Information Technology Security Awareness Training

Created by Cal-DOJ March 2016

Information System

In order to understand the importance of information system security or information technology security, you first need to know what an information system is.

Information System

The term “information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System

An information system may also include other communications equipment:

- Fax machines
- Desktop Computers
- Laptops Computers
- Handheld Computers
- Portable Electronic Devices (PED)
- Mobile Data Terminals (MDT)
- Smart phones
- Tablets

Information Technology Security

The term “Information Security” refers to protection of information and Information Technology (IT) systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Confidentiality
- Integrity
- Availability

Information Technology Security

Confidentiality: to ensure that information is not disclosed to unauthorized individuals.

Integrity: to make sure that information and systems are not modified maliciously or accidentally.

Availability: the reliability and timely access to data and resources by authorized individuals.

Why is Information Technology Security Important?

NCIC Requirement

Individuals, businesses and government organizations have become increasingly reliant on information technology systems. This fact makes protecting these assets more important than ever before.

Systems have become more complex and interconnected, increasing the potential risk with their operations.

NCIC Requirement

DOJ requires all agencies to provide basic security awareness training for all new employees and all appropriate personnel who have access to Criminal Justice Information within six months of initial assignment, and biennially thereafter, who have access to Criminal Justice Information.

Security Awareness Topics

CJIS Security Policy

Desktop Security

Passwords

Storing of Sensitive Data

Disposal of Sensitive Data

Vulnerabilities and Threats

Sanctions

CJIS Security Policy

Initially written and approved in 1999

- Living Document current version 5.2
  dated 08/2014

Changes occur as a result of an Advisory Process with each policy change, a new edition is issued to supersede all prior updates.

CJIS Security Policy

The CJIS Security Policy provides the minimum level of security requirements determined acceptable for the transmission, processing, and storage of CJIS data.

They include:

- **Rules of behavior policy for employees**
- **Laws, regulations and management goals**
- **Security Procedures**

CJIS Systems Agency (DOJ)

The DOJ serves as the CJIS System Agency for the State. As the CJIS System Agency, the CA DOJ is responsible for establishing and administering an IT Security Program throughout the user community.

CJIS Systems Officer

Responsible for the following:

Managing the security of CJIS systems within their state or agency.

Ensure state/federal agency compliance with policies approved by the CJIS Advisory Policy Board and adopted by the FBI.

DOJ Information Security Officer

Responsible for the following:

- Serve as the security point of contact for the FBI CJIS Division ISO. (Information Security Officer)

- Document technical compliance with the CJIS Security Policy.

DOJ Information Security Officer

Responsible for the following:

Establishing a security incident response and reporting procedures to discover, investigate, document and report on major incidents that significantly endanger the security or integrity of the criminal justice agency systems to the DOJ, the affected criminal justice agency, and the FBI CJIS Division ISO.

Awareness and Training

Within six months of appointment/assignment:

- All personnel with access to sensitive Law-Enforcement Information

Must happen biennially thereafter to:

- Personnel who manage users
- Personnel with physical and logical access
- Personnel with Information Technology roles

Physical Security

Computer Security must be enforced at all times against any unauthorized access including the routine viewing of Criminal Justice data displayed in computer monitors, printed or stored.

Includes: Mobile/remote devices such as MDC's, handheld devices, laptops, smartphones and tablets.

Visitors Access

Visitors must be escorted by authorized personnel at all times while visiting the computer center or any area that has terminals.

Personnel Security

State of residency and national fingerprint-based record check shall be conducted within 30 days of employment or assignment.

Proper Access To Use and Disseminate FBI CJIS System Information

- Proper access and use of the Criminal History and the III - Interstate Identification Index systems ensures information is for authorized purposes only.
- Must have both “right to know” and “need to know” at time of performing a transaction.
- Third party dissemination is authorized only if the other agency is an authorized recipient.

What is the weakest link to having a successful Security Program?

Desktop Security

CLETS / NCIC terminals are “For Official Law Enforcement Business Only.”

CLETS / NCIC terminals must be operated only in controlled space and under the direct supervision of authorized personnel.

Desktop Security

When not under the direct supervision of an authorized person either during or outside regular working hours, Any CLETS / NCIC terminals must be:

Turned off; USB Flash, CD's diskettes, tapes, removable hard disks, and or printer ribbons must be removed and secured.

IDs and Passwords

Each employee who is authorized to access CJIS data shall be uniquely identified by one or a combination of the following:

- **Full name**
- **Badge number**
- **Employee or pin number**
- **Unique alphanumeric identifier**

IDs and Passwords

The DOJ mandates these passwords requirements. Passwords are often the weak link in the authentication process. You must follow these requirements:

- **Minimum 8 characters**
- **Not a dictionary word or proper name**
- **Not same as user ID**
- **Changed within a maximum of 90 days**
- **No password reuse of last 10 passwords**

Good Password Sense

It's your responsibility to protect your password.

You will be held responsible if someone else uses your password in connection with a system transaction.

A secure password is one that is not:

Posted

Written Down

Shared

Experienced hackers know to look for exposed passwords that are taped to monitors, hidden under keyboards, or even in a desk drawer.

Password Sharing Does The Following:

Places information that is protected at great risk.

Unwanted break-ins from unknown individuals, as well as known individuals.

Protect Your Passwords

Memorize it - do not put it in writing.

Safeguard it - your password is the key to one of the most valuable resources.

If you forget your password, notify County ISD at 565-2030; your old password will be deleted from the system and a new one issued.

Protect Your Passwords

Immediately following the suspected or known compromise of a system password, a new password must be issued and the compromised password must be deleted from the system.

When a system user no longer needs access, the password must be removed from the system.

When you leave a terminal unattended for any reason, log off or lock the computer.

Storing Sensitive Data

Criminal History:

- Shall be stored in a secure, locked, records environment.
- Shall be stored only for necessary periods of time.
- Shall not be stored in individual personnel files.

Today's crime scene is in your:

- Living room
- Home office
- Workplace

Disposal of Media

- Confetti Shred
- Avoid straight shredders

- Burn
- Destroy

Vulnerabilities and Threats

A vulnerability is a point where a system is susceptible to attack. They include:

- **Physical**
- **Natural**
- **Media**
- **Human**
- **Communication**
- **Hardware and Software**

Vulnerabilities and Threats

A threat is an unintentional or deliberate event or circumstance which could have an adverse impact on an information system. Threats can come from internal or external sources. There are three main categories of threats:

- **Natural**
- **Unintentional**
- **Intentional**

Vulnerabilities and Threats

Natural threats can endanger any facility or piece of equipment. You may not be able to prevent a natural disaster, but damage can be minimized with proper planning. Natural threats include:

- **Fire**
- **Flood**
- **Lightning**
- **Power Failures**

Vulnerabilities and Threats

Unintentional threats are actions that occur due to lack of knowledge or through carelessness. Unintentional threats can be prevented through awareness and training. Unintentional threats include:

- Physical damage to equipment
- Deleting information
- Permitting unauthorized users to access information

Vulnerabilities and Threats

Intentional threats are those threats that are deliberately designed to harm or manipulate an information system, its software and/or data.

Security software such as an antivirus program is designed to protect against intentional threats.

Vulnerabilities and Threats

Intentional threats include:

- Social Engineering
- Phishing
- Sabotage
- Eavesdropping
- Unauthorized data access
- Intrusions
- Denial of Service
- Theft

Social Engineering

Every burglar knows that the easiest way to break into a building is to unlock the door with the key.

In the context of computer security, one process of getting the “key” is called social engineering.

Social Engineering

Social engineers don't need to be "technically" savvy.

Their "people skills" get them in where they're **NOT** suppose to be.

- Charm
- Intimidation
- Trickery

Well known social engineer / hacker:

Kevin Mitnick

Social Engineering

How does Social Engineering Work?

Definition:

"Non-technical type of intrusion which relies heavily on human interaction and often involves tricking other people to break normal security procedures"

Social Engineering

Social Engineering Scenarios:

#1

Telephoning a user and posing as a member of the IT support team, who needs the user's password and other information in order to troubleshoot problems with the network or the user's account.

Social Engineering

Social Engineering Scenarios:

#2

Telephoning the IT department and posing as a high ranking executive in the company, pretending to have forgotten their password and demanding that information immediately because of a pressing business urgency.

Social Engineering

Some Social Engineering tactics:

"Dumpster Diving"

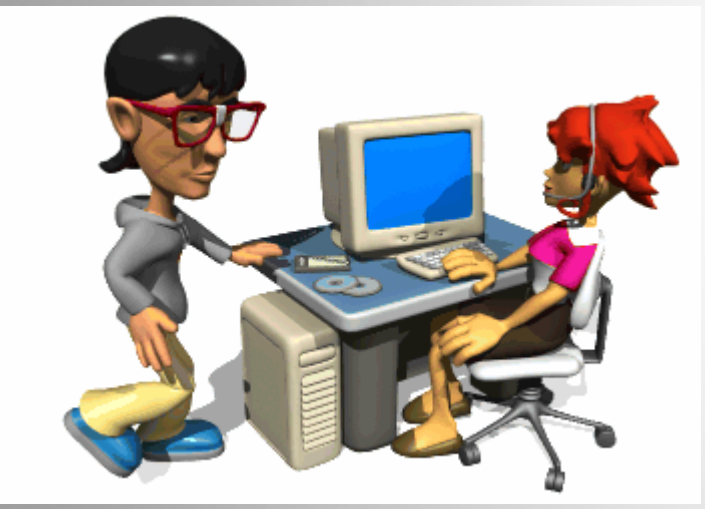
Posing as company employees:

- IT team member
- Building repair personnel
- Janitors

"Shoulder Surfing"

Social Engineering

"Reverse Social Engineering"



Social engineer creates a problem on the network or the user's computer.

Social engineer or hacker comes to the rescue, fixes the "**problem**" thereby gaining the victim's confidence.

Social Engineering

Defense Against Social Engineers:

Don’t assume personnel know better than to freely give out confidential information.

Social Engineering 101

FOREWARNED IS FOREARMED

Don’t be “asleep at the switch”.

Phishing

“Phishing” is the act of sending an email pretending to be from online store, a financial institution, or an Internet Service Provider with the intention of gaining personal information.

Phishing

A good anti-virus software protection package that protect against phishing emails attempts is another way of protection.

Report Security Violations

If you become aware of any policy violation or suspect that your password may have been used by someone else, it is **your responsibility** to report that information **immediately to your supervisor** (or CLETS Information Security Officer Justin Riedel).

You can e-mail the CLETS Information Security Officer at sheriff-it@sonoma-county.org or Justin.Riedel@sonoma-county.org

Audit of CJIS Information Systems

The DOJ CJIS Audit Unit conducts systems compliance audits every three years of each CLETS/CJIS subscribed agency.

The DOJ conducts records and database audits on all Criminal Justice Agencies every three years.

All system transactions are subject to routine review for inappropriate or illegal activity.

Standards of Discipline

Information contained within the FBI CJIS Information System is sensitive information.

Improper access, use or dissemination of CJIS Information is serious and may result in administrative sanctions including, but not limited to:

- Termination of services.
- State and Federal criminal penalties.

Sanctions

It is your responsibility to conform to the requirements of the DOJ CLETS Policy and the FBI CJIS Security Policy when using computers with access to CJIS data.

Failure to comply with Rules of Behavior may constitute a security violation resulting in denial of access to the system.

Remember

1. You are the key to security, it begins with you.

2. It's your responsibility to ensure you're aware of and adhere to all policies and procedures regarding IT Security.

3. If you have any questions about the proper operation or security of computer systems entrusted to you, contact your CLETS Information Security Officer.

Questions

For any additional Questions please:

- E-mail sheriff-it@sonoma-county.org
- Call the 707-565-8885