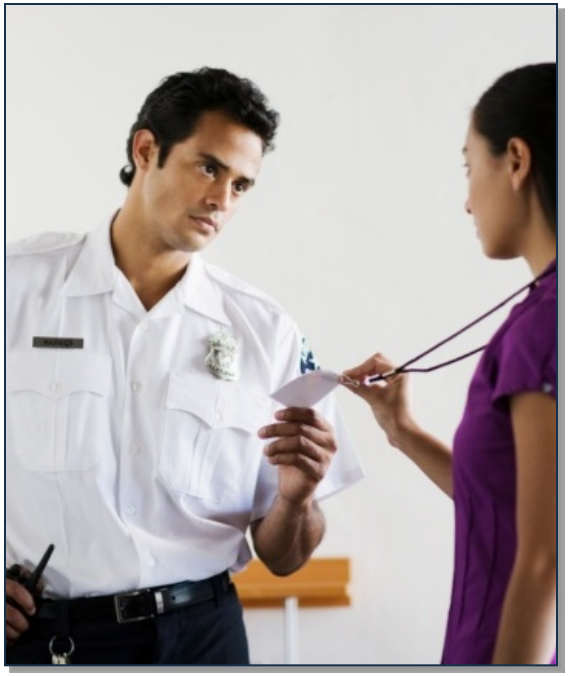
IS-906: Workplace Security Awareness

Course Administration

- Sign-in sheet
- Course evaluation forms
- Site logistics
  - Emergency procedures
  - Breaks
  - Restrooms
  - Cell phones/Blackberrys

Course Objectives

- Identify potential risks to workplace security.
- Describe measures for improving workplace security.
- Determine the actions to take in response to a security situation.



Discussion Question

Components of Risk

Three components:

- **Threat**
- **Vulnerability**
- **Consequence (Impact)**

Security Begins With You

- Ever-increasing risks threaten:
  - Worker safety.
  - Employee morale.
  - Economic livelihood.
- Employees are an integral part of the security solution.

Security Measures for Employees

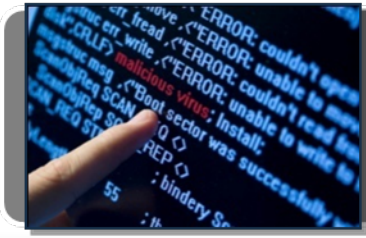
- Determine what should be reported.
- Report the incident.
- Never confront the situation alone.

Common Threats

Access & Security Control Threats

Criminal & Terrorist Threats

Workplace Violence Threats



Information & Cyber Threats

Securing Access Points

- Limit access points.
- Use appropriate locks.
- Control entrances.
- Restrict access to key areas, roofs, and HVAC systems.
- Use identification systems.
- Post signs.

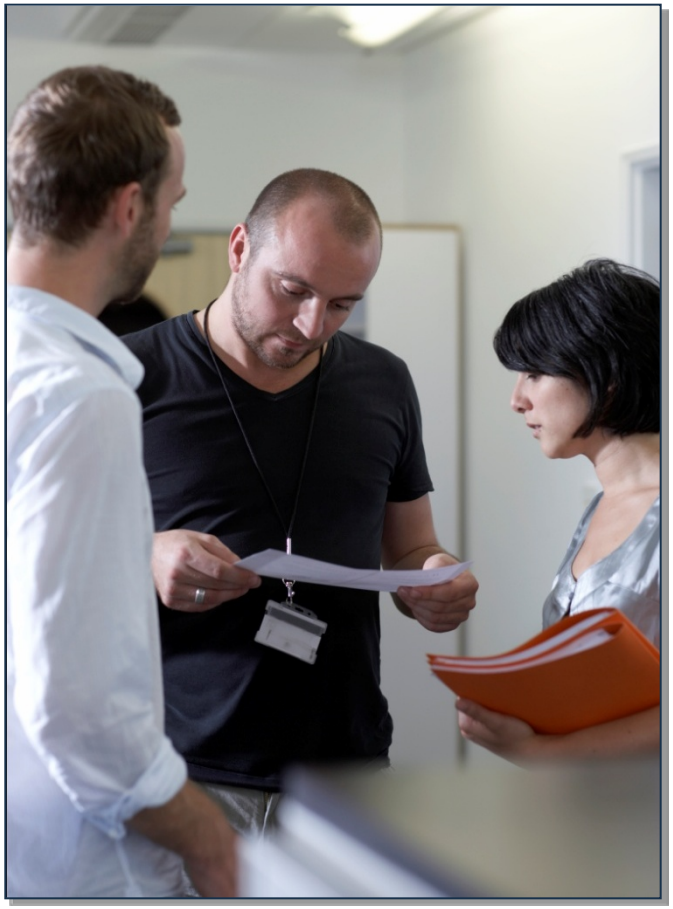
Access Control Procedures

- Identification checks
- Limit on keys and cards
- Delivery search or verification
- Employee-owned vehicle database
- Limited access
- Personnel training

ID Badges

ID badges or picture IDs provide quick identification of personnel.

Typical Badge Requirements

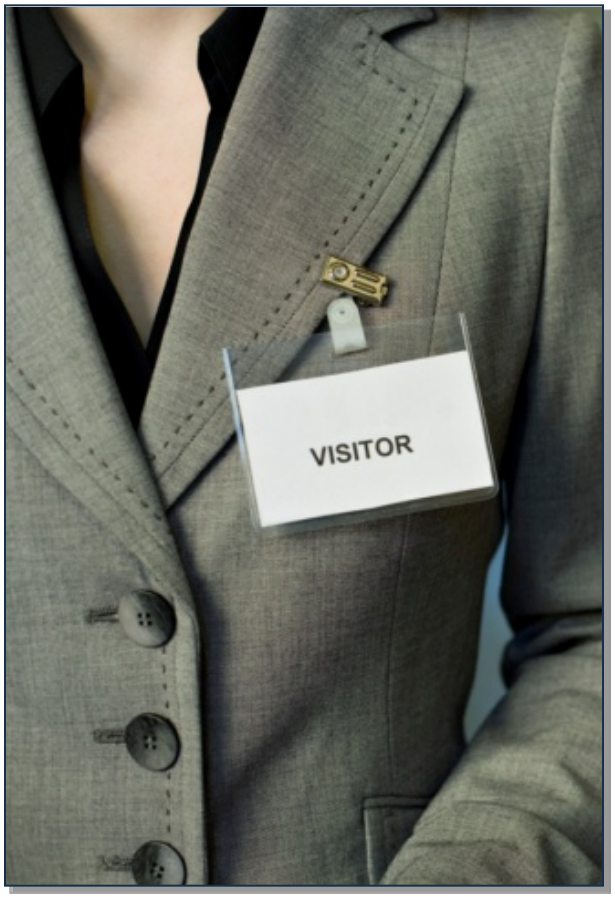


- Worn on outermost garment
- No “piggybacking”
- No lending, sharing, or borrowing of badges
- Report lost badges immediately

Scenario: Piggybacking

Nonemployees

- **Should wear a visitor's badge.**
- **Should be escorted at all times.**



Discussion: Missing ID Badge

Unknown Individuals

Challenge if they:

- **Are not wearing identification or escorted appropriately.**
- **Are inconsistent with the workplace dress code.**
- **Appear lost or are asking for directions.**

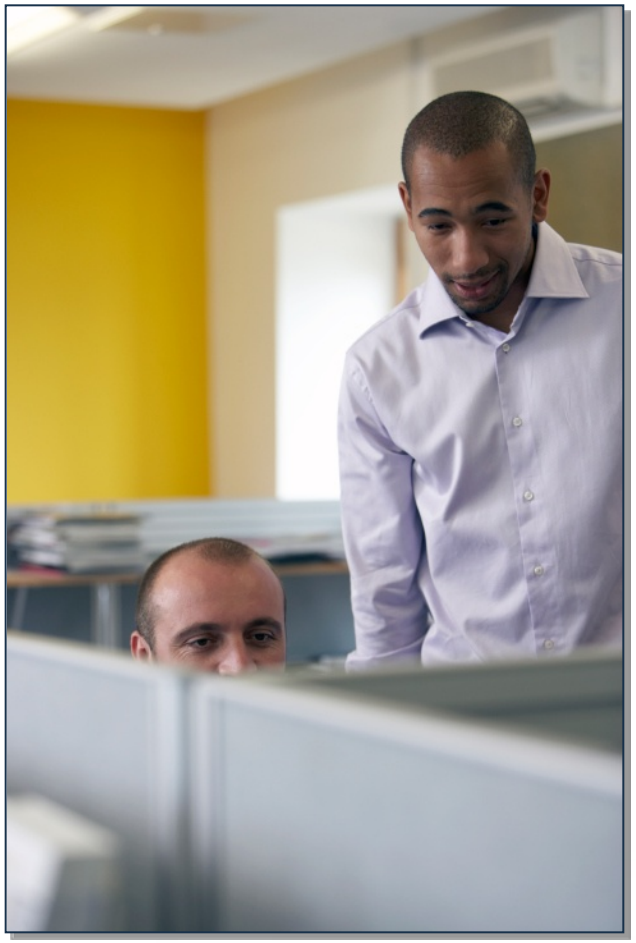
Scenario: Unknown Individual

What should Anne do differently?

Lack of Proper Identification

When you see someone without proper ID:

- **Follow policies and procedures.**
- **Approach only if comfortable.**
- **Notify appropriate personnel.**
- **Provide descriptive information.**



Activity: Unknown Individual

Instructions: Working as a team:

1. **Create a list of five techniques to use when approaching an unknown individual.**
2. **Record your list on chart paper.**
3. **Select a spokesperson and be prepared to present your list in 5 minutes.**

Report the Situation

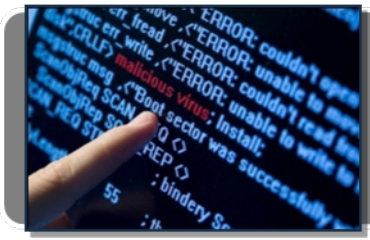
Always report situations that may threaten security.

Common Threats

Access & Security Control Threats

Criminal & Terrorist Threats

Workplace Violence Threats



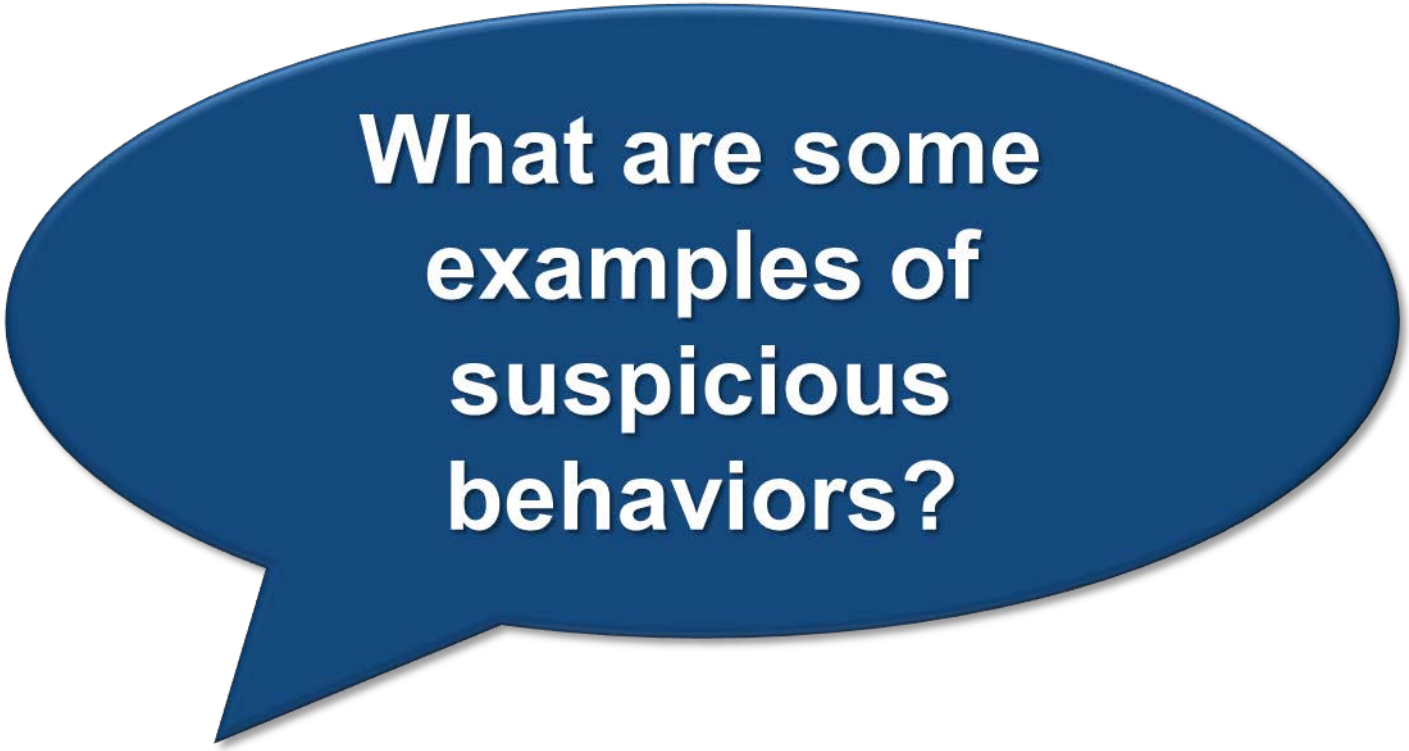
Information & Cyber Threats

Criminal or Terrorist Threats

Criminal or terrorist activities may occur anywhere, including:

- **Hotels.**
- **Banks.**
- **Grocery stores.**
- **Manufacturing plants.**
- **Nonprofit organizations.**

Discussion: Suspicious Behaviors



Scenario: Suspicious Behavior

Unusual or Suspicious Items

Be alert for:

- **Unusual situations.**
- **Suspicious packages or items:**
  - **Unusual substances in quantity.**
  - **Fumes, odors, or liquids coming from a package.**
  - **Disassembled electrical components.**
  - **Plans, drawings, schematics, or maps.**

Perimeter Breaches and Suspicious Packages

- Immediately notify the appropriate person.
- Do not approach or attempt to open or inspect a suspicious package.

Scenario: Being Observant

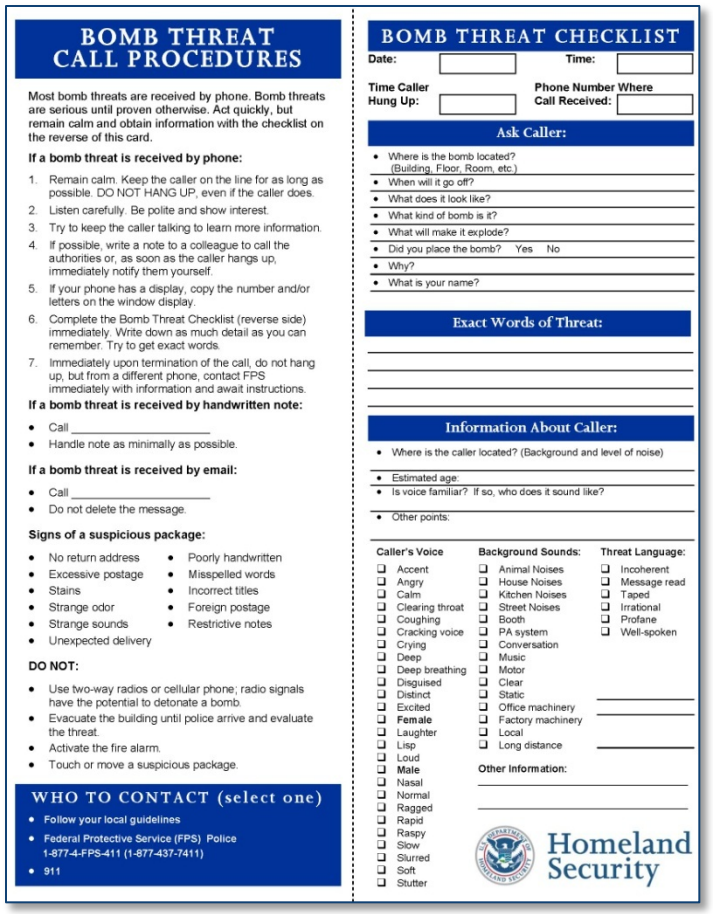
Compromised Vehicle Access

- **Unattended or suspicious vehicles**
- **Changes in vehicle patterns**

Scenario: Suspicious Van

What should James and Sanjay have done?

Bomb Threat Procedures



BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (reverse side) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by email:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.

WHO TO CONTACT (select one)

- Follow your local guidelines
- Federal Protective Service (FPS) Police 1-877-4-FPS-411 (1-877-437-7411)
- 911

BOMB THREAT CHECKLIST

Date: _____ Time: _____

Time Caller Hung Up: _____ Phone Number Where Call Received: _____

Ask Caller:

- Where is the bomb located? (Building, Floor, Room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (Background and level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice	Background Sounds:	Threat Language:
☐ Accent	☐ Animal Noises	☐ Incoherent
☐ Angry	☐ House Noises	☐ Message read
☐ Calm	☐ Kitchen Noises	☐ Taped
☐ Clearing throat	☐ Street Noises	☐ Irrational
☐ Coughing	☐ Booth	☐ Profane
☐ Cracking voice	☐ PA system	☐ Well-spoken
☐ Crying	☐ Conversation	
☐ Deep	☐ Music	
☐ Deep breathing	☐ Motor	
☐ Disguised	☐ Clear	
☐ Distinct	☐ Static	
☐ Excited	☐ Office machinery	
☐ **Female**	☐ Factory machinery	
☐ Laughter	☐ Local	
☐ Lisp	☐ Long distance	
☐ Loud		
☐ **Male**		
☐ Nasal		
☐ Normal		
☐ Ragged		
☐ Rapid		
☐ Raspy		
☐ Slow		
☐ Slurred		
☐ Soft		
☐ Stutter		

Other Information: _____

Homeland Security

- **Keep calm.**
- **Keep the caller on the line.**
- **Record every word.**
- **Obtain information.**
- **Pay attention to background noises and caller's voice.**
- **Report immediately.**

Suspicious Mail or Package

Be alert for:

- **Threatening letters.**
- **Suspicious contents (white powder, photos of the workplace).**
- **Oil or grease spots, an inaccurate address, or excessive postage or packaging.**

Theft and Diversion

- **Theft** is an unlawful or unauthorized acquisition by force or stealth.
- **Diversion** is an unlawful or unauthorized acquisition by fraud or deceit.

Container Breach

- A container possibly missing some of its contents.
- Should be reported.
- Can indicate a much larger security problem.

Scenario: Theft and Diversion

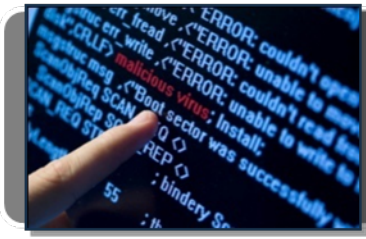
What should Jermaine do?

Common Threats

Access & Security Control Threats

Criminal & Terrorist Threats

Workplace Violence Threats



Information & Cyber Threats

Workplace Violence

- Carried out by current or former employees.
- Can be noticed by intuitive managers and/or coworkers.
- Behavioral indicators displayed over a period of time.

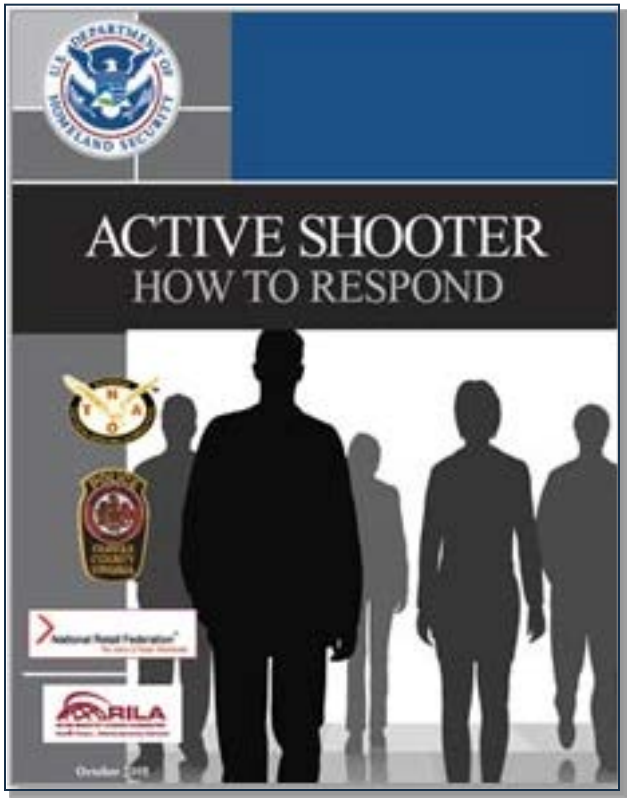
Activity: Indicators of Workplace Violence

Instructions: Working as a team:

1. **Create a list of five indicators of potentially violent behavior.**
2. **Record your list on chart paper.**
3. **Select a spokesperson and be prepared to present your list in 5 minutes.**

Workplace Violence Resources

- Active Shooter Booklet
- Active Shooter Pocket Guide
- Active Shooter Poster

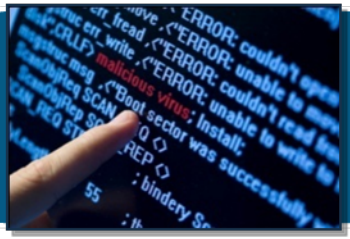


Common Threats

Access & Security Control Threats

Criminal & Terrorist Threats

Workplace Violence Threats



Information & Cyber Threats

Information and Cyber Threats

Security can fail through unauthorized access to:

- **An account name and/or password.**
- **Locked areas containing intellectual property and other sensitive information.**
- **Portable devices.**

Scenario: Trash Bins

Protecting Information

Common privacy law principles are based on the following Federal laws:

- **Privacy Act of 1974**
- **Freedom of Information Act (FOIA)**
- **E-Government Act of 2002**
- **Fair Credit Reporting Act (FCRA)**
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- **Children's Online Privacy Protection Act (COPPA)**

Personally Identifiable Information (PII)

- Apply "need to know" principle.
- Challenge need before sharing information.
- Consider PII materials for official use only.
- Limit collection of PII for authorized purposes.

PII Examples

- Name
- Social Security number
- Mailing address/ZIP code
- Telephone number
- Account numbers
- Date and place of birth
- Biometric identifiers (e.g., fingerprints)
- Certificate/license numbers
- Vehicle identifiers including license plate numbers
- Internet protocol (IP) addresses
- Email addresses
- Photographic/facial images

Safeguarding Sensitive Information

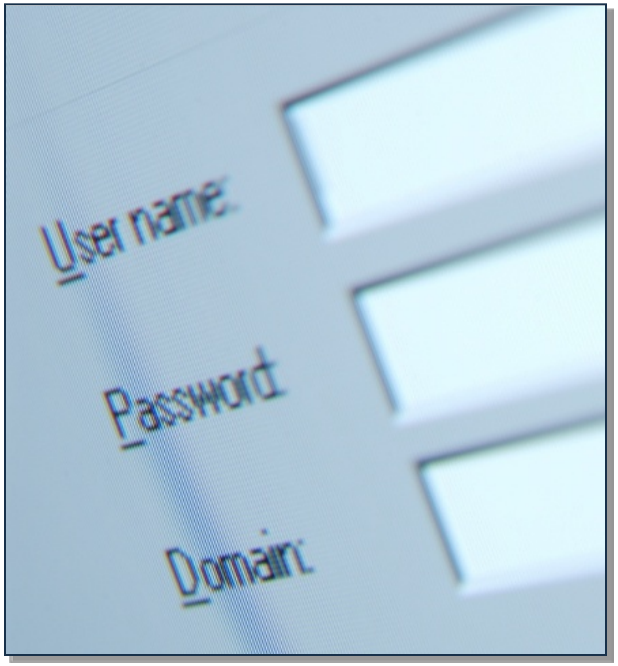
- Store in a secure area or destroy appropriately.
- Never email to unauthorized individuals.
- Never leave on community printers.
- Take precautions against loss or theft of computers and storage media.
- Notify immediate supervisor if loss or compromise occurs.

“Clean Desk” Policy

- Set date and time.
- Use secure recycling bins.
- Don’t print unnecessarily.
- Handle papers once.
- Scan and store documents.
- Clear space before going home.

Scenario: Sensitive Document

Use of Social Engineering



Social engineers obtain information through:

- **Telephone interactions.**
- **Face-to-face interactions.**
- **Email or web interactions.**

Social Engineering Example

Jean calls Mark posing as a Help Desk technician and requests user account information.

What should Mark have done differently?

Activity: Social Engineering

Instructions: Working as a team:

1. **Write a fictional scenario in which an act of social engineering takes place.**
2. **Describe what the employee in your scenario should have done.**
3. **Select a spokesperson and be prepared to present your scenario in 5 minutes.**

Cyber Threats and Vulnerabilities

Active Threats

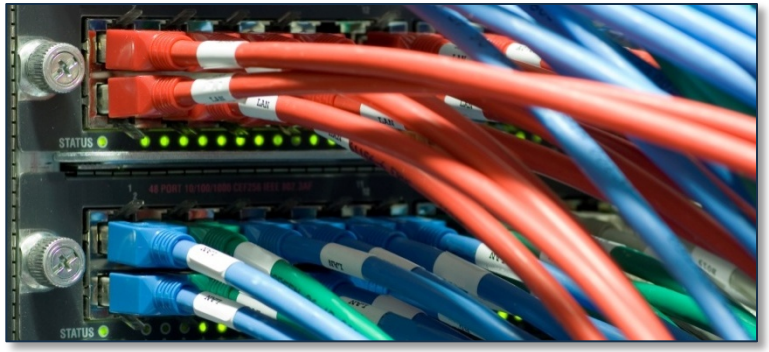
- Hackers
- Cyber warfare
- Malicious code
- Information gathering
- Identity theft

Systems Threats

- Peer-to-peer software
- Removable media

Passive Threats

- Natural hazards
- Power failures
- Software glitches
- Human error

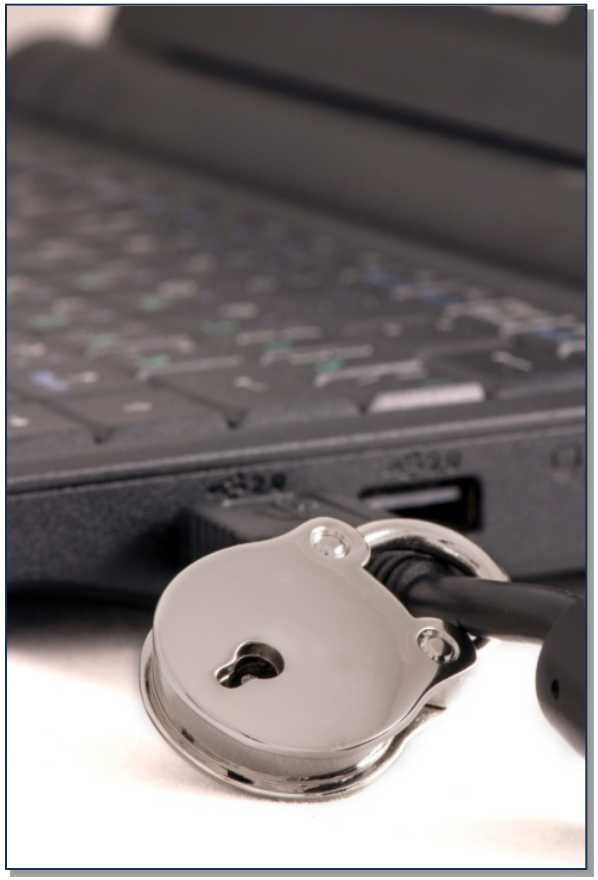


Cybersecurity Protective Measures

- Firewalls and virus protection
- Password procedures
- Encryption software
- Access control systems
- Computer staff background checks
- Staff training and 24/7 on-call technical support
- Intrusion detection systems
- System recovery and restoration plans

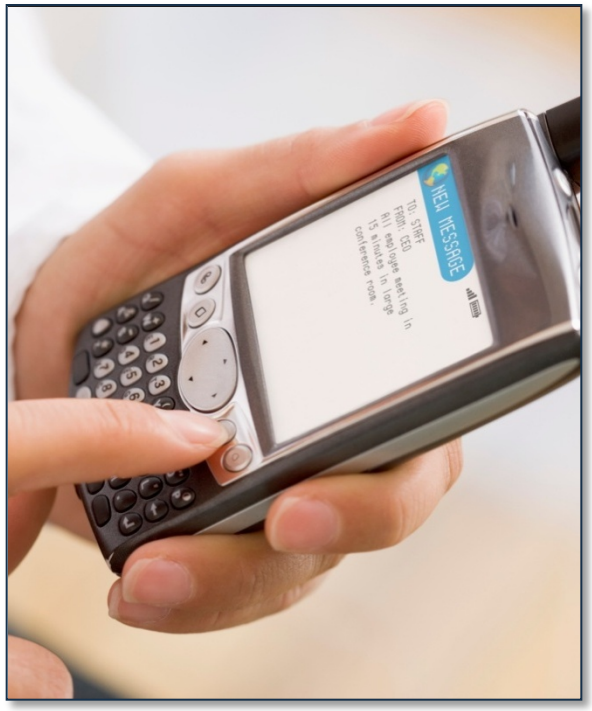
Strong Passwords

- Minimum of eight characters
- Combination of different character types
- Not solely a dictionary word
- Not easily guessed or obtained information



Discussion: Leaving the Office

If You See Something, Say Something™



- Be vigilant.
- Take notice of surroundings.
- Report suspicious items or activities to local authorities immediately.

"If You See Something, Say Something™" used with permission of the New York Metropolitan Transportation Authority.

Security Is Everyone's Business

- Identify vulnerabilities.
- Avoid complacency.
- Observe with all senses.
- Be aware.
- Take note of unusual or suspicious behavior.
- Know whom to call.
- Get assistance.

Additional Resources

- Training
- Web pages
- Videos
- Publications

Final Exam

Instructions:

1. **Take a few moments to review the Student Manual and identify any questions.**
2. **Ensure all questions are answered.**
3. **When taking the test . . .**
   - **Read each item carefully.**
   - **Check all work and enter the answers online.**

Feedback

Please complete the course evaluation form.

Your comments are important!