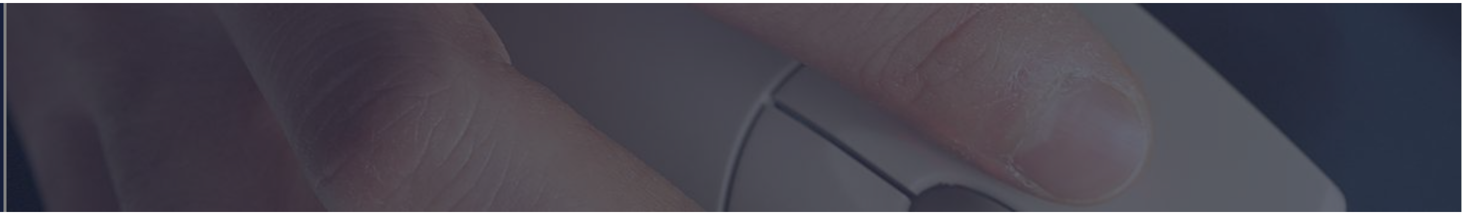


Cyber Security Awareness Training

What You Will Learn in this Program

- Potential risks and vulnerabilities
- Definitions
- Your role in cyber security and protecting privacy
- Best practices in security and privacy

Security Tips

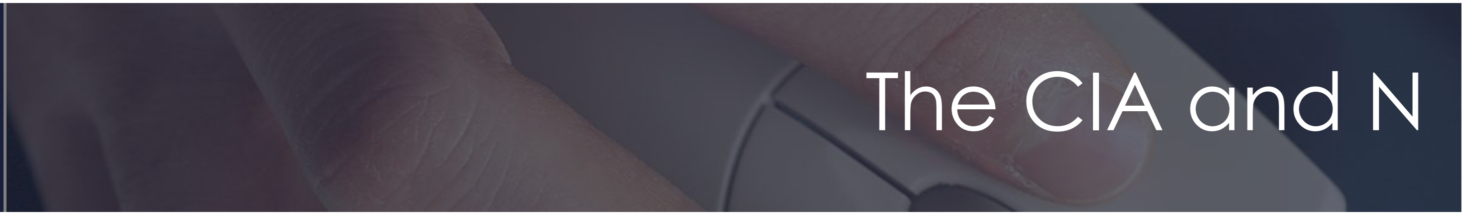
Commit to a disciplined practice of information security and continue to refresh yourself so you don't become a point of vulnerability in our security defenses.

Cyber Security Defined

- Cyber Security’s goal: **Protect our information and information systems**
- Cyber Security is: “**Protection** of information systems **against unauthorized** access to or **modification** of information, whether in storage, processing or transit, and against the **denial** of service to authorized users, including those measures necessary to detect, document, and counter such threats.”

Privacy Defined

- Information privacy, or data privacy: the relationship between **collection** and **dissemination** of data, technology, the public **expectation of privacy**, and the legal and political issues surrounding them.
- Information privacy is the **right to control** what **information** about a person is **released**.



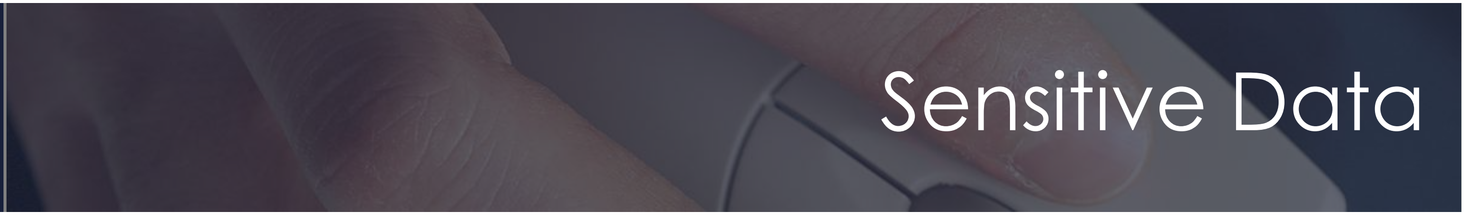
The CIA and N

- **Confidentiality**: **Safeguards** information from being **accessed** by individuals without the proper clearance, access level, and need to know.

- **Integrity**: Results from the **protection** of unauthorized **modification** or destruction of information.

- **Availability**: Information services are **accessible** when they are needed. Authentication means a security measure that establishes the **validity** of a transmission, message, or originator, or a means of **verifying** an individual's authorization to receive specific categories of information.

- **Non-repudiation**: Assurance the sender of data is provided with **proof of delivery** and the recipient is provided with proof of the sender's **identity**, so neither can later deny having processed the data.



Sensitive Data

- Information is considered **sensitive** if the **loss** of **C**onfidentiality, **I**ntegrity, or **A**vailability could be expected to have a **serious**, **severe**, or **catastrophic** adverse **effect** on organizational operations, organizational assets, or individuals.
- **Types** of sensitive information include:
  - Personnel
  - Financial
  - Payroll
  - Medical
  - Privacy Act information.

Tips to Help Protect PII

- Minimize PII
- Secure PII
- Safeguard the Transfer of PII
- Dispose of PII Properly

PII – Personally Identifiable Information

Prevent Spillage

- When storing sensitive information, including PII, **prevent *spillage*** by following these security tips:
  - **Encrypt** data before storing
  - **Store** data only on a **network** that has been **certified** and **accredited** to store this type of information
  - Remember, **some systems** are strictly **non-sensitive—never** transmit, store, or process **sensitive data** on a non-sensitive system
  - **Label** paperwork containing PII **appropriately** and ensure it is **not left lying around**
  - **Use** the **secure bins** provided to **dispose** of paperwork containing PII

Threats and Vulnerabilities

- What are we protecting our and our stakeholders information from?
  - **Threats**--any circumstances or events that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable
  - **Vulnerabilities**--weakness in an information system or its components that could be exploited.

Securing the Department

- Don’t store PII on unencrypted storage devices
- Remove your Personal Identity Verification (PIV), or smart card, when leaving your desktop PC
- Never transmit secure information over an unsecured fax machine
- Check for security badges and make sure guests needing escorts have them
- Don’t write down passwords
- Use only authorized thumb drives
- Properly label removable media such as CDs or DVDs
- Be careful how you dispose of anything that might contain sensitive information

Department Password Policy

- The Department has guidelines pertaining to password use.
  - Passwords must be:
  - Obscured during login and during transmission.
  - Changed after the initial login.
  - Forced by the system to be changed every 90 days.
  - Strong - shall include three of the four characteristics:
    - Numerals
    - Alphabetic characters
    - Upper and lower case letters
    - Special characters
    - Passwords shall be at least eight (8) characters in length.

Secure Passwords

Do

- Use a combination of: lower and upper case letters, numbers, and, special characters
- Change it every 90 days
- Create a complex, strong password, and protect its secrecy

Don't

- Use personal information
- Dictionary words (including foreign languages)
- Write it down
- Share it with anyone

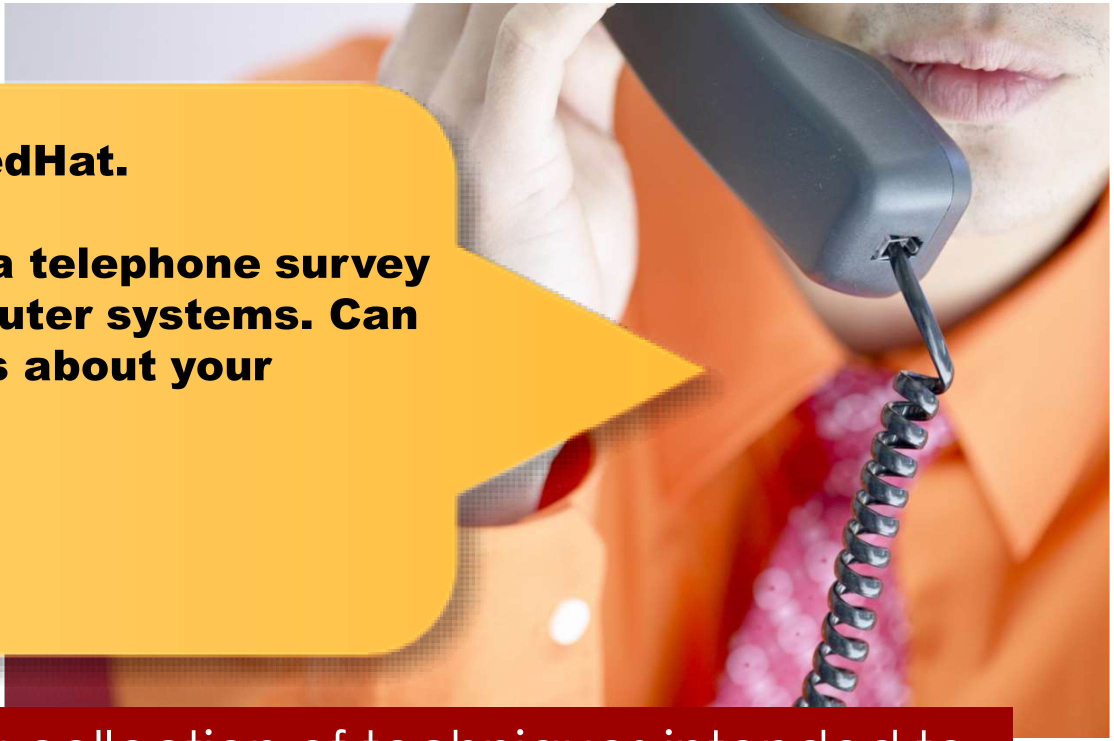
Protect Your Facility

- Protect your facility by following these general security tips:
  - Always use your own badge to enter a secure area
  - Never grant access for someone else using your badge
  - Challenge people who do not display badges or passes.
  - Report any suspicious activity that you see to your ISM or building security using the Information Security Incident Response and Reporting Procedures.

Situational Awareness

- To practice good situational awareness, take the following precautions, including but not limited to:
  - Avoid discussing topics related to Government business outside Government premises, whether you are talking face to face or on the phone
  - Remove your security badge after leaving your work station
  - Don’t talk about work outside the office
  - Avoid activities that may compromise situational awareness
  - Be discreet when retrieving messages from smart phones or other media

Social Engineering



Hello, I'm calling from RedHat.

Today we're conducting a telephone survey about the usage of computer systems. Can I ask you a few questions about your computer system?

Social engineering is a collection of techniques intended to trick people into divulging private information. Includes calls emails, web sites, text messages, interviews, etc.

Social Engineering

Do

- Document the situation—verify the caller identity, obtain as much information as possible, if Caller ID is available, write down the caller's telephone number, take detailed notes of the conversation
- Contact your ISSO

Don't

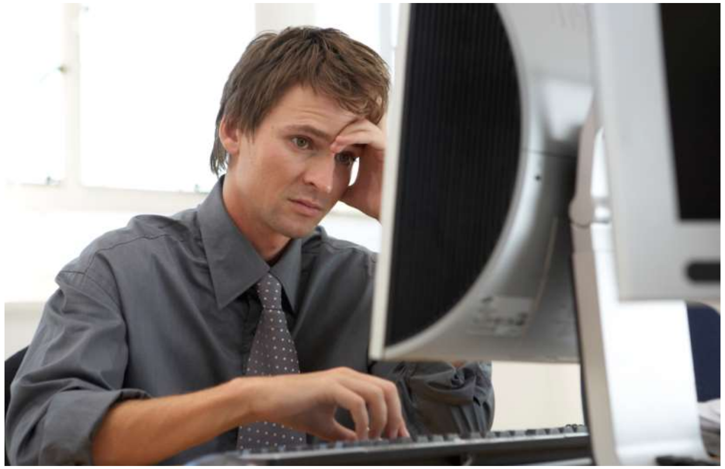
- Participate in surveys
- Share personal information
- Give out computer systems or network information

Mobile Computing

- Always maintain physical control of mobile devices!

- Properly label with classification and contact information
- Disable wireless functionality when it is not in use

Report Suspicious Computer Problems

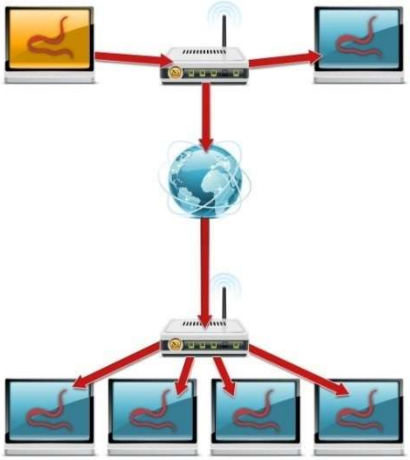


If your system acts unusual!

Report immediately to your ISM or Servicedesk

Trojan Horse

Spyware



Worm

Use of Social Media

- Be aware of what you post online!
- Monitor privacy settings
- Refrain from discussing any work-related matters on such sites.