Everything you ~~need~~, ~~should~~ ~~could~~, ~~would want~~….. to know about data security.

Steve Scott

University of Utah

Information Security Office

How about "a few things that are important to know about data security"

This is just an introduction!

Topics – in no particular order

- Passwords
- Use your password
- Back up your data
- Automatic updates
- Phishing and personal information
- Antivirus protection and other tools
- Peer to Peer
- Protecting sensitive data
- A few miscellaneous things
- Why do we worry about these things? Identity theft!
- Q and A

Please ask questions!

Passwords

- Often viewed as a hassle.
- It is your first line of defense!
- Constant reminder that security is important.
- What are you trying to protect?
- Examples of bad and good passwords.

Lock your screen/password protect your computer!

- Now that you’ve created that awesome password make sure that you use it.
- Don’t leave an account without a password.
- Lock your screen when you get up and walk away.

Back up your data!

- My hard drive crashed and I lost….

a. All of my iTUNEs.
b. All of my family pictures.
c. All of my homework.
d. All of my financial data.

- It is recoverable for a cost…..

Use the autoupdate feature of your operating system of choice

- Microsoft had six critical vulnerabilities on the last “patch Tuesday”.
- There are already exploits being used against some of these “holes”.
- All Operating Systems need updates!
- Worms and the cost of not patching.

Update software

- Software needs to be updated!
- Browsers.
- Office suites.
- Media players….

Phishing expeditions and personal data

- Don’t give out any personal information, even if it looks legitimate.
- If you have a question, call the bank/credit union.
- Beware of phone calls too.
- Postal mail.

Website Data -- Know what information is out there about you

- E-mail address? Do you get SPAM?
- Do a web search.

Virus protection

- Should be on all computers, no exceptions.
- Updated daily, even hourly.
- Scan e-mails and downloads automatically and scan entire hard drive weekly.
- Don’t turn off.
- New viruses have “backdoors”.
- Your computer becomes part of a “botnet”.

Other “malware”

- Spyware.
- Firewalls.
- Spam filters.
- Email client configuration.
- 60,000 different “threats” in Symantec’s database.

Peer to Peer file sharing

- Neat, I can get movies, music and software for free!
- Not so neat, the DMCA is suing me, and my computer is hacked…..

Sensitive data

- Do you have it?
- Do you know where it is?
- Do you do your taxes with a computer?
- Do you shop online?
- Make sure it’s protected by considering all of the things that have been mentioned so far.

Other things to consider….

- Wireless networks.
- Shared computers.
- Cable, DSL and other connections.
- Email and chat are unencrypted.
- Other devices like PDAs and cell phones.
- Appropriate use…..

Appropriate use of U resources, and of the Internet

Policy

- PPM1-15 Information Resources Policy.
- Other ISPs have Acceptable use policies.

PPM 1-15

"The University of Utah makes available Information Resources which may be used by University students, faculty, staff and others. **These resources are intended to be used for educational purposes and the legitimate business of the University and in a manner consistent with the public trust**. Appropriate use of the resources includes instruction, independent study, authorized research, independent research and the official work of the offices, departments, recognized student and campus organizations of the University."

More PPM 1-15

“**Access to computer systems and/or networks owned or operated by the University of Utah imposes responsibilities and obligations on its Users**. Access is granted subject to University and Board of Regents policies, and local, state, and federal laws. Appropriate use is ethical, reflects academic honesty, and shows restraint in the utilization of shared resources. Appropriate use is consistent with intellectual property rights, ownership of data, system security mechanisms, and rights to privacy and to freedom from intimidation, harassment, and annoyance.”

Even more PPM 1-15….

“No computer security system can absolutely prevent a determined person from accessing stored information that he/she is not authorized to access.”

Why do we try and stay secure? Identity theft!

- So what happens if you’ve been a security aware user and someone else loses your data?
- Assume that it’s already happened…..
- www.freecreditreport.com

How Common Is Identity Theft?

- Top consumer fraud complaint.
- The fastest-growing crime.
- Estimated 10 million victims last year.
- A recent FTC survey shows 12.7 percent of respondents had discovered a misuse of personal information in the last 5 years.
- 1 in 50 people have had identity theft issues, 1 in 20 has had fraudulent use of credit.

More reasons to stay secure…

- Costs to industry.
- Lost work time.
- Botnets.

Resources

- http://www.it.utah.edu/leadership/security
- http://www.sans.org/newsletters/ouch/
- http://www.ftc.gov/infosecurity/
- http://www.staysafeonline.info/

Questions?