Information Security

BCUG
May 21, 2013

UNIVERSITY OF NEBRASKA–LINCOLN

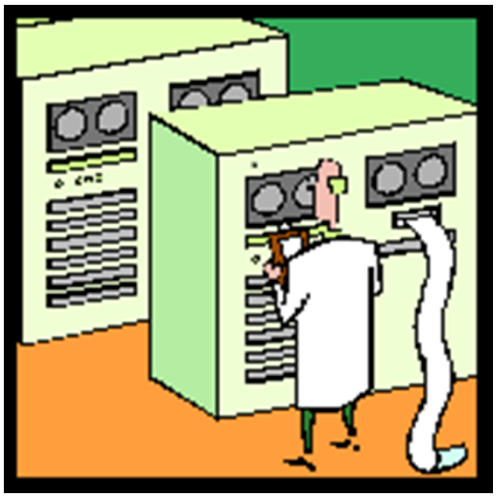
Rene Mayo-Rejai

IT Auditor
Operations Analysis
OA.UNL.EDU

What is Information Security?

The Practice of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction regardless of form (electronic, physical, etc…)

Information Security
10 Years ago



Computer Rooms

Desk

Physical Computers

Information Security Now

Information Security Focus

- Physical
  - Computer Rooms
  - Offices
  - Workstations
  - Mobile Devices
  - Sensory (Visual, Hearing)

- Logical
  - User IDs/Passwords
  - Appropriate Access
  - Email

Regulations and Policies

- FERPA (Family Educational Rights and Privacy Act)
- PCI (Payment Card Industry)
- PII (Personally Identifiable Information)
- Digital Millennium Copyright Act of 1998
- University of Nebraska Executive Memorandum 16 (Policy for Responsible Use)
- University of Nebraska Executive Memorandum 26 – Gramm Leach Bliley Compliance (Safeguards to Protect Covered Data and Information)

Information Impacted

- Original Source
  - Campus Mainframe
  - Campus Servers (Department Applications)
  - Departmental Workstations (sensory)
- Downloaded Data (Databases, Spreadsheets, Reports)
  - Departmental Servers
  - Departmental Workstations (sensory and hard drive)
- Email
  - Body of Email
  - Attachments containing Data

Ways to Protect Information

- Work with Minimum Required for Job
  - Risk Reduction
- User ID/Passwords
- Server Physical Location
- Screen Position – Screen Locking
- Security of Mobil Devices with Access (Email and Network)
- Data Storage Considerations
  - Workstation vs. Server
  - Data Classification

Ways to Protect Information

- VPN on Non-Secure Wireless Connections
- Verbal discussion of Protected Data
  - Phones, Hallways, Break Areas
- Review Business Processes
  - Employee Checklist
    - Application and Network Access Removal
- Education

Training Available at UNL

- SANS Security Awareness Training
  - 32 Modules each are 2-5 minutes in Length
  - Security.unl.edu/video-training
  - Complete the Request Access form
  - More Information on Modules: https://www.securingthehuman.org/media/resources/pdfs/security-awareness-brochure.pdf

Language

English

Change Password>

Manual>

Contact Support

You have completed 32 of 32 modules

< Back to Library

Introduction Completed	You Are The Target Completed	Social Engineering Completed	Email and IM Completed
Browsing Completed	Social Networking Completed	Mobile Devices Completed	Passwords Completed
Encryption Completed	Data Protection Completed	Data Destruction Completed	Wi-Fi Security Completed
Working Remotely Completed	Insider Threat Completed	Help Desk Completed	IT Staff Completed
Physical Security Completed	Protecting Your Personal Computer Completed	Protecting Your Home Network Completed	Protecting Your Kids Online Completed
Hacked Completed	Senior Leadership Completed	PCI DSS Completed	FERPA Completed
HIPAA Completed	PII Completed	Criminal Justice Completed	Federal Tax Information Completed
Gramm Leach Bliley - EDU Completed	Gramm Leach Bliley - FIN Completed	Ethics Completed	END Completed

Security Awareness Modules

MODULE: You Are A Target **TIME:** 2:09 minutes

Employees often believe they are not a target, exposing your organization to tremendous risk. This module addresses that misconception by explaining how they are under attack and why. In addition, we explain that that this training will not only protect them at work but at home. This engages people, helping ensure the success of your organization's security awareness program.

MODULE: Social Engineering **TIME:** 3:03 minutes

Many of today's most common cyber attacks are based on social engineering. As such, we explain what social engineering is, how attackers fool people and what to look out for. We then demonstrate several common social engineering attacks, including a non-technical and technical example. We finish how people can detect these attacks and how to respond to them.

MODULE: Email & Instant Messaging **TIME:** 5:30 minutes

One of the primary means of attacks and exploitation is through email. Email is used for both simple, large scale attacks and more targeted spear phishing attacks. We explain how these attacks work, including recent examples of phishing, spear phishing, malicious attachments and links, and scams. We then explain how to detect these attacks, how to respond to them, and how to use both email and IM securely.

MODULE: Browsing **TIME:** 3:10 minutes

The browser has become the gateway to the Internet; it is the primary tool that employees use for online activity. As such, browsers (and their plugins) have become a common target for attackers. We teach people about these attacks and how to browse safely, including keeping the browser and plugins updated, avoiding bad neighborhoods, and being careful of and scanning what they download.

MODULE: Social Networking **TIME:** 5:04 minutes

Sites such as Facebook, Twitter and LinkedIn have exploded in popularity, with employees and managers sharing all sorts of private information, not only about themselves but about their work. Cyber attackers know this and use this information for identity theft, spreading malware, scams and even targeted attacks. We discuss these risks and the steps your employees can take to protect themselves and your organization.

MODULE: Mobile Device Security **TIME:** 3:25 minutes

Today's mobile devices are extremely powerful, including tablets and smartphones. In most cases these devices have the same functionality, complexity and risks of a computer, but with the additional risk of being highly mobile and easy to lose. We cover how to use mobile devices safely and how to protect the data on them.

Website: http://www.securingthehuman.org

Email: info@securingthehuman.org

Information Security Management

- Ongoing – business and technology changes
- Minimize Risks
  - Likelihood of something bad happening
- Minimize Vulnerabilities
  - Weakness to information asset
- Minimize Threats
  - Manmade potential to cause harm

WHAT CAN YOU DO TO HELP PROTECT UNIVERSITY INFORMATION?

Thank You!

Rene Mayo-Rejai
IT Auditor
RMayoRejai2@unl.edu
472-6288

OA.UNL.EDU