Data Protection and Privacy

Brad Miller
UND IT Security Officer
What will we cover?

- Why protect data?
- What data needs to be protected?
- What can I do to protect data?
- Securing your operating system (Windows XP and Windows 7) and common applications
- Protecting your personal information when using the Internet
- Some “must-have” security software
- Encrypting sensitive data
- Backing up your sensitive data
Why should I protect data?

- Because we have a legal responsibility - HIPAA, GLB, FERPA
- Because we have an “ethical” obligation – protecting the personal information of students, faculty, and staff is important
- Because the reputation of the University may be at stake
- Because there may be financial costs to the University
- Because failure to protect research data and intellectual property could endanger grants
- Because your personal information is important
What data needs to be protected?

- **Private and Confidential University Information**
  - **NDUS Data Classification and Information Technology Security Standard**
  - **Private** – Employee/Student ID, birth dates, gender, ethnicity, citizenship, grades, etc.
  - **Confidential** – SSNs, legal investigations, sealed bids, intellectual property, health records, passwords, etc.

- **Private and Confidential Personal Information**
  - SSN, credit cards, drivers license number, birth date, financial information, tax forms, medical information, browsing history, etc.
What can I do to protect data?

- Foster a security-minded culture
- Stop collecting and storing data unnecessarily
- Store data on servers (not workstations)
- Identify and remove all unnecessary files from your computer and server, especially those that contain SSNs, credit card #s, drivers license #s, or other such information, if no longer required
  - Cornell’s Spider
  - Identity Finder
- Protect the paper documents
- Restrict access to sensitive data
- Report potential compromise of sensitive data
What can I do to protect data? (con’t)

- Understand Email Security
  - Do not send sensitive data via email
  - Be suspicious of attachments
  - Don’t fall prey to phishing attempts
- Stop using P2P
- Use good passwords
- Turn off computer when not in use
- Protect your information and your computer
  - Antivirus
  - Automatic updates
  - Personal firewall
  - Anti-Spyware
  - Encryption
  - Backup your data
Securing your operating system

- Enable Automatic updates
- Rename Administrator account – leave the existing admin account as decoy (strong password/disabled)
- Disable and assign a strong password to or remove Guest account
- Turn off file sharing
- Use a password protected screensaver
Secure web browsing

- Consider Using Firefox/Chrome
- Secure IE
  - Upgrade to latest version of IE if possible
- Look for https://
- Use McAfee SiteAdvisor
- Use WOT (Web of Trust)
Protecting your personal information online

IE – Safety and Security
- Protected mode
- Tracking protection
- In-private browsing
- ActiveX filtering

Avoid phishing scams
- Microsoft’s phishing filter
- Firefox phishing protection
“Must-have” Security Software

- **Antivirus/ AntiSpyware**
  - UND-owned – Microsoft Forefront Endpoint Protection
  - Personally-owned – Microsoft Security Essentials
  - Malwarebytes
  - AdAware
  - Spybot S&D

- **Personal Firewall**
  - Windows Firewall
  - ZoneAlarm (free for home use)

- **Password Safe**

- **Office Inspect Document**
Encrypting Sensitive Data

- What is encryption?
- Why encrypt data?
- Some encryption tools:
  - Microsoft Office Encryption
  - GNU PG for Windows
  - TrueCrypt
Backup your data

- Why backup data?
- Backup tool:
  - Windows Backup Utility
Questions?