DOL New Hire Training: Computer Security and Privacy

Table of Contents

Introduction

- The Security Awareness Training is divided into four sections:.
  - The first section, Computer Security Basics, will focus on the key concepts in computer security. You will learn about the importance of safeguarding our data and keeping our network secure.
  - The second section, Protecting Personally Identifiable Information, will talk about the various types of PII, the importance of keeping PII secure, and the steps DOL has taken to accomplish that goal.
  - In the third section, Appropriate Use Policies, we will cover policies related to using DOL computers and the network. You will learn about what you are allowed to do and what you are not allowed to do using DOL equipment.
  - And in the last section, Good Security Practices, you will learn about the important practical steps you can take to help keep DOL data and computers secure.
- By the end of this training, you will be able to identify information security risks associated with using a government computer. You will know the rules of appropriate behavior when using DOL computers. You will also be able to recognize a security incident and respond to it appropriately.

Lesson One: Computer Security Basics

Risk Awareness

Lesson 1.1 Risk Awareness

- DOL computer systems are important to our job functions. However, networked computers and the Internet pose some significant security risks:
  - Information passing between computers might be intercepted or misdirected.
  - Hackers may exploit weaknesses in security to get access to things that should stay protected.
  - Viruses can spread from computer to computer over the network, damaging our systems and endangering reliability
  - Sensitive information, if it gets into the wrong hands, can be used for identity theft and fraud.

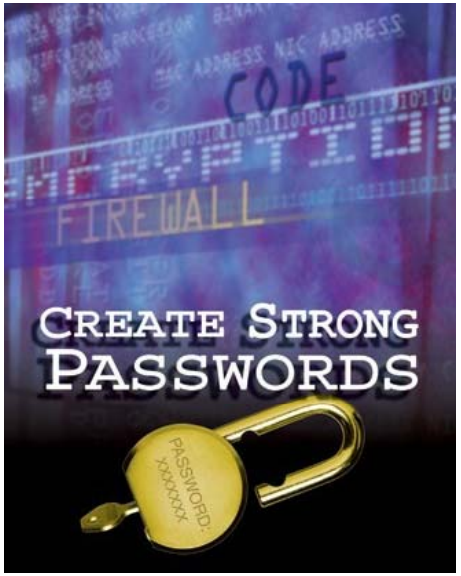
- Because of these risks, DOL has developed comprehensive security policies and practices that we all must follow.

- Strong security depends on the cooperation of all of us.

User Responsibilities

Lesson 1.2 User Responsibilities

- Because DOL is committed to safeguarding the confidentiality and integrity of its information resources, all staff using DOL computers are required to understand and adhere to our security policies and practices. These include the following requirements:
  - Safeguarding sensitive data like Personally Identifiable Information (PII)
  - Implementing sound physical security practices
  - Refraining from inappropriate use of DOL technology
  - Adhering to strict password standards
  - Employing our Computer Security Incident Response Capability (CSIRC) to ensure that if a security incident does arise, our staff members are prepared to handle it
- Ultimately, staff training is the first line of defense in our network security strategy.



Lesson Two: Protecting Personally Identifiable Information

ur Responsibility to Protect PII

Lesson 2.1 Our Responsibility to Protect 'PII'

- The loss of Personally Identifiable Information or 'PII,' has become a major problem in recent years.
- A recent report from ComputerWorld magazine found that "Data loss was widespread at government agencies - Since 2003, 19 agencies have reported at least one loss of personal information."
- What is PII? PII is defined by DOL as any information about an individual which can be used to distinguish or trace an individual's identity.
  - PII examples include all of the following :
    - First and last name, email address, business address
    - Gender, race, ID badge or identification number
    - Credit card number, bank account number, home address
    - Photo, fingerprints, date and place of birth, mother's maiden name, criminal or medical records
- It is DOL policy to comply with all Federal mandates and laws that govern the protection of PII and other sensitive data.

Overview of PII

Lesson 2.2: Overview of Personally Identifiable Information

- DOL policy defines two types of PII: Non-Sensitive PII and Protected PII
  - Non-Sensitive PII is PII whose disclosure cannot be expected to result in personal harm
    - Examples: First and last name, email address, business address, business telephone, general education credentials, gender or race, etc.
  - Protected PII is PII of a sensitive nature whose disclosure could result in harm to an individual.
    - Protected PII is often truly unique to a particular person; such as a Social Security Number, biometric data like a fingerprint, or a credit card number.
- Next, we will focus on Protected PII and DOL' s commitment to safeguarding it.

Focus on Protected PII

- As we've discussed, Protected PII is information that is often unique to an individual. Examples include but are not limited to:
  - Social Security Number, credit card numbers, legal documents, bank account number, home address, vehicle identifiers, home and/or personal phone numbers, photo, fingerprints, date and place of birth, mother's maiden name, criminal, medical, and financial records.
- Any of these pieces of Protected PII, even by themselves, could allow an identity thief or other criminal to harm a DOL student or staff member.
- That's why DOL is highly committed to safeguarding Protected PII and has implemented security policies to accomplish that goal.

Safeguarding PII

Lesson 2.4 Procedures for Safeguarding PII

- Protected PII is the most sensitive information that you may encounter in the course of your duties at DOL and it is vitally important that we remember to safeguard it.

- Lets talk about the things you can do to help DOL protect PII:
  - Staff may not use personally owned or public computers to download or store protected PII without approval.
  - Always use Pointsec Media Encryption (PME) to encrypt data that is moved to a portable device like a thumb drive, CD or floppy disk.
  - Immediately report any missing documents or equipment that contains Protected PII to your agency Information Security Officer (ISO).

- For details on how to handle media and documents containing PII; including labeling, storage, disposal, and shipping, see Department of Labor Manual Series DLMS-9-1200, "DOL Safeguarding Sensitive Data Including Personally Identifiable Information".

Safeguarding PII with Encryption

Lesson 2.5 Safeguarding PII with Encryption

- We've discussed the things that you can do to protect PII, now let's take a look at the things DOL is doing.
- The loss of PII has become a major problem in recent years. Because of this risk, on June 23, 2006, the Office of Management and Budget (OMB) distributed a mandate to protect PII. This directive required that DOL take the following steps to protect PII:
  - All workstations and laptops in the DOL system now have Pointsec Media Encryption (PME) software installed. Encryption is the process of transforming information to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. PME encrypts and password-protects any data exported to a removable media device.
  - DOL has also issued laptop computers with full disk encryption, removable media encryption, and two-factor authentication to thousands of staff members that access the network remotely.
  - Remote access to DOL systems has been limited and further protected with additional security measures including two-factor authentication, SSL Virtual Private Networking (VPN), as well as the disabling of downloading & local drive mapping through Citrix.
- These security initiatives have greatly increased the security and integrity of DOL data. We will discuss Pointsec Media Encryption (PME) in more detail later in the training.

Lesson 3: Appropriate Use Policies

Appropriate Use

Lesson 3.1: Appropriate Use

- Your Agency's Rules of Behavior outline how staff may use government-owned resources.
  - This includes computers, telephones, fax machines, photocopiers, email, and the Internet.
- Here are some general guidelines:
  - To keep our network running smoothly, staff should refrain from using DOL resources to run an outside business or conduct trade online.
  - Government property, such as laptops or PDAs, should only be taken from your office for approved business reasons, like work-related travel.
  - Because DOL is part of the Federal Government, staff should not do any fundraising, make endorsements, lobby for an issue, or perform political activities using DOL resources.

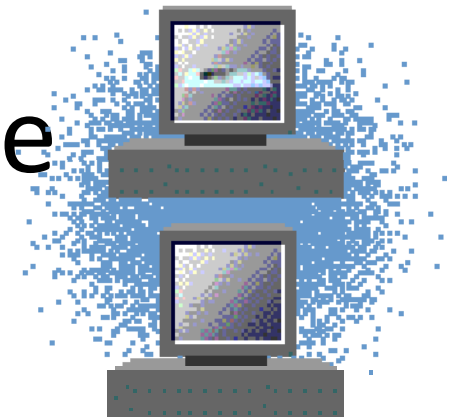
- In the next portion of this training, we'll look at some additional guidelines to follow when using the DOL network.

Personal Use of the Internet

Lesson 3.2: Personal Use of the Internet

- Here are some guidelines to follow when using the DOL network
- Keeping our network running smoothly is very important to DOL. But some popular technologies, like streaming video and music, live stock market feeds, and sports updates can bring a network to its knees and severely affect performance. DOL employees are expected to refrain from using government equipment for such activities
- In order to protect the network from threats including viruses, worms and spyware, Peer-to-Peer file sharing which is not DOL or Agency moderated and controlled shall not be allowed on DOL or Agency systems or infrastructure
- To help combat identity theft and fraud, staff should refrain from buying or selling merchandise and services online.
- To prevent the spread of malicious software like spyware, you should only install software that has been approved by DOL.
- For more information on DOL's policies on Internet usage, refer to DLMS-9-900, "Appropriate Use of IT"

Email-Appropriate Use



Lesson 3.3: Email – Appropriate Use

- Email is a powerful tool for communication. However, because of the easy and familiar nature of it, it's easy to forget that DOL Email is not private and needs to be used with care.
- Use the following guidelines when using our email system:
  - To help fight the spread of spam email, staff should not send or forward any chain letters, junk-mail, or hoax related email, and be cautious when using the "Reply to All" feature.
  - If you receive a notice regarding a computer virus, do not forward it. Sometimes virus warnings actually contain viruses. Virus alerts will come from official DOL sources. It's the Security Team's job to look out for new viruses and protect our systems.
  - Be professional, courteous and remember that your email account is not private. Assume that every email you write will be read by your coworkers.

Representing DOL Professionally

Lesson 3.4: Representing DOL Professionally

- While performing your duties at DOL, bear in mind that you are representing DOL when you use your network account. Be professional, courteous and use common sense.
- In order to create a safe and professional workplace, DOL policy prohibits viewing certain content like adult-oriented material, information or Web sites that promote racism, bigotry and unlawful or violent acts. Obviously, these activities are not allowed for good reasons and DOL implements certain technologies to prevent users from engaging in them.
- Also, to help keep our network and data secure, Federal law prohibits staff from turning off security software or using any tools to bypass security measures or disrupt operation of the network.
- You should know that using any DOL computer system means that you consent to having your activities monitored and recorded, so staff can have no expectation of privacy.
- Since you are representing DOL, you need to be careful what you post online or say in email. When people see your email address, they might assume that you represent DOL in an official capacity and your personal views may be taken as though they were the views of DOL.
- If you must express personal opinions via email, you should add the following disclaimer to the message: "The contents of this message are mine personally and do not reflect any position of the Government or my agency."
- If you have any questions about DOL policy, please consult DLMS-9-900

Lesson 4: Good Security Practices

Good Security Practices Overview

Lesson 4.1: Good Security Practices Overview

- By now, we hope you have a better understanding of the security risks associated with using a DOL computer.
- Section 4, the final section of this training, provides an overview of good computer security practices.
- You'll learn how to use encryption to protect data on mobile devices, how to secure your work area, and how to protect against viruses, hackers and other threats.
- And we'll also cover password protection and show you what to do if you notice a security incident.
- You are responsible for complying with DOL policies and procedures, which will help to reduce our computer security risks.

Security for Mobile Devices

Lesson 4.2: Security for Mobile Devices

- As part of your duties at DOL, you may be required to travel or work from home using mobile computing devices like laptops and PDAs, or portable storage devices like USB thumb drives, that can access PII via the DOL network.
- It is your responsibility to ensure that these devices and the data they contain are kept secure at all times.
- Some guidelines for protecting mobile devices are these:
  - Mobile computing and storage devices like laptops, PDAs, and USB drives must be kept in your direct possession.
  - If you must leave the device, put it in a locked drawer or a security locker.
  - Secure your laptop with a strong password and use encryption to secure the contents of mobile storage devices.
  - USB thumb drives, CDs, DVDs, portable hard-drives, floppy disks, and other data storage devices must not contain protected PII or other sensitive data unless the data is protected with encryption
  - If something is lost or stolen, report it to your Information Security Officer (ISO) within 1 hour of discovery.

Pointsec Media Encryption

Lesson 4.3: Pointsec Media Encryption

- As we've discussed, encryption technologies play a large part in DOL's security strategy. Encryption is the process of transforming data to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. If you must store data on a mobile device, DOL has provided you with an easy way to protect the data with encryption using Pointsec Media Encryption (PME).
- All workstations and laptops in the DOL system now have Pointsec Media Encryption (PME) software installed.
- PME encrypts and password-protects any data exported to a removable device.
- To decrypt your data, simply double-click the PME.exe utility that has been copied to the mobile device and enter the correct Account name and Password.
- There are several methods for exporting files that are commonly used by DOL users:
  - The Send to menu option, Save as, Copy and Paste, and Drag and Drop
  - Staff can also use the new Encryption right-click menu option to create an encrypted package for export to a CD.
  - Commonly used mobile devices include USB thumb drives, CDs, DVDs, portable hard-drives, floppy disks and flash memory sticks.

Physical Security

Lesson 4.4: Physical Security and Environmental Controls

- Physical Security controls help prevent theft, fraud and information abuse by keeping unauthorized people away from our systems.
- It is important to remember your role in creating a secure workplace.
- When you are required to, remember to turn in all DOL issued equipment, badges, and work files.
- Always secure your computer by locking it when you leave for any length of time. To lock it, simply press and hold Ctrl + Alt + Del and hit Enter.
- Remember to report unauthorized building access attempts to your security guard or facilities management personnel.

Protecting Against Hackers

Lesson 4.5: Protecting Against Hackers

- Hackers sometimes use sophisticated methods to break into computers and steal data. The most common attacks use one or more of the following:
  - Password cracking
  - Exploiting known security weaknesses
  - Network spoofing
  - Social engineering
  - Phishing

- Our best protection against these kinds of attacks is to be sure that you choose a strong password. Also, make sure your computer is set up to install Microsoft's automatic updates.

- We will talk more about how to create strong passwords later in this section.

Social Engineering and Phishing

Lesson 4.6: Social Engineering and Phishing

- Another security risk is the growing use of Social Engineering and Phishing by unauthorized persons in order to obtain sensitive information through deception.
- Social Engineering and Phishing often occur when someone sends an email or calls you on the phone, falsely claiming to be a legitimate business or a real staff member in an attempt to trick you into divulging sensitive information that could be used for fraud, identity theft, or unauthorized system access.
- A Social Engineer may by a former coworker or a 'friend of a friend' that tries to sway you into giving access to systems or data by claiming that they need to retrieve some old files they left behind, or they are picking up something for a mutual friend.
- Phishing often takes the form of an email or phone call falsely claiming to be an established legitimate business in an attempt to trick the user into surrendering sensitive information that could be used for fraud or identity theft.
- Follow these guidelines:
  - Never give unauthorized persons or people you don't know access to DOL information, personnel information, or our networks & systems.
  - Always check with your agency ISO when you are approached by someone seeking information or access to the DOL systems.
  - You must report all unauthorized access attempts, inquiries, and suspicious emails to your agency ISO immediately.

Wireless Security

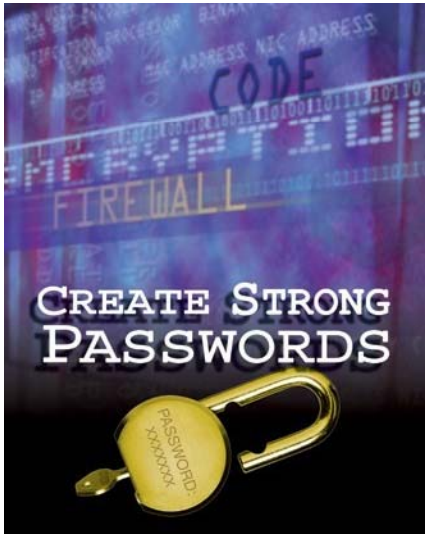
Lesson 4.7: Wireless Security

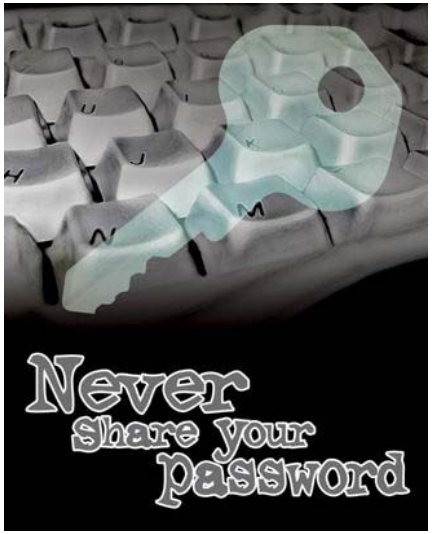
- Wireless technology is a rapidly growing means to connect computers to networks.
- With wireless connections, you only need to be in range of a wireless access point to log in and access the network.
- However, the very nature of transmitting data through the air greatly increases the risk of system intrusion and data theft.
- It is DOL policy that no unauthorized wireless devices may be used to access or store protected PII or other sensitive data. This includes personal laptops, game devices, PDAs, or any other kind of wireless device.
- All remote access, especially wireless access, into sensitive data must be protected using a secure encrypted channel.
- Public wireless networks are more vulnerable to hackers targeting unsecured computers and networks. Technologies such as Citrix and Virtual Private Network (VPN) use advanced encryption to protect the data being transmitted to and from your laptop or wireless device.
- Now, let's take a moment to talk about the importance of Password Security.

Password Protection

Lesson 4.8: Password Protection

- Your password plays an important part in computer security, and strong passwords often are the first line of defense against unauthorized access.
- When you set the password on your computer or on an application that you use, you should choose a password that's hard to guess, and that would be difficult for a computer program to break.
- Your DOL password must conform to the following:
  - Your password must be at least eight characters long, and it must mix uppercase and lowercase letters.
  - Your password must include at least one number, and it must include at least one special character – for example: !, @, #, :, > and %
- To help you remember the password, try creating a pass phrase using a series of words and incorporate all the features listed above.
- Don't use names of family or pets, or leave notes with passwords near your desk.
- Never give your password to anyone
- Here are some examples of passwords:
  - Good Password: B^3rK*)9
  - Bad Password: john123





Security Incident Response Program

Lesson 4.9: Security Incident Response Program

- Security incidents can pose a risk to DOL computer systems and to our data. We need your help in detecting and responding to these incidents.

- Computer security incidents can include things like viruses, unauthorized access to computer systems, missing PII documents or altered data, or any programs that send email or use the Internet when you're not expecting it.

- If any of these things happen to you, or you have any other indication that there might be a security problem with your computer, you should respond with three steps.
  - 1. First, stop using the computer. Don't turn it off, or finish your task, or attempt to fix the problem. Just leave the computer alone. Please, DON'T send email using the infected computer.
  - 2. Second, put a note on the computer indicating that it has a problem. This will keep other staff from using the computer as well.
  - 3. Immediately call your IT Help Desk to report the incident. Include all the details, including what you were doing when it happened.
  - For an incident involving lost equipment or any PII issue, call your agency ISO immediately.

Conclusion

Conclusion

- Congratulations, you have finished this training!

References

DLMS-9-900, Appropriate Use of IT

DLMS-9-1200, DOL Safeguarding Sensitive Data Including Personally Identifiable Information

Acknowledgement

This is an acknowledgement that I have received and reviewed the Computer Security Training for new DOL users.

Printed Name:_____

Signature:_____

Date Signed:_____

Agency:_____