Cybersecurity Awareness Month

Computer and Data Security

Security is everyone's responsibility!

October 2015

Presented to New Mexico Public Procurement Association
Carlos S. Lobato, CISSP, CISA
IT Compliance Officer at NMSU

Why do we need security?

- To protect our important data from being stolen or compromised.
- To comply with regulatory requirements (if applicable to your institution, local government, company, etc.

What is sensitive data?

It is information that is protected against unwarranted disclosure through the establishment and practice of regulations and policies.

Examples of Sensitive Data

- **Personally Identifiable Information:**
  - Social Security Numbers, Human Resource Information, Health Information
- **Financial Information:**
  - Credit Card Numbers, Loan Information, Bank Account Information

Data Privacy/Security Regulations

- **FERPA** - *Family Educational Rights and Privacy Act*
  Protects the privacy of student data

- **HIPAA** - *Health Insurance Portability and Accountability Act*
  Protects the privacy of protected health information

- **GLBA** - *The Gramm-Leach-Bliley Act*
  - Requires a Written Information Security Program
  - Protects nonpublic data typically financial

- **RFR** - *Red Flags Rule*
  The FTC requires identity theft prevention

- **FISMA** - *Federal Information Security Management Act*
  Requires proper protection and security of data

- **PCI DSS** - *Payment Card Industry Data Security Standard*
  Protects credit card information

Data Security

Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or institutional data.

- **Encryption is one way of ensuring digital/computer data security as it scrambles data into unreadable text.**

Secure Your Data

- Encrypt your computers using whole disc encryption.
  - BitLocker for Windows 7 and up
  - Apple's built-in encryption FileVault
- Encrypt your files (Word, Excel, PDF, etc.)
  - Password Encryption

Example: Excel, Word and PDF

- Use encryption on flash drives
  - BitLocker To Go
  - Built-in encryption

Safe Computing practices

- Secure your area
- Secure your computer
- Keep up-to-date
- Set strong passwords
- Discussion on safe computing practices by topic

Secure your area

- Secure equipment and data before leaving an area unattended.
- Physically lock down laptops and workstations when possible.
- Close down your browser after visiting a web site with sensitive data.
- Enable password protected screen saver (screen locker) and log off when you step away.
- Do not leave sensitive papers or data on printers or fax machines. Ensure printing to the correct printer.

Secure your computer

- Enable the computer's firewall before you connect to the internet
- Disable automatic login
- Do not install or open unknown programs or files.
- Control access to folders
- Password-protect your screen saver and set it to start after five minutes of inactivity.
- Shut-off your computer at the end of your work day unless needed to leave on for updates or backups.
- Ensure your computer is enrolled in your department's domain.

Keep up-to-date

- Turn on Automatic Updates for the:
  - Operating System
  - Browser
  - Application Software
  - Antivirus Client and Definitions

Set strong passwords

- Construct good passwords with:
  - A minimum of 8 characters, and
  - A combination of upper and lower case letters, numbers and special characters.

The Password Meter

- Protect your password.
  - Do not share your password with others. Your password should be considered like your toothbrush.
  - Do not write down or post your password.

Don’ts of Security

- Don’t save sensitive data locally to your computer unless absolutely necessary.
- Don’t share your sensitive data with others.
- Don’t throw reports or printouts that have sensitive data in the trash without shredding them first. Hackers do DumpsterDiving
- Don’t click on links or inquiries through e-mail known as phishing attacks.
- Be cautious - Don’t install a network printer in your office
- Be cautious - Don’t install a wireless access point

Discussion by Topic

- Malware
- Phishing
- Mobile Devices
- Social Media Guidelines
- Passwords
- Other

For more information, visit:

- Windows Security
  - Microsoft Security Center
- Mac Security
  - Apple Security (Mac, iMac, iPhone, etc.)
  - 4 Mac Security Options Everyone Should Know
- Safe computing and online browsing
  - Stay Safe Online
- OnGuardOnline.gov

Q & A

Carlos S. Lobato, CISA, CIA, CISSP, CPA
IT Compliance Officer
NMSU ICT – IT Compliance Function
clobato@nmsu.edu
http://compliance.ict.nmsu.edu/
646-5902
Thank you for your time!