

Information Systems Security Awareness



What Is Information Systems Security?

- Protection of information and information systems
- Protection of information from unauthorized users accessing or modifying information
- Insurance that information systems are available to authorized users

2

What Is Information Systems Security?

- A secure information system maintains:
 - **Confidentiality**
 - Safeguards information from being accessed by individuals without proper clearance, access level or need to know
 - **Integrity**
 - Protects availability and information stored from being modified or destroyed

3

What is Information Systems Security?

– Availability

- Information services are accessible when needed



As an authorized user, you are also responsible for contributing to the security of all computer systems you have access to in your daily work routine

4

Why Information Systems Security Awareness Training?

- To provide Information Systems Security Awareness Training and functional training **before** system users are allowed access to the system
- To help system users become familiar with using the system's security features and understand their responsibilities and security procedures for protecting any sensitive information they manage

5

Why Information Systems Security Awareness Training?

- After initial training, refresher security training will be required annually
- Each user (including contractors) must be versed in acceptable rules of behavior before being allowed access to the system
- They should also be able to identify a computer security incident

6

Why Information Systems Security Awareness Training?

- Agencies should develop an Information Systems Security Program to implement and maintain the most cost-effective safeguards to protect against deliberate or inadvertent acts, including:

7

Why Information Systems Security Awareness Training?

- Unauthorized disclosure of sensitive information or manipulation of data
- Denial of service or decrease in reliability of critical information system (IS) assets
- Unauthorized use of systems resources
- Theft or destruction of systems assets
- Fraud, embezzlement, or misuse of resources and assets

8

Threats to Information Systems Security

Information Systems Security Threat vs. Vulnerability

Threat
vs.
Vulnerability

14

Threats

• Two types of threats can affect information systems security

– *Environmental*

– *Human*

15

Environmental Threats

• Environmental

– Natural Environmental

• Lightning, fires, hurricanes, tornadoes, floods

– System Environmental

• Poor building wiring or insufficient cooling for the system

16

Human Threats

- Human
 - Internal
 - Malicious or disgruntled user
 - User recruited by terrorist groups or foreign countries
 - Self-inflicted unintentional damage—accident or bad habit
 - External
 - Hackers, terrorist groups, foreign countries or protesters

17

Social Engineering

- Phishing is a high-tech scam that uses:
 - *Email*
 - *Cell phone*
 - *Websites*
- Tricks you into disclosing personal sensitive information
- Legitimate companies do not ask for personal information via email

18

Social Engineering

- Social engineering is a hacking technique that relies on human nature

19

TIPS

Don't

- Do not give out passwords
- Do not give out employee information
- Do not follow commands from unverified sources
- Do not distribute dial in phone numbers to any computer system except to valid users
- Do not participate in telephone surveys

Do

- Use caller ID to document phone #
- Take detailed notes
- Get person's name/position
- Report incidents

20



Internet

Internet Browsing Security Risks

- Cookies
- Mobile Code
- Peer 2 Peer
- Malicious Code
- Hoaxes

28

Cookies

- Cookies
 - Text file stored by a web server
 - Retrieved when web site is revisited
- Security problems
 - Saved unencrypted personal information for future business with that site
 - Can track activities on the web

29

Cookies

- Browser should be set to not accept cookies
- Contact your help desk or system administrator for further assistance in dealing with cookies

30

Mobile Code

- Scripting languages used for internal applications
 - ActiveX
 - Java
- Mobile code embedded in a web page that can recognize and respond to user events
 - Mouse clicks, form input, and page navigation

31

Peer-to-Peer (P2P)

- File sharing applications that enable computers connected to the internet to transfer files between computers (i.e. Morpheus and BitTorrent)
- Creates risk and enables possibility of a security breach, in addition to legal and ethical concerns

32

Peer-to-Peer (P2P)

- Common avenue for spreading viruses and spyware
- Increases your agency's vulnerability by providing outsiders a link into its' network system and information
- Can compromise network configurations

33

What is Malicious Code?

- Software or firmware intended to perform an unauthorized process which adversely impacts an information system
- Examples of malicious codes:
 - Viruses, Trojan horses, worms

34

Malicious Code

- Spread through email attachments, downloading files from the internet and visiting web sites
- It's your responsibility to scan all outside files using current anti-virus software

35

Malicious Code

- Email messages and attachments, provide a common route to transfer malicious code
- Use caution with opening email attachments
 - Malicious code can corrupt files, erase computer hard drive or enable hackers to gain access to your computer

36

Malicious Code

- Attachments to look for which might contain malicious code
 - Those ending in *.exe*, *.com*, *.vbs*, *.bat* and *.shs*
- Don't assume attachments are safe because a friend or coworker sent it

37

Preventing Malicious Code

- Scan email attachments and outside files using current anti-virus software
- Set your system to scan daily

38

Preventing Malicious Code

- Delete email from unknown or unexpected sources—do not open
- Turn off option to automatically download attachments

39

Reacting to Malicious Code

- System acting erratically, running much slower
 - You may have a virus
 - Viruses can remain hidden for months and appear later to infect your system

40

Hoaxes

- Email messages designed to influence you to forward message to everyone you know
- Encourages forwarding by warning of new viruses, promote moneymaking schemes, or citing fictitious causes

41

Hoaxes

- Encourages mass distribution and causes clog networks and slows down internet and email services
- If you receive one do not forward

42

User Role and Responsibilities

- As an authorized user of the WIC information systems you have certain responsibilities when using WIC computers
- Rights to privacy are limited
- Any activity conducted on a WIC computers can be monitored
- Anytime you login to a WIC system you consent to being monitored
- Use your computer for WIC business only—avoid misuse

43

User Role and Responsibilities

•Examples of misuse are:

- Viewing or downloading pornography
- Internet gambling
- Conducting private commercial business activities or profit making ventures
- Loading personal software or making unauthorized configuration changes

44

User Role and Responsibilities

There are eight basic generally accepted ethical guidelines for using WIC computer systems

1. Do not use computer for harm
2. Do not interfere with other's work
3. Do not snoop in other's files
4. Do not use a computer to commit crimes

45

User Role and Responsibilities

5. Do not use or copy unlicensed software
6. Do not steal intellectual property
7. Do not use computer to pose as someone else
8. Do not use computer resources without approval

46

Appropriate Email Use

Appropriate Email Use

- Email is for official business use
- Some incidental and casual use of email is permitted

56

Appropriate Email Use

- Guidelines for personal email use
 - May not adversely affect performance of official duties
 - Must not reflect poorly on WIC

57

Appropriate Email Use

- May not be used to send pornographic, racist, sexist or otherwise offensive emails
- May not be used to send chain letters or sell anything
- Email use must not overburden the system (i.e. mass emails)

58

Appropriate Email Use

- Do not forward jokes, pictures or inspirational stories
- Avoid using Reply All unless absolutely necessary

59

Appropriate Email Use

- Per Local Agency, personal use may be authorized if it is of reasonable duration and frequency—preferably on employees' personal time (lunch or break)
- Permitted when it serves a legitimate public interest (allowing job search in response to downsizing)

60

Secure Passwords

Secure Passwords

- Tips for creating a secure password
 - Password should be a mixture of lower and upper case letters, numbers, and special characters
 - Use methods such as alphanumeric combinations or phrase associations to create easy for you to remember, hard for others to guess

66

Secure Passwords

- Tips for creating a secure password
 - Memorize password refrain from writing it down
 - Never share with others
 - Change password regularly

67

Secure Passwords

- Tips for creating a secure password
 - Avoid words or phrases that can be found in a dictionary in any language
 - Don't use personal information like names or birthdays of family members, pets or favorite sports team

68

Physical Security

Physical Security

- Physical security includes protection of the entire facility
 - Outside perimeter to offices inside the building including all information systems and infrastructure
- You are responsible for knowing your organization's physical security policies and following them

72

Physical Security

- Procedures should exist for:
 - Gaining entry
 - Securing work area at night
 - Emergency procedures

73

Physical Security

- Procedures may include:
 - Use of badge or key code for entry

 - Locking your cubicle undocking laptops and storing in a separate location

 - Locking data storage devices
 - Hard drives, and thumb drives

74

Physical Security

- Ensure others follow your organization's physical security policies

- Challenge people who
 - Attempt to tailgate or allow others to do so
 - Don't display badges or passes

- If you're the last to leave, check to ensure others have secured their equipment properly

75

Inventory Control

- WIC Local Agencies are responsible for controlling their inventory of office and computer equipment
- Sign for property receive and ensure it doesn't get lost or stolen

76

Inventory Control

- If property is lost or stolen, follow agencies procedures for reporting loss
- In addition, you must report loss of information stored on equipment and significance of lost information

77

Tracking Inventory Examples

Inventory Control List	
Telephones	57
Desktop Computers	256
Laptop computers	108
Fax Machines	20
Printers	50

Sign-out sheet
Laptop computer
Serial # 1234567-08
Signed out to <u>John Smith</u>
Signature _____

Property Pass
<u>John Smith</u> has permission to take laptop computer, serial # 1234567-08, out of the building.
Jane Doe Property Manager
Signature _____

78

Telework

Telework Procedures

- Telework is known as telecommuting
- Advances in computer and telecommunications capabilities make telework increasingly practical
- Risks associated with remote access to your agencies computer network

86

Backups, Storage and Labeling

Backups, Storage, and Labeling

- Large amount of data is stored on removable media (CD's thumb drives, pen drives, or removable hard drives)
- Take extra precaution to protect from loss or theft

88

Backups, Storage, and Labeling

- Backup files on a regular basis and store in a secure location—this will minimize loss of data if hard drive crashes or infected by virus
- Store all removal media in solid storage containers, such as metal cabinets to protect against fire and water damage

89

Backups, Storage, and Labeling

- Label all removable media including backups, and the contents of the media to reflect classification or sensitivity level
- Removable media must be properly marked and stored according to appropriate security classification of information it contains

90

Backups, Storage, and Labeling

- When info on removable media is no longer needed, do not erase or sanitize the information
- Removable media must be degaussed or destroyed if not reused at the same or higher classification level

91

Media Devices

Media Devices

- Information stored or transmitted on devices other than computer must be protected according to its classification or sensitivity level

97

Media Devices

- Cell Phones
 - merely transmitters
 - Use a landline for more privacy
 - Never discuss sensitive information on an unsecure phone

98

Media Devices

- Personal Digital Assistants (PDA's)
 - Blackberrys, or Palm Pilots, pose a security threat

 - Small size and low cost make them easy to obtain and difficult to control

99

Media Devices

- Can be easily setup to download information from your computer

- All PDA's connecting to WIC systems should be in compliance with your agency's policy and Office of Management & Budget (OMB) guidelines

100

Media Devices

- Laptops
 - Convenience makes vulnerable to theft or security breaches
 - Password protect User logon information
 - Be careful what you display on your screen
 - When traveling to prevent theft, maintain possession at all times

101

Media Devices

Laptops

- Upon arrival of temporary travel destination, be sure laptop is secured while unattended

- If wireless capable, ensure wireless security features are properly configured

- Turn wireless capability off when not in use

102

Media Devices

Laptops

- If is not possible to turn the wireless feature off, configure to recognize Internet access points, not ad hoc networks

- Encrypt all sensitive data stored on laptops and other portable computer devices

- Ensure you follow your agency's guidance on encryption of sensitive data on laptops

103

Media Devices

Wireless networks

- Operate by radio signals instead of traditional computer cables to transmit and receive data
- Unauthorized access to your network can be gained by someone with a receiver
- Unauthorized user may be able to capture data being transmitted and data stored on your network

104

Media Devices

• Fax machines

- Ensure recipient will be present to pick up immediately
- Contact recipient directly to confirm delivery

105

Media Devices

- Never transmit classified information via an unsecured fax machine
- Always use a cover sheet so fax is not immediately visible

106

Spillage

Spillage

Spillage

- Also referred to as contamination

- When information of a higher classification level is introduced to a network at a lower classification level

114

Spillage

- Improper storage, transmission, or processing of classified information on an unclassified system
 - Ex. Information classified as Secret is introduced to an unclassified network

- If you suspect spillage has occurred—contact your security point of contact immediately

115

Spillage

Spillage Prevention

- Tips to prevent spillages from occurring
 - Check all emails for possible classified information
 - Mark and store all removal media property
 - With emails, ensure all file names and subject headers properly identify content sensitivity

116

Spillage

Spillage Prevention

- Spillage cleanup is a resource intensive process
- Can take weeks to contain and clean an affected information system
- Greatly impact the security of your agency's information

117

Personal Information

Personal Information

- Special rules govern protection of personal information
- The Privacy Act enacted in 1975
 - Government entities must safeguard personal information processed by government entities or contractor computer systems

119

Personal Information

- Government entities must provide access to the information by the individual
- Must amend the information if it is not accurate, timely, complete or relevant

120

Personal Information

- New guidance concerning greater measures for protection of personal identifiable information (PII) is outlined in several OMB Memoranda
- OMB requires lost or stolen PII be reported within one hour to the U.S. Computer Emergency Response Team (CERT)

121

Personal Information

- Each agency has its own policies to implement OMB's guidance
- Check with your security point of contact for additional PII requirements
- Authorized users must ensure personally identifiable information is protected on your agency's computer systems

122

Your Responsibility

- Information is a critical asset to your agency
- It's your responsibility to protect your agency's sensitive and classified information entrusted to you

123

Your Responsibility

- Remember—absolutely NO unencrypted classified information is allowed on unclassified systems
- Contact your security point of contact for more information about classification or handling of information

124

Spyware

- Software that performs certain behaviors
 - Advertising
 - Collecting personal information
 - Changing the configuration of your computer
- Without your consent or knowledge

125

Spyware

- Your computer may be infected if you
 - Receive pop-up advertisements even when not on the internet
 - Web browser's home page has changed
 - New toolbar is on your browser that you didn't want

126

Spyware

- Ways spyware or unwanted software enter your system
 - Covertly install software during installation of wanted software
 - Read all disclosures, license agreements and privacy statements carefully with installing something on your computer

127

Spyware

- To detect and remove spyware
 - Use an up-to-date spyware detection and eradication program
 - Detection software should scan and remove spyware

128

E-Commerce

E-Commerce

- Business transactions conducted using electronic documents, rather than paper
 - (i.e. direct deposit of salary from employers' account into your bank account)
- Allows consumers and businesses greater flexibility as to how and when transactions are conducted

132

E-Commerce

- Common ways for individuals to fall victim to identity theft
 - Increases vulnerability when you transfer personal information over the internet
 - To reduce risk, confirm e-commerce site you use conducts business over an encrypted link before providing any personal information

133

E-Commerce

- Encrypted links are indicated by “https” in the URL
- Note: not all https sites are legitimate, you are still taking a risk by entering personal information online

134

Final Summary Information Systems Security

**Final Summary
Information Systems Security**

- You are the first line of defense in protecting you agency’s information system
- You are your own defense against online attacks against your personal computer

136

**Final Summary
Information Systems Security**

- Basic guidelines to protect your office and home computer
 - Use anti-virus and spyware detection software and keep them up to date
 - Scan your system regularly for viruses and spyware
 - scan all email attachments and files downloaded from the internet

137

**Final Summary
Information Systems Security**

- Delete files infected with viruses
- Regularly download software updates and patches to fix security flaws
- Install and use a firewall if you are connected to the internet
- Make backups of all important files

138

Final Summary Information Systems Security

- Use hard-to-guess passwords
- Physically disconnect your computer from the internet when you are working online
- Secure wireless network by passwording your router
- Be aware of risks using peer-to-peer, file sharing programs
 - You could be exposing all of the information stored on your computer to anyone who uses these applications

139

In Closing

- Download additional Automation Training QWEST Student Packets at
Website: <http://www.dshs.state.tx.us/wichd/hd/qwest.shtm>
- If you have any questions or comments about this class, please email us
WicAppTraining@dshs.state.tx.us
or fax us @ 512-341-4479

140



- We want to thank you for your participation in this training
- For technical questions please call the WIC Application Support Help Desk
@ 1800-650-1328

141
