2009 Information Security and Privacy Awareness

This alternate version of the training is for USDA employees, contractors and partners who are unable to complete the training online, in AgLearn. **Every effort should be made to use AgLearn**.

After reading the course material **you also need to take and pass the assessment** that should have been provided to your supervisor. Supervisors are responsible for administering the test. Passing score is 70%.

To get **credit for completing** this version of the training the completion must be reported and recorded. Your agency will provide information on how to do that.

Information Security and Privacy Awareness

Lesson 1: Course Introduction

Welcome.

By taking this course, you are meeting the legal requirement for all users of federal information systems to take annual computer security training. This course is designed to help you understand the importance of Information Systems Security, or ISS, its guiding principles, and what it means for your agency.

It will identify potential risks and vulnerabilities associated with federal information systems, review your role in protecting these systems, and provide guidelines to follow at work and at home to protect against attacks on information systems.

This course consists of six lessons:

1. The Course **Introduction** will provide you with a brief overview of the course.
2. The **Importance of Information Systems Security** lesson will introduce the principles of ISS, its evolution, and ISS-related policies and laws. It will also introduce the critical infrastructure protection program.
3. The **Threats to Information Systems Security** lesson will explain the difference between threats and vulnerabilities. It will also provide information regarding various types of threats.
4. The **Malicious Code** lesson will introduce the concept of malicious code, including its impacts and the methods it uses to infect information systems.
5. The **User Roles and Responsibilities** lesson will identify important guidelines for ensuring a secure system, define classification levels for federal information, and outline your role as a user in protecting this information.
6. Finally, the **Personal and Home Computer Security** lesson will introduce the threats associated with identity theft and the vulnerabilities presented by e-commerce. It will also provide security tips to practice in your daily routine to increase your home computer security.

After completing this course, you should be able to:

- Identify what information systems security is and why it is important.
- Explain the difference between a threat and vulnerability, and identify the risks associated with each.
- Understand the threat posed by malicious code and identify how to protect federal information systems from malicious code.
- Explain the classification levels for federal information and identify what you must do to help protect federal information.
- Identify the guidelines you should follow to secure your home computer system.

Information Security and Privacy Awareness

Lesson 2: Importance of Information Systems Security (ISS)

The Internet has made it extremely easy to quickly obtain and transfer information. While global connectivity is very convenient, it also increases our vulnerability to outside attacks. The goals of ISS are to protect our information and information systems.

ISS protects information from unauthorized access or modification and ensures that information systems are available to its users.

This means that a secure information system maintains **confidentiality**, **integrity**, and **availability**.

History of ISS

Fifty years ago, computer systems presented relatively simple security challenges. They were expensive, understood by only a few, and isolated in controlled facilities.

Protecting these computer systems consisted of controlling access to the computer room and clearing the small number of specialists who needed such access.

As computer systems evolved, connectivity expanded, first by remote terminals, and eventually by local and wide-area networks, or LANs and WANs.

As the size and price of computers came down, microprocessors began to appear in the workplace and homes all across the world.

What was once a collection of separate systems is now best understood as a single, globally connected network. ISS now includes infrastructures neither owned, nor controlled by the federal government. Because of this global connectivity, a risk to one is a risk to all.

ISS Legal Requirements

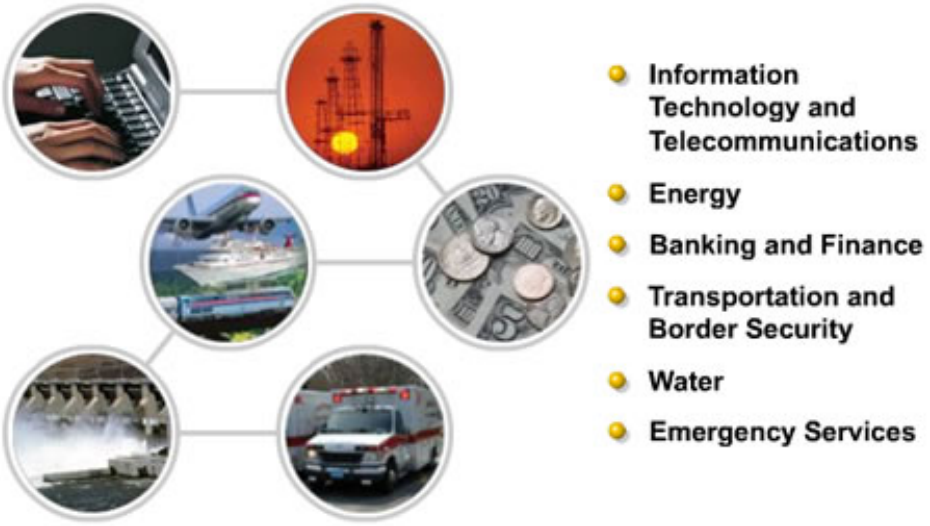
It is important that you are aware of the possibility of attacks against federal systems and the method in which potential attacks could occur.

Understanding your responsibilities for protecting information resources and how you can contribute to preventing attacks will contribute to the safety of federal information systems.

The Federal Information Security Management Act, or FISMA; and the Office of Management and Budget, or OMB, Circular A-130 require that all users of federal computer systems be trained in information systems security concerns. U.S. Office of Personnel Management, or OPM, regulations also require each agency to have computer security awareness training.

Critical Infrastructure

Critical Infrastructure Protection, or CIP, is a national program established to protect our nation's critical infrastructures. Critical infrastructure refers to the physical and cyber-based systems essential to the minimum operations of the economy and government.



Sectors considered part of our nation's critical infrastructure include, but are not limited to, information technology and telecommunications, energy, banking and finance, transportation and border security, water, and emergency services. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. However, these infrastructures have become increasingly automated and interlinked. Increased connectivity creates new vulnerabilities.

Equipment failures, human error, weather, as well as physical and cyber attacks impacting one sector, could potentially impact our nation's entire critical

infrastructure. For example, if the natural gas supply is disrupted by a computer virus, and electrical power is cut, computers and communications would shut down. Roads, air traffic, and rail transportation would also be impacted. Emergency services would be hampered. An entire region can be debilitated because an element critical to our infrastructure has been attacked.

CIP was established to define and implement proactive measures to protect our critical infrastructure and respond to any attacks that do occur.

Information Security and Privacy Awareness

Lesson 3: Threats to Information Systems Security

Threats and Vulnerabilities

It is important to understand the difference between threats and vulnerabilities and how they can affect your system.

A threat is any circumstance or event 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.

A vulnerability is a weakness in an information system or its components that could be exploited. Vulnerabilities exist when there is a flaw or weakness in hardware or software that could be exploited by hackers. Vulnerabilities are frequently the result of a flaw in the coding of software. To correct the vulnerability, vendors issue a fix in the form of a patch to the software.

Threat Categories

There are two types of threat categories: environmental and human threats.

Natural environmental events, including lightning, fires, hurricanes, tornadoes, or floods, pose threats to your system and information. A system's environment, including poor building wiring or insufficient cooling for the systems, can also cause harm to information systems.

Human threats can be internal or external. An internal threat can be a malicious or disgruntled user, a user in the employ of terrorist groups or foreign countries, or self-inflicted unintentional damage, such as an accident or bad habit.

An external threat can be hackers, terrorist groups, foreign countries, or protesters.

Internal vs. External Human Threats

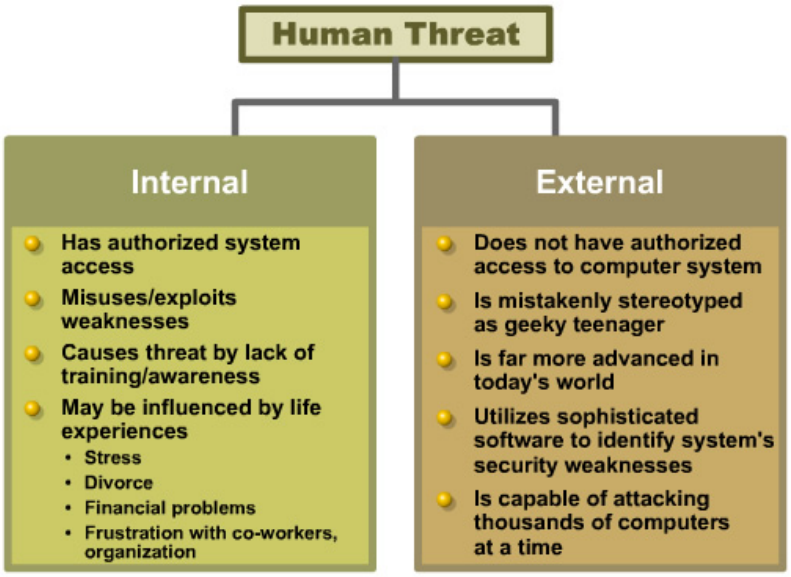
Internal/Insider Threat

External/Outsider Threat

Let's look more closely at human threats to federal information systems. The greatest threats to federal information systems are internal, from people who have working knowledge of, and access to, their organization's computer resources.

An internal threat, or insider, is any person who has legitimate physical or administrative access to the computer system. Insiders can misuse or exploit weaknesses in the system. Others, due to lack of training and awareness, can cause grave damage. Although there are security programs to prevent unauthorized access to information systems, and employees undergo background investigations, certain life experiences can alter people's normal behavior and cause them to act illegally. Stress, divorce,

financial problems, or frustrations with co-workers or the organization are some examples of what might turn a trusted user into an insider threat.



External threats, or outsiders, are most commonly hackers. An outsider is an individual who does not have authorized access to an organization's computer system. In the past, hackers have been stereotyped as socially maladjusted teenagers trying to crack one computer at a time.

Today's hacker may include representatives of foreign countries, terrorist groups, or organized crime. Today's hacker is also far more advanced in computer skills and has access to hacking software that provides the capability to quickly and easily identify a system's security weaknesses. Using tools available on the Internet, a hacker is capable of running automated attack applications against thousands of host computers at a time. Because of this, hackers pose a serious risk to the security of federal information systems.

Social Engineering Overview

Social engineering is a hacking technique that relies on human nature. This approach is used by many hackers to obtain information valuable to accessing a secure system.

Rather than using software to identify security weaknesses, hackers attempt to trick individuals into revealing passwords and other information that can compromise your system security.

They use social engineering tactics to learn passwords, logon IDs, server names, operating systems, or other sensitive information. For example, a hacker may attempt to gain system information from an employee

by posing as a service technician or system administrator with an urgent access problem.

Nobody should ever ask you for your passwords. This includes system administrators and help desk personnel.

Your Role in Social Engineering

Preventing social engineering:

- Verify identity
- 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

Reacting to social engineering:

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

Understanding social engineering behaviors will enable you to recognize them and avoid providing important security information to unauthorized sources.

Phishing

A social engineering scam that you need to be aware of is phishing. Phishing is a high-tech scam that uses email or websites to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

Phishers send an email or pop-up message that claims to be from a business or organization that you deal with. For example, phishers often pose as your Internet service provider, bank, online payment service, or even a government agency. The message usually says that you need to update or validate your account information. It might threaten some dire consequence if you don't respond. The message directs you to a website that looks just like a legitimate organization's site, but it is not affiliated with the organization in any way.

The purpose of the bogus site is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name. The bogus site may also install malicious code on your system.

If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message.

Legitimate companies do not ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine.

A recent real life example of social engineering occurred when a U.S. government employee, visiting another country, provided his business card to several people.

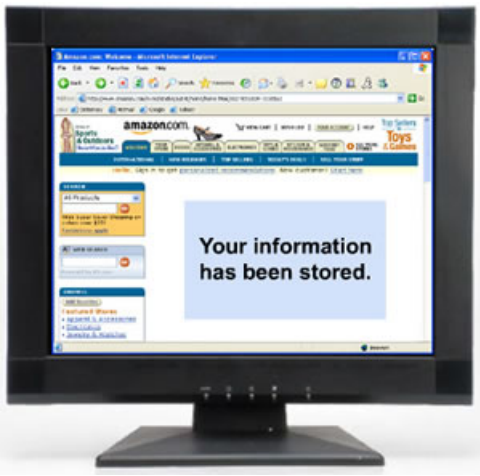
A few months later, a highly-visible U.S. government official received an "official-looking" e-mail containing an attachment from a valid ".gov" address.

Fortunately, the recipient did not open the e-mail's attachment, but instead, sent the email back to the person whom he thought sent it to him for verification.

It turns out that the originating e-mail spoofed the email address of the government employee who traveled to the foreign country. The attachment contained malicious code.

Cookies

There are several security risks associated with browsing the Internet. One common risk is known as cookies.



A cookie is a text file that a web server stores on your hard drive when you visit a website. The web server retrieves the cookie whenever you revisit that website. When you return, the cookie recognizes you, saving you the trouble of re-registering.

The most serious security problem with cookies has occurred when the cookie has 'saved' unencrypted personal information, such as credit card numbers or Social Security numbers, in order to facilitate future business with that site.

Another problem with cookies is that the site potentially can track your activities on the web.

To reduce the risk associated with cookies, and better protect your system, your browser should be set up not to accept cookies.

Mobile Code

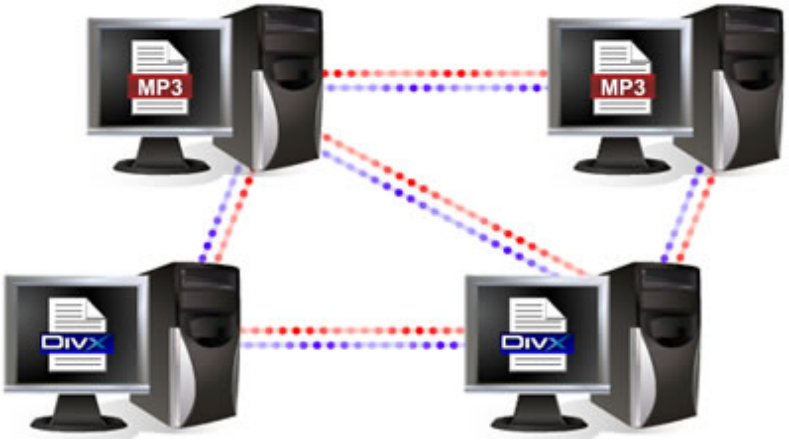
Mobile code, such as ActiveX and Java, are scripting languages used for Internet applications.

Mobile code embedded in a web page can recognize and respond to user events such as mouse clicks, form input, and page navigation. It can also play audio clips.

However, it does introduce some security risks. Mobile code can automatically run hostile programs on your computer without your knowledge simply because you visited a web site. The downloaded program could try to access or damage the data on your machine or insert a virus.

Your agency may have developed policy guidance for the use of mobile code. If so, it may restrict the application of mobile code in your agency's information systems. If you have a question regarding the use of mobile code, contact your help desk or security point of contact.

Peer-to-Peer (P2P)



Peer-to-peer, or P2P, refers to file sharing applications, such as Morpheus and BitTorrent, that enable computers connected to the Internet to transfer files to each other.

Peer-to-peer software enables files to be accessed and transferred with ease. However, there are legal, ethical, and security concerns associated with the use of unauthorized peer-to-peer applications.

Music files, pornography, and movie files are the most commonly transferred files using unauthorized peer-to-peer software. Obtaining these files at no cost raises not only ethical concerns, but could result in criminal or civil liability for illegal duplication and sharing of copyrighted material. Additionally, participating in peer-to-peer file sharing increases your vulnerability. Opening up your computer via the Internet provides outsiders a link into your system, creates risk and enables the possibility for a breach in security.

Peer-to-peer is a common avenue for the spread of computer viruses and spyware.

The installation and use of unauthorized peer-to-peer applications can also result in significant vulnerabilities to your agency's networks, including exposure to unauthorized access of information and compromise of network configurations.

Office of Management and Budget, or OMB, requires all Agencies to develop guidance on the use of peer-to-peer applications.

Contact your security point of contact for further information on your specific policy regarding the use of peer-to-peer applications.

Information Security and Privacy Awareness

Lesson 4: Malicious Code

What is Malicious Code?

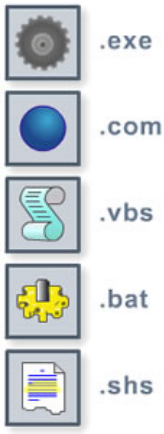
Malicious code is defined as software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

It is designed with the intent to deny, destroy, modify, or impede systems configuration, programs, or data files.

Malicious code comes in several forms including viruses, Trojan horses, and worms.

The most common methods for the spread of malicious code are through email attachments and downloading files from the Internet, but you can also get malicious code just from visiting web sites.

Email and Attachments



Email messages and email attachments provide a common route to transfer malicious code.

Always be cautious when opening email attachments – they may contain malicious code that could corrupt files, erase your hard drive, or enable a hacker to gain access to your computer. Specific attachments to look for that could contain malicious code are those ending in .exe, .com, .vbs, .bat, and .shs.

Don't assume that an attachment is safe because a friend or coworker sent it. Save the attachment to your hard drive and scan it with current anti-virus software before opening it. Some malicious code is activated by merely opening the message.

Protect Your Computer System

- Scan email attachments and outside files using current anti-virus software
- Ensure system is scanned daily
- Delete email from unknown or unexpected sources
- Turn off option to automatically download attachments

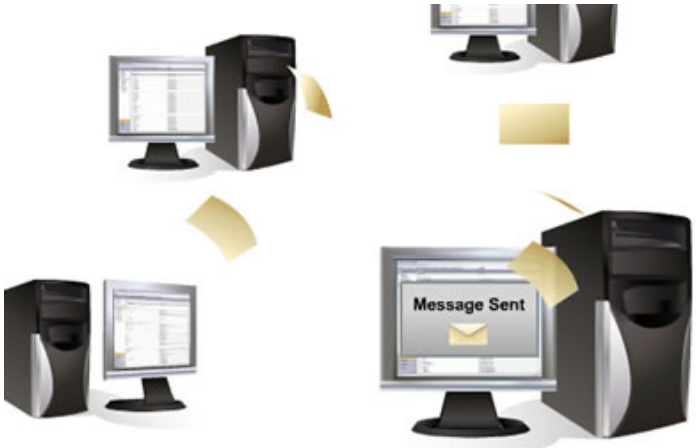
Respond to Virus Attack

- Do not email the infected file
- Contact help desk or security contact

Hoaxes

Internet hoaxes are email messages designed to influence you to forward them to everyone you know.

Hoaxes encourage you to forward email messages by warning of new viruses, promoting moneymaking schemes, or citing a fictitious cause. By encouraging mass distribution, hoaxes clog networks and slow down Internet and email service for computer users.



If you receive an email message requesting that you forward it to all your friends and coworkers, do not forward the email.

Information Security and Privacy Awareness

Lesson 5: User Roles and Responsibilities

Basic User Guidelines

As an authorized user of federal information systems, you have certain responsibilities when using a government machine.

Remember that your rights to privacy are limited when using government computer resources.

Any activity conducted on a government system can be monitored. Each time you log on to a government system, you consent to being monitored. You should use your computer for government business only.

Avoid government computer misuse. Some examples of computer misuse are: viewing or downloading pornography, gambling on the Internet, conducting private commercial business activities or profit-making ventures, loading personal software, or making unauthorized configuration changes.

There are eight basic generally accepted ethical guidelines that should govern your actions when using a government computer system.

Ethical guidelines

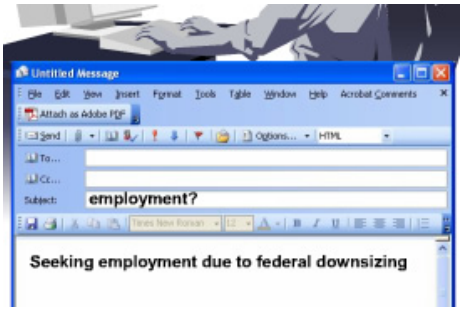
- Do not use computer for harm
- Do not interfere with other's work
- Do not snoop in other's files
- Do not use a computer to commit crimes
- Do not use or copy unlicensed software
- Do not steal intellectual property
- Do not use computer to pose as someone else
- Do not use computer resources without approval

Appropriate Email Use

Email is also for official business. Your organization may permit some incidental and casual email use.

Guidelines on the types of personal email use that may or may not be authorized are as follows:

- Email use may not adversely affect the performance of official duties.
- Email use must not reflect poorly on the government.
- You may not use government email to send pornographic, racist, sexist, or otherwise offensive emails, to send chain letters, or to sell anything.
- Email use must not overburden the system, as happens when you send mass emails.
- To keep networks open and running efficiently, don't forward jokes, pictures, or inspirational stories.
- Similarly, avoid using *Reply All* unless it is absolutely necessary.
- Personal email use may be authorized if it is of reasonable duration and frequency, preferably on employees' personal time, such as on a lunch break.



- Email is also permissible when it serves a legitimate public interest, such as allowing employees to search for a job in response to federal government downsizing.

Public Key Infrastructure

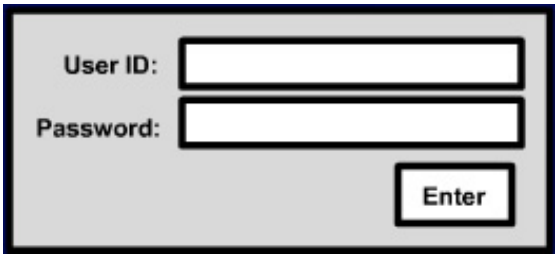
Federal information systems identify and authenticate each user either through a smart card login or user ID and password.

The preferred method of access to information systems is through the use of public key infrastructure, or PKI, which enables your agency to issue electronic keys, called digital certificates, to authorized users.

PKI allows users to encrypt and digitally sign emails and documents.

Tips for Creating a Secure Password

Many federal information systems still identify and authenticate users by his or her user ID and password. The user ID and password determines the user's right to access the system.



Remember, it is your responsibility to ensure that all activity done under your user ID is appropriate use of federal information systems resources.

It is important to create a complex password in order to protect government information systems from being compromised.

- Combine letters, numbers, special characters
- Use alphanumeric combinations or phrase associations
- Avoid words or phrases in dictionary
- Avoid using personal information
- Memorize password and refrain from writing it down
- Change password regularly

Physical Security

Protecting federal information systems and the information they contain starts with physical security, commonly referred to as guns, gates, and guards.

Physical security includes protection of the entire facility, from the outside perimeter to the offices inside the building, including all the information systems and infrastructure.

You are responsible for knowing your organization's physical security policies and following them. Your organization should have procedures for gaining entry, procedures for securing your work area at night, and emergency procedures. These may include:

- the use of a badge or key code for entry
- locking your cubicle
- undocking your laptop and storing it in a separate location
- locking data storage devices, such as hard drives and thumb drives, before you leave for the evening and during emergency procedures such as fire alarms.

You should also make sure others follow your organization's physical security policies and challenge people who don't. Don't allow people to gain entrance to a building or office by following someone else instead of using their own badge or key code.

Challenge people who do not display badges or passes. If you are the last person to leave in the evening, make sure that others have secured their equipment properly.

Finally, you are responsible for reporting any suspicious activity that you see.

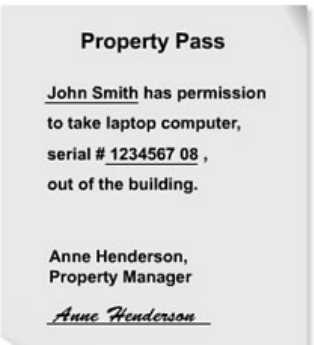
Inventory Control

Part of physical security includes controlling the inventory of equipment that stores federal information. When government laptops are lost or stolen, so is the information that is on them. In recent years, federal inventory control procedures have been tightened in response to the loss of thousands of government laptop computers.

Federal agencies are responsible for controlling their inventory of office and computer equipment, including phones, computers, printers, faxes, monitors, and thumb drives.

When you receive government property, you should sign for it. Once it has been signed out to you, you are then responsible for that equipment and taking the necessary precautions to ensure that it doesn't get lost or stolen.

To remove equipment from the building, or bring equipment into the building, your organization may require you to have a property pass signed by the property manager.



If that property is lost or stolen, follow your organization's procedures for reporting the loss. In addition to reporting the loss of the equipment itself, you must report the loss of the information that was on the equipment, and the significance of that lost information.

Telework Procedures

Telework, also known as telecommuting, is emerging as a viable option for many government employees. Advances in computer and telecommunications capabilities make telework increasingly practical.

There are risks associated with remote access to your government computer network.

If you have received approval for telework, you are required to satisfy the requirements in your agency's policies and guidelines.

Classified and Unclassified Information

All federal information, combined with the right conditions and circumstances, could provide an adversary insight into our capabilities and intentions. Additionally, the aggregation of unclassified information can elevate the sensitivity level of information.

Thus, even unclassified information, if compromised, could impact the safety of our personnel and systems.

All federal unclassified information not specifically cleared for public release requires some level of security protection. At a minimum, it must be reviewed before it is released, in any form, outside the U.S. government. Each agency has its own unclassified information policy. Contact your security point of contact for additional information on your agency's policy.

Unclassified Information:

- For Official Use Only, or FOUO; Controlled Unclassified Information, or CUI; and Sensitive But Unclassified, or SBU,
- Examples are personnel, financial, payroll, medical, operational, and Privacy Act information
- CUI must be stored in a locked drawer or secure container. When it is no longer needed, it should be destroyed.

Classified information:

- Confidential, Secret, or Top Secret
- The specific level of classification is determined by the original classification authority
- Must be used in an area that has been approved and cleared for the appropriate classification level
- When not in use, must be stored in a General Services Administration, or GSA, approved vault or container

Backups, Storage, and Labeling

A large amount of federal information is stored on removable media such as CDs, thumb drives, pen drives, or removable hard drives. Because these devices can store large amounts of information, you need to take extra precaution to protect them from loss or theft.

It is essential that important files are backed up on a regular basis and stored in a secure location. This will minimize the loss of data if your hard drive crashes or is infected by a virus.

Store all removable media, including CDs, thumb drives, and removable hard drives in solid storage containers, such as metal cabinets, to protect against fire and water damage.

It is very important to label all removable media, including backups, and the contents of the media, to reflect the classification or sensitivity level of the information the media contains.

Removable media must be properly marked and stored according to the appropriate security classification of information it contains.

When you no longer need the information on the removable media, you should not erase, or "sanitize" the information. Removable media must be degaussed or destroyed if it is not reused at the same or higher classification level of the system in which it was used.

Follow your agency's policies regarding handling, storage, labeling, and destruction of removable media.

Media Devices

Be extremely careful when using fax machines, cell phones, laptops, personal digital assistants, or PDAs, and wireless networks. You need to be as vigilant about security on these devices as you are with your computer at work.

Fax Machines
When transmitting sensitive information over a fax machine, ensure that the recipient will be present to pick up the fax immediately. Contact the recipient directly to confirm receipt of the fax. Never transmit classified information via an unsecured fax machine.

Always use a cover sheet so that the content of your fax isn't immediately visible.

Cell Phones
If you use a cell phone, anyone with the right equipment could potentially listen to your conversation. Cell phones are merely transmitters.

Use a landline for more privacy, and never discuss sensitive information on an unsecured phone.

PDAs
Personal digital assistants, or PDAs, such as Blackberrys, or Palm Pilots, pose a security threat for a number of reasons.

Their small size and low cost make them easy to obtain and difficult to control.

They have tremendous connectivity and storage capabilities, and are extremely popular. It can be very easy for a person to set up a PDA to download information from your computer.

All PDAs connecting to government systems should be in compliance with your agency's policy and OMB guidance.

Laptops
The convenience of laptops and other portable computing devices also makes them extremely vulnerable to theft or security breaches.

User logon information should always be password protected.

Be careful what you display on your screen when it is visible by others, especially in close quarters, such as on airplanes.

Maintain possession of your laptop at all times when traveling to prevent theft. When reaching your temporary travel destination, be sure that your laptop is properly secured when left unattended.

If your laptop has wireless capability, ensure that the wireless security features are properly configured in accordance with your agency's wireless policy. When not in use, laptop wireless should be turned "off" or, if this is not possible, configured to connect to recognized Internet access points, not ad hoc networks.

The Office of Management and Budget, or OMB, issued a memorandum stating that all sensitive data stored on laptops and other portable computer devices should be encrypted. Ensure that you follow both your agency's and OMB's guidance on encryption of sensitive data on laptops.

Wireless Network
Wireless networks operate by using radio signals, instead of traditional computer cables, to transmit and receive data.

Unauthorized users with a receiver can intercept your communications and can access your network.

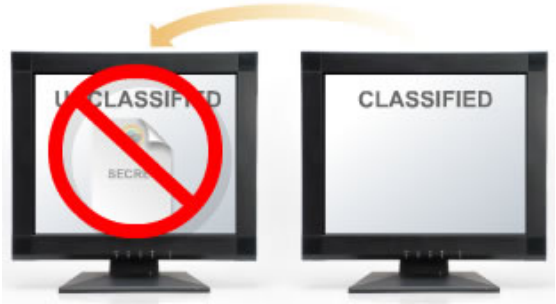
This is dangerous because unauthorized users may be able to capture not only the data you are transmitting, but also any data stored on your network.

Ensure you are in compliance with your agency's policy regarding the use of wireless technologies.

Spillage

Spillage, also referred to as contamination, is when information of a higher classification level is introduced to a network at a lower classification level. It is the improper storage, transmission, or processing of classified information on an unclassified system.

An example would be when information classified as Secret is introduced to an unclassified network. Any user who identifies or suspects that a spillage has occurred should immediately notify his or her security point of contact.



Cleaning up after a spillage is a resource intensive process. It can take roughly three weeks to contain and clean an affected information system. Be aware that spillages can greatly impact the security of federal information

Helpful hints:

- Check all emails for possible classified information
- Mark and store all removable media properly
- Ensure all file names and subject headers reveal the sensitivity of the information

Personal Information

The Privacy Act, signed into law in 1975, requires the government to safeguard information about individuals that is processed by federal agency or contractor computer systems. The act also requires the government to provide access to the information by the individual and to amend the information if it is not accurate, timely, complete or relevant.

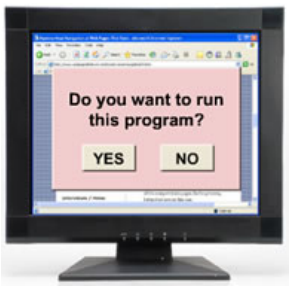
New guidance concerning greater measures for protection of personally identifiable information, or PII, is outlined in several OMB Memoranda.

For example, OMB requires that lost or stolen PII be reported within one hour to the U.S. Computer Emergency Response Team, or CERT.

Each agency has its own policies to implement OMB's guidance. Check with your security point of contact for additional PII requirements.

As an authorized user, you should ensure that personally identifiable information is protected on federal computer systems.

Your Responsibility



Information is a critical asset to the U.S. government. It is your responsibility to protect government sensitive and classified information that has been entrusted to you.

Please contact your security point of contact for more information about classification or handling of information.

Information Security and Privacy Awareness

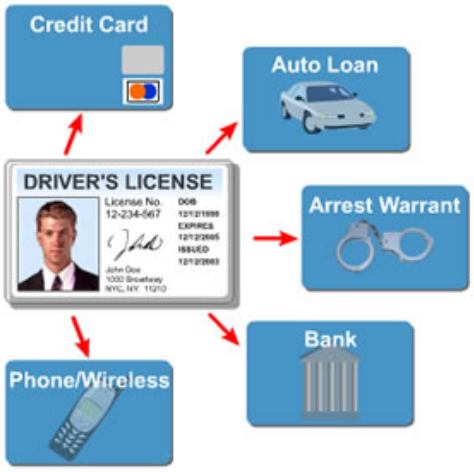
Lesson 6: Personal and Home Computer Security

Identity Theft

According to FBI statistics, identity theft continues to be the nation's fastest growing crime.

Identity theft occurs when someone uses your name, address, Social Security number, bank or credit card account number, or other identifying information without your knowledge to commit fraud or other crimes.

Identity thieves can use the information they obtain to open credit card accounts, take out loans, or drain a bank account without your knowledge.



Identity theft is a serious problem with extreme consequences for its victims. You are the first line of defense against identity theft. It is important that you take action to minimize your risk.

Protect your identity:

- Ask how information will be used before giving it out
- Pay attention to credit card and bank statements
- Avoid common names/dates for passwords and PINs
- Pick up mail promptly

- Shred personal documents
- Cancel credit cards you do not use
- Refrain from carrying SSN card and passport
- Order credit report annually

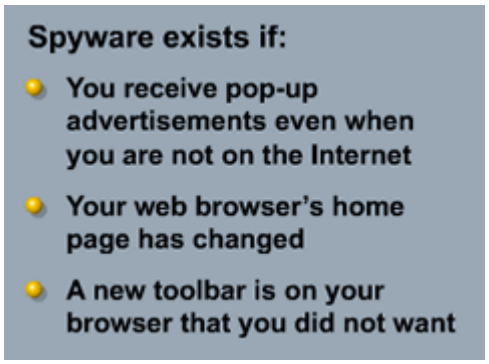
Responding to identity theft:

- Contact credit reporting agencies: Equifax, TransUnion and Experian
- Contact financial institutions/creditors to cancel accounts
    - Credit cards
    - Bank accounts
- Monitor credit card statements for unauthorized purchases
- Report crime to the local police

Spyware

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, without your consent or knowledge.

Your computer might be infected with spyware if: you receive pop-up advertisements even when you're not on the Internet, your web browser's home page has changed, or a new toolbar is on your browser that you didn't want.



There are a number of ways spyware or other unwanted software can get on your system. A common trick is to covertly install the software during the installation of other software you want. Whenever you are installing something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement.

To detect and remove spyware programs from your computer use an up-to-date spyware detection and eradication program that scans and removes this type of software.

Spyware exists if:

- You receive pop-up advertisements even when you are not on the Internet
- Your web browser's home page has changed
- A new toolbar is on your browser that you did not want

Use a spyware detection and eradication program if authorized by your agency.

E-Commerce

Electronic commerce, or e-commerce, refers to business transactions conducted using electronic documents, rather than paper.

E-commerce gives consumers and businesses greater flexibility as to when and how transactions are conducted.

For example, the direct deposit of your salary from your employer's account into your bank account eliminates the need for traditional paper checks.

E-commerce is a common way for individuals to fall victim to identity theft. Conducting business transactions online increases a user's vulnerability to identity theft by transferring personal information over the Internet.

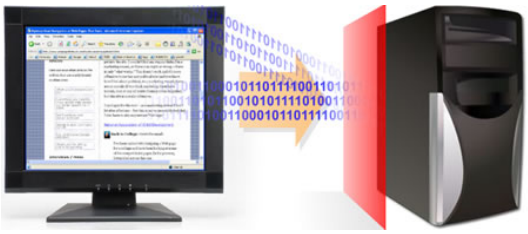
To reduce the risk of identity theft, confirm that the e-commerce site you are using conducts its business over an encrypted link before providing any personal information.

An encrypted link is indicated by "https" in the URL. Note that not all https sites are legitimate and you are still taking a risk by entering your information online.

Basic Security Principles

Security Tips:

- Scan your system regularly with updated software:
  - Anti-virus
  - Spyware detection and eradication
- Scan all email attachments and files downloaded from the Internet
- Delete infected files
- Download software updates and patches regularly
- Install and use firewall when connected to the Internet



- Back up all important files
- Use complex passwords
- Disconnect computer from Internet when not online
- Protect your wireless network with a password
- Be aware of the risks of P2P programs

Distributed Denial of Service (DDoS)

Distributed denial of service, or DDoS, attacks are a threat to Internet security.

These attacks involve bombarding a web server with huge amounts of data from many different machines and locations in an effort to bring the server down and deny its availability.

The attacks can be launched from systems across the Internet, unified in their efforts, or by compromised systems that are controlled by servers, which can hide the true origin of the attack.

You can help mitigate DDoS attacks by practicing safe computing habits to keep your home computer from being used to launch these attacks.

Technology

Security needs must constantly keep pace with ever changing technologies and applications. The rapid pace of technological advances poses new challenges in information systems security.

It is important that you keep up to date on these changes to better protect yourself, your home computer, and federal information systems.

THIS IS THE END OF THE TRAINING MATERIAL.
YOU NOW NEED TO TAKE AND PASS THE ASSESSMENT.
PLEASE CONTACT YOUR SUPERVISOR.

GLOSSARY

Availability
Timely, reliable access to data and information services for authorized users.

Confidentiality
Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Cookie
Text file that a web server stores on your hard drive when you visit a website.

Critical Infrastructure Protection (CIP)
A national program established to protect our nation's critical infrastructures. Critical infrastructure refers to the physical and cyber-based systems essential to the minimum operations of the economy and government.

Distributed denial of service (DDoS)
Attacks that are a threat to Internet security. These attacks involve bombarding a web server with huge amounts of data from many different machines and locations in an effort to bring the server down and deny its availability.

Electronic commerce (e-commerce)
Business transactions conducted using electronic documents, rather than paper.

Information Systems Security (ISS)
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 used to detect, document, and counter such threats.

Integrity
Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Internet Hoax
Email messages designed to influence you to forward them to everyone you know.

Federal Information Security Management Act (FISMA)

- Mandates a computer security program at all federal agencies
- Provides for development and maintenance of minimum controls required to protect federal information systems
- Provides comprehensive framework for ensuring effectiveness of information security controls
- Requires agencies to identify risk levels and implement appropriate protections
- Requires each agency to develop and maintain an inventory of major information systems
- Requires government employees and contractors using these systems to undergo periodic computer security training
- Requires that agencies report to Congress on FISMA compliance
- Defines national security systems

Malicious code
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Office of Management and Budget (OMB) Circular A-130, Appendix III
Requires all federal information systems to:

- Possess information security plans
- Address computer security in reports to Congress through OMB
- Provide computer security awareness and training for system users, operators, and managers
- Conduct improved contingency planning
- Maintain formal emergency response capabilities
- Assign a single individual operational responsibility for security

Peer-to-peer (P2P)
Refers to file sharing applications that enable computers connected to the Internet to transfer files to each other, such as Morpheus and BitTorrent.

Personally Identifiable Information (PII)
Any information about an individual maintained by an agency, including, but not limited to education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information that is linked or linkable to an individual.

Phishing
A high-tech scam that uses email or websites to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

Spillage
When information of a higher classification level is introduced to a network at a lower classification level. It is the improper storage, transmission, or processing of classified information on an unclassified system.

Spyware
Malicious software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, without your consent or knowledge

Threat
Any circumstance or event 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.

Vulnerability
A weakness in an information system or its components that could be exploited. Vulnerabilities exist when there is a flaw or weakness in hardware or software that could be exploited by hackers. Vulnerabilities are frequently the result of a flaw in the coding of software. To correct the vulnerability, vendors issue a fix in the form of a patch to the software.

THIS IS THE END OF THE TRAINING MATERIAL.
YOU NOW NEED TO TAKE AND PASS THE ASSESSMENT.