# Information Technology Security Awareness Training


Rev. Dec. 27, 2011

# Information System

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

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

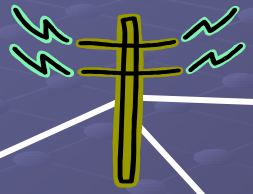
This means that your computer, laptop, and any other equipment connected to your computer are part of an information system.

This also includes telecommunications and network equipment used to connect your computer to other computers.

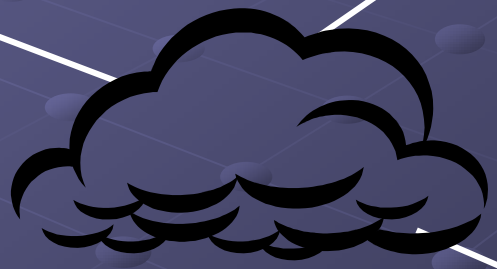
May also include other communications equipment, such as a fax machine, handheld computers, Portable Electronic Devices (PED), Mobile Data Terminals, etc….

# Information System

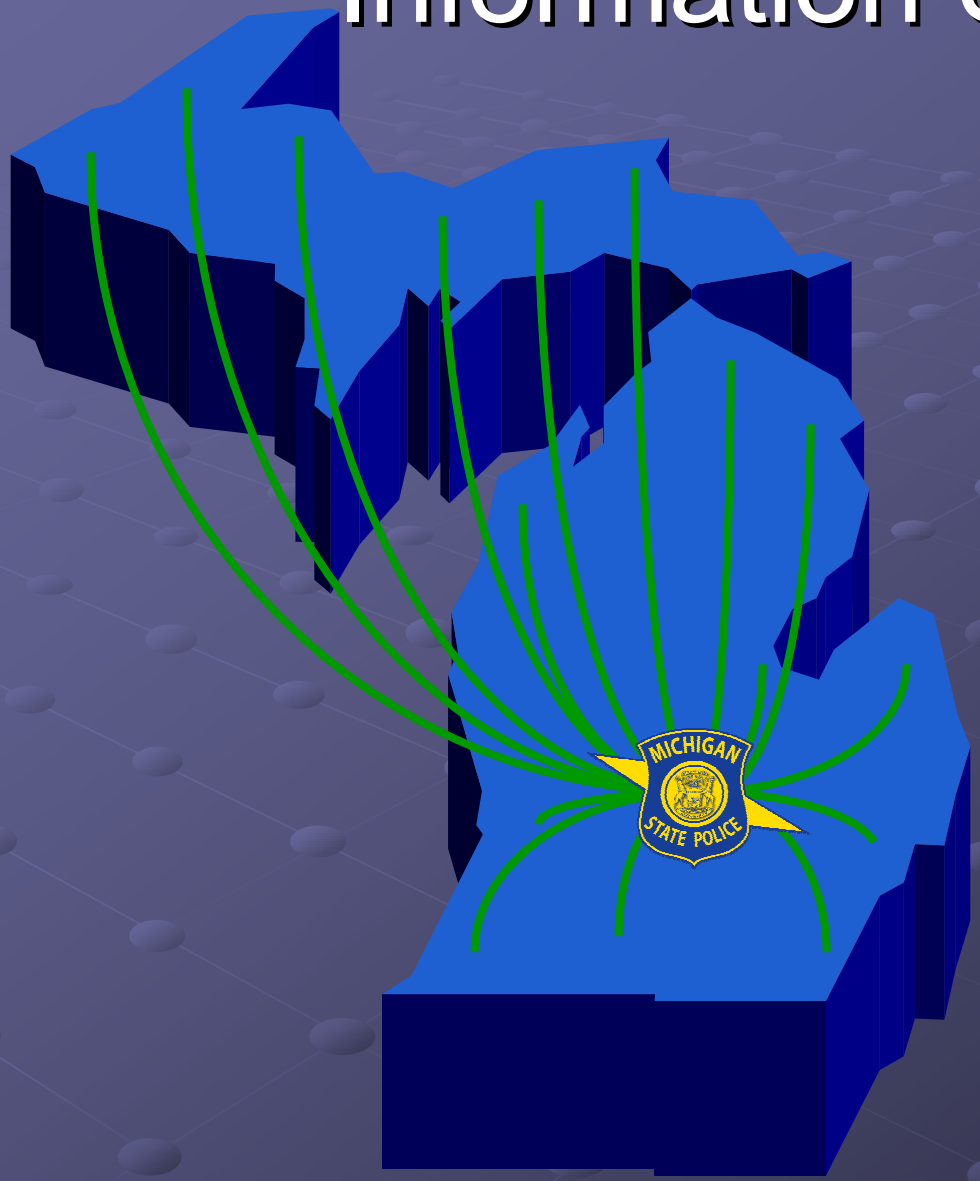
**LEIN, APRS, SOR, MICR, CHR, AICS, Livescan**

Over 1000 agencies accessing LEIN alone



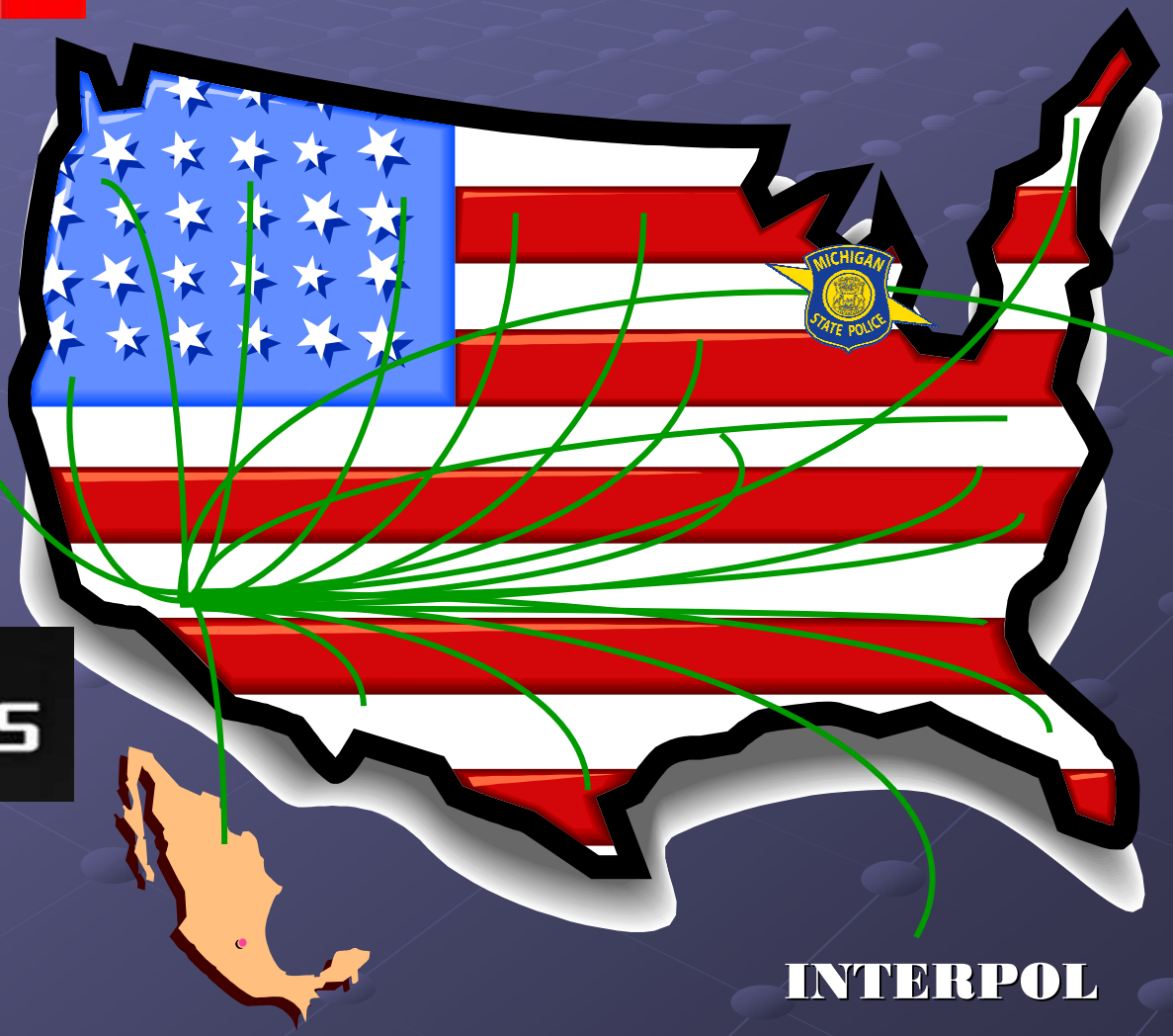

# Information System




The information system you're using extends a lot further than you might think. For example, your agency's connection to the Michigan State Police (i.e. LEIN, APRS, SOR, MICR, CHR, AICS, LiveScan) extends throughout the state of Michigan…..

# Information System

….to other states, and even to other countries





Powered By Nlets

INTERPOL

# Information Technology Security

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

# 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?

Individuals, businesses and government organizations have become increasingly reliant on information technology systems.

Information systems have become more complex and interconnected, increasing the potential risk with their operation.

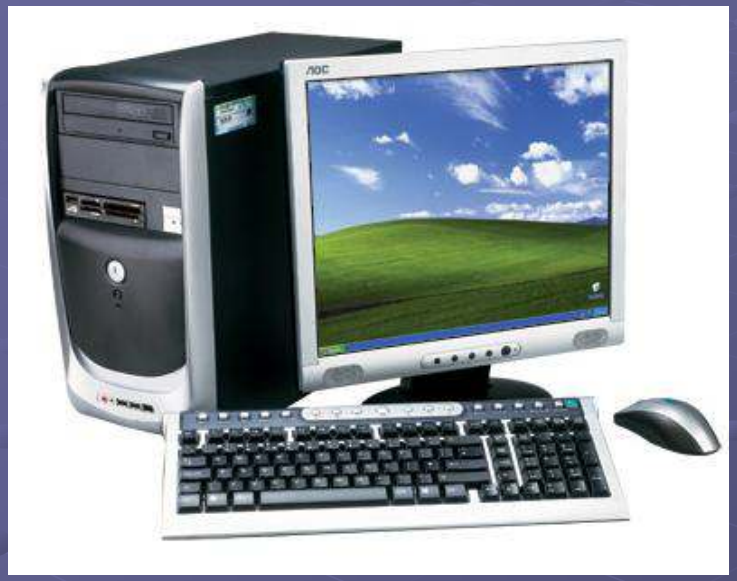
Contain personal/private information.

FBI CJIS Requirement.

# What we used to use……

# and……

# Now we use……



# FBI CJIS Requirement

Agencies shall provide security awareness training to all new employees and all appropriate IT personnel who have access to CJI (Criminal Justice Information) and/or FBI CJIS systems, ***within six (6) month of hire/assignment*** and once ***every two years***, thereafter.

This includes:

- Personnel with access to CJI
- Personnel with access to CJIS Systems
- Personnel who manage users/computers/network

# Security Awareness Topics

- **CJIS Security Policy** (Training, Duties/Responsibilities, Personnel Security, Physical Security, Visitors Access)
- **Device Security**
- **IDs and Passwords**
- **Access, Use and Dissemination**
- **Storing/Disposal of Sensitive Data**
- **Audit and Sanctions**
- **Vulnerabilities and Threats**

# CJIS Security Policy

# CJIS Security Policy

The CJIS Security Policy provides the minimum level of security determined acceptable for the transmission, processing, and storage of data obtained from an FBI CJIS system to be used for the administration of criminal justice (CJI).

They include:

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

# CJIS Systems Agency (CSA)

The Michigan State Police (MSP) serves as the CJIS System Agency for the State of Michigan.

As the CJIS System Agency, the MSP is responsible for establishing and administering an IT Security Program throughout the user community.

# CJIS Systems Officer (CSO)

Responsible to set, maintain and enforce:

Standards for selection, supervision, and separation of personnel who have access to CJI/CJIS systems.

Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS Systems used to process, store, or transmit criminal justice information, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.

# CSA Information Security Officer (ISO)

Responsible for the following:

- Serve as the security Point of Contact for the FBI CJIS Division ISO.
- Document technical compliance with the CJIS Security Policy.
- Document and provide assistance for implementing the security-related controls for the Interface Agencies and its users.
- Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

# Local Agency Security Officer (LASO)

Every agency with access to CJI must designate a LASO

The LASO shall:

Identify who is using CSA approved hardware/software, ensure no unauthorized access, document how the equipment is connected to the state system

Ensure personnel security procedures are followed

Ensure approved/appropriate security measures are in place and working

Support policy compliance and notify CSA ISO of security incidents

# User Agencies

Criminal Justice Agencies

Non-Criminal Justice Agencies (when authorization is pursuant to a Executive Order, statute, regulation, or inter-agency agreement)

Private Contractors (as well as the CJIS Security Addendum)

All agencies must enter into a User Agreement

# Device Security

# Physical Security

Computer Security - Must be protected at all times against any unauthorized access to or routine viewing of computer devices, access devices, and printed/stored data

Includes mobile/remote devices such as MDCs and handheld devices such as a Blackberry

# Visitors Access

Must be escorted by authorized personnel at all times when visiting the computer center, or any computer terminal and/or records storage areas where CJI is processed or stored.

Escorting does not mean being in the same room.

# Personnel Security

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

Conducted on:

- All personnel having authorized access to CJI/CJIS Systems
- All personnel who configure and maintain computer systems and networks with direct access to FBI CJIS systems
- All support personnel, vendors, volunteers, contractors, and custodial workers who have unescorted access to computer terminal and records storage areas where CJI is processed/stored

# Desktop Security

Computers accessing CJIS systems are “For Official Business Only.”

You have NO EXPECTATION OF PRIVACY in their use.

Computers accessing CJIS systems must be operated only in controlled space and under the direct supervision of authorized personnel.

Physically position your computer display so that you can see all persons that might be able to look at your keyboard, monitor, or screen of your computer.

# Desktop Security

If you know you are going to be away from your desk for an extended period of time, either shut down your system or lock your computer.

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

Turned off

Diskettes, tapes, removable hard disks, and printer ribbons must be removed and secured.

# Desktop Security

Timeout/Session Lock

Any user signed onto a terminal which has been inactive for 30 minutes must be automatically signed off

An unattended terminal is vulnerable to masquerading

You must re-identify yourself by reestablishing the session (re-enter your password)

# Mobile / Wireless devices

Mobile computers, laptops, BlackBerries aren't always going to be located in a physically secure location.

- Must employ similar physical controls as those in a physically secure location (i.e. screen positioning, locked when not in use, etc.)
- Residing resting data must be encrypted
- Must employ *Advanced Authentication*

# IDs and Passwords

# IDs and Passwords

The most common way to identify yourself is to provide a user ID and password, aka *Authentication*

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
- Serial Number
- Unique alphanumeric identifier

# IDs and Passwords

User IDs may be publicly known, passwords must be kept secret.

User IDs serve as an "electronic signature" on all system transactions for which they are used.

A password ensures the user is who they say they are.

# IDs and Passwords

Passwords are often a weak link in the authentication process. Systems must enforce the following 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 must not display/be transmitted in clear text

# Good Password Sense

A good password is a strong, secure password

A good password is a secret password

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

It’s your responsibility to protect your password

# A secure password 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.

If you forget your password, notify appropriate personnel; your old password will be deleted from the system and a new one issued.

# Password sharing….

…places protected information at great risk

…causes unwanted break-ins from unknown/known individuals

…subjects you to possible sanctions

# Protect Your Passwords

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

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

When you leave a terminal unattended for any reason, log off or lock it (control-alt-delete)

# Advanced Authentication

Used on mobile computers, laptops, BlackBerries that access CJIS systems.

- Another layer of protection, in addition to your User ID and password, to prove you are who you claim to be
- Token
- Challenge/Response questions
- Biometrics (i.e. fingerprint, retina scan, etc.)
- Device Forensics

# Report Security Violations

**It is your responsibility** to immediately report to your respective Security Officer, any policy violation you become aware, or if suspect that your password may have been used by someone else.

# Access, Use and Dissemination

# Access, Use and Dissemination

Least Privilege

The agency shall approve individual access, enforcing the most restrictive set of rights/privileges needed, based on:

- Job assignment or function
- Physical location
- Time of day/day of week

# Access, Use and Dissemination

Information obtained from CJIS systems is protected and may only be accessed/used for appropriate purposes.

Learn the applicable laws, rules and policies for the specific system you are accessing.

Understand the applicable reasons for accessing the system and for disseminating information.

# Storing Sensitive Data

# Storing Sensitive Data

Criminals no longer have to break through a window or pick a lock to invade your privacy; they just enter via the internet and remove the personal information that you have stored for private use believing it to be safe. The objective of the hacker is to break into your computer and steal your information; so it is very important that you make this as difficult as possible.

# Security of CJIS System Information

Criminal History Record Information (CHRI):

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

CHRI may be transmitted via a facsimile device as long as both agencies involved in the transmission are authorized to receive the information. Verification of the receiving agency's authenticity shall be made prior to the transmission.

# Securing Sensitive Data

Ways to protect your employer, your family, your friends, and yourself.

- Make sure that your computer/device is protected with a strong password.
- Make sure that your computer/device is patched (OS and applications).
- Practice smart internet habits when performing financial transactions on line. Be selective of the sites you visit and check for the security level of web pages that require you to enter personal information.
- When entering your personal information on a website, make sure the website is encrypted. To do this, look in the browser window for an object that looks like a lock. This lock signifies that the website is encrypted.
- Address line in the browser window for an address that starts with https://. This is another indication that the web site is secured.

# Securing Sensitive Data

## Encryption

The process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Encoding/decoding

CJIS information transmitted outside the boundaries of a physically secure facility must be encrypted at a minimum of 128-bit.

# Securing Sensitive Data

All CJIS data must be properly secured throughout its lifecycle

- Encrypted queries
- Properly background checked/fingerprinted users
- Disseminated only to authorized users
- Secure records storage areas (i.e. hard copy/paper, storage, backup media, on-site/off-site, etc.)
- Ensure proper destruction

# Disposal of Sensitive Data

When no longer using diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items destroy them by shredding or incineration.

**DO NOT PLACE SENSITIVE DATA IN TRASH CANS**

# Disposal of Media

- Cross-cut shred

- Burn

# Audit and Sanctions

# Audit of CJIS Information Systems

To ensure compliance with agency and FBI CJIS Division policy and regulations, CJIS Audit Unit will conduct a compliance audit every three years of each CSA

CSA will conduct audits on all criminal justice and noncriminal justice agencies every three years

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

# Standards of Discipline

FBI CJIS information is sensitive information. Improper access, use, and dissemination is serious and may result in the imposition of administrative sanctions including termination of services, as well as state/federal criminal penalties.

# Sanctions

It is your responsibility to conform to the requirements of the Rules of Behavior 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.

A violation of security requirements could result in termination of system access privileges and/or serious disciplinary action and the possibility of dismissal.

# Sanctions

CJIS Policy Council Act (MCL 28.211-215)

- May not use CJIS system/information for personal reasons
- May not disseminate to an unauthorized entity/person
- 1st offense = Misdemeanor; 2nd offense = Felony

Driver Privacy Protection Act

- May not use SOS/personal data for a reason not allowed by law
- First offense = Felony

# Vulnerabilities and Threats

# Vulnerabilities and Threats

A vulnerability is a point where a system is susceptible to attack.

Vulnerabilities may 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 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

## Social Engineering Scenarios:

#3

Developing a personal relationship with a user or IT team member with the intent of "sweet talking" the person out of confidential information that can be used to break into the network

# Social Engineering

Some Social Engineering tactics:

"Dumpster Diving"

Posing as a company employee:

- 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.

The average employee has no reason to question someone who seems to have a legitimate need.

Even IT team members (who are security-conscious) may trust an irate person claiming to be upper management.

# Social Engineering

## Summary

Social engineering could be considered the easiest way for a hacker to access your network and one of the most common.

As a rule, most companies do nothing to prevent exploitation of the human factor.

# Social Engineering

## Summary

Establishing policies is the first step in preventing socially engineered attacks.

Most important step – educating employees to make them aware of the danger of social engineering.

People who fall prey to social engineering scams are those who haven’t heard about them.

# Phishing

“Phishing” is the act of sending an email pretending to be from online store, a financial institution, or an Internet Service Provider, etc., with the intention of gaining personal information. The email usually claims that you need to go to the link provided in the email to update your account information. Phishing hackers use this technique to obtain personal information such as credit card numbers, bank PINS, and Social Security Numbers. Like traditional fishing, it relies on a computer user to take the bait.

**Be very careful of web links provided in emails.**

# Phishing

In addition to being educated, a good anti-virus software package can protect against phishing emails.

*Required on all devices accessing CJIS systems.

**Immediately delete an email from an unknown sender that includes an attachment!!**

# SPAM

A form of Phishing, SPAM is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately.  Large companies and government entities are often targets of spam.

Direct effects include the consumption of computer and network resources, and the cost in human time and attention of dismissing unwanted messages.

Can saturate internet with email or take down an email server causing an inability to communicate.

# Are you being hacked? How to tell.

- A system alarm or similar indication from an intrusion detection tool
- Suspicious entries in system or network accounting
- Accounting discrepancies (e.g., an 18-minute gap in the accounting log in which there is no correlation)
- Exceptionally slow network activity, disconnection from network service or unusual network traffic
- Unsuccessful logon attempts
- New User accounts of unknown origin
- Unusual log entries such as network connections to unfamiliar machines or services
- New files of unknown origin and function
- Unexplained addition, deletion, or modification of data
- Poor system performance
- Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords
- Port scanning (use of exploit and vulnerability scanner, remote requests for information about systems and/or users, or social engineering attempts)
- Unusual usage times
- An indicated last time of usage of a account that does not correspond to the actual last time of usage Unusual usage patterns
- Denial of service activity or inability of one or more users to login to an account; including admin/root logins to the console
- System crashes

# Reminder

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 Security Officer

# Reminder

**FOREWARNED IS FOREARMED**


Don’t be “asleep at the switch”

# Security Awareness Training
# Proof of Completion

- **Print this page!**
- **Print and sign your name in the space below, include the date.**
- **Provide a copy to your LASO/TAC.**

Printed name: _____

Signature: _____

Date: _____