (HEOA)
- FTC Red Flag Rules
- Copyright Laws – DMCA, etc.
- Communications Assistance for Law Enforcement Act (CALEA)
- 40+ Individual State Breach Notification Laws

- Breach Statistics –
  - http://www.privacyrights.org/data-breach#CP
  - http://www.adamdodge.com/esi/

#1 Administrator versus User Permissions

- Administrators can install software and maintain the computer; ~70% of attacks would not work against standard user account
- Set a strong password on an administrator account, just in case
- Create and use a user account for day to day stuff
- Upgrade to Windows Vista or 7 and use User Access Control (UAC) for short.

#2 Passwords

- How long would it take to crack your password?
  - http://www.lockdown.co.uk/?pg=combi
- Create a good Password
- Test your password strength
  - https://www.microsoft.com/security/pc-security/password-checker.aspx
- Don’ts:
  - Don’t use automatic logon
  - Don’t put your password on a Post-it note, in your drawer, etc.

#3 Antivirus

- Make sure you are getting the latest signature files
- Periodically perform a full scan
- Microsoft Security Essentials is a good free version for home use.
- Periodically check the quarantine and logs to see what it's taken care of for you automatically or what others may have run into.

#4 Firewall

- Different types – Enterprise, Home Wi-Fi, Personal Computer
- Your computer is like a house with lots of doors and windows that bad guys could come in. Firewalls close the entrances unless you explicitly want them open.
- Visit GRC ShieldsUP! to see what ports, if any, you have open.

#5 Patches – Windows Operating System and Office Suite

- Configure your computer to automatically update
- Periodically check for patches manually – visit http://update.microsoft.com if you're using Windows XP or select "Windows Update" from your list of programs and tell it to "Check online for updates from Microsoft Update"

#6 Patches – 3rd Party Applications

- 3rd party applications like iTunes and Adobe Reader have become the biggest threat
- Use the FileHippo.com Update Checker to check for updates to these

#7 Removable Media

- Disable Autorun

- Encryption
  - IronKey USB Flash Drives
  - Western Digital My Passport External Hard Drives
  - TrueCrypt software encryption

- UDit's Next Step – Checkpoint Full Disk Encryption for all UD owned laptops.

#8 Find SSNs

- Do you know what's on your computer and removable media?
  - Cornell Spider
- Do you really need sensitive information on your machine? If not, delete it.

#9 Browsing the Web

- Make sure you are using the latest version of your browser of choice – Internet Explorer, Firefox, Chrome
- Never save passwords for important sites
- Make sure you see a lock icon and https:// whenever dealing with sensitive information
- Don’t ever let a web site convince you that your machine has a virus and you need to download their software to fix it. Don’t trust the buttons; click the little ‘x’ icon in the top right corner of the dialog and then restart your web browser

#10 Spam

- Social Engineering – Bad guys taking the attack right to the end user and not just by email – phone, USB flash drives, etc.
- If possible, delete email from folks you don't know
- Don't be too quick to open attachments
- Verify web links. What's wrong with the following:
  - https://chase.com
  - http://www.udayton.edu/
- FTC is the government agency for addressing SPAM. They've got a lot of good information at http://www.ftc.gov/bcp/edu/microsites/spam/consumer.htm

Conclusion

- UD employs a layered, defense in depth strategy. User is a part of that because our program is only as strong as the weakest link in the chain.

- If you have any questions, contact UDit. Nothing's too trivial; we are asked to verify email and explain security settings almost everyday.

- Resources
  - http://community.udayton.edu/provost/it/policies/security.php
  - http://community.udayton.edu/provost/it/policies/index.php

  - http://isc.sans.edu/index.html
  - http://technet.microsoft.com/en-us/security/default
  - http://www.h-online.com/security/