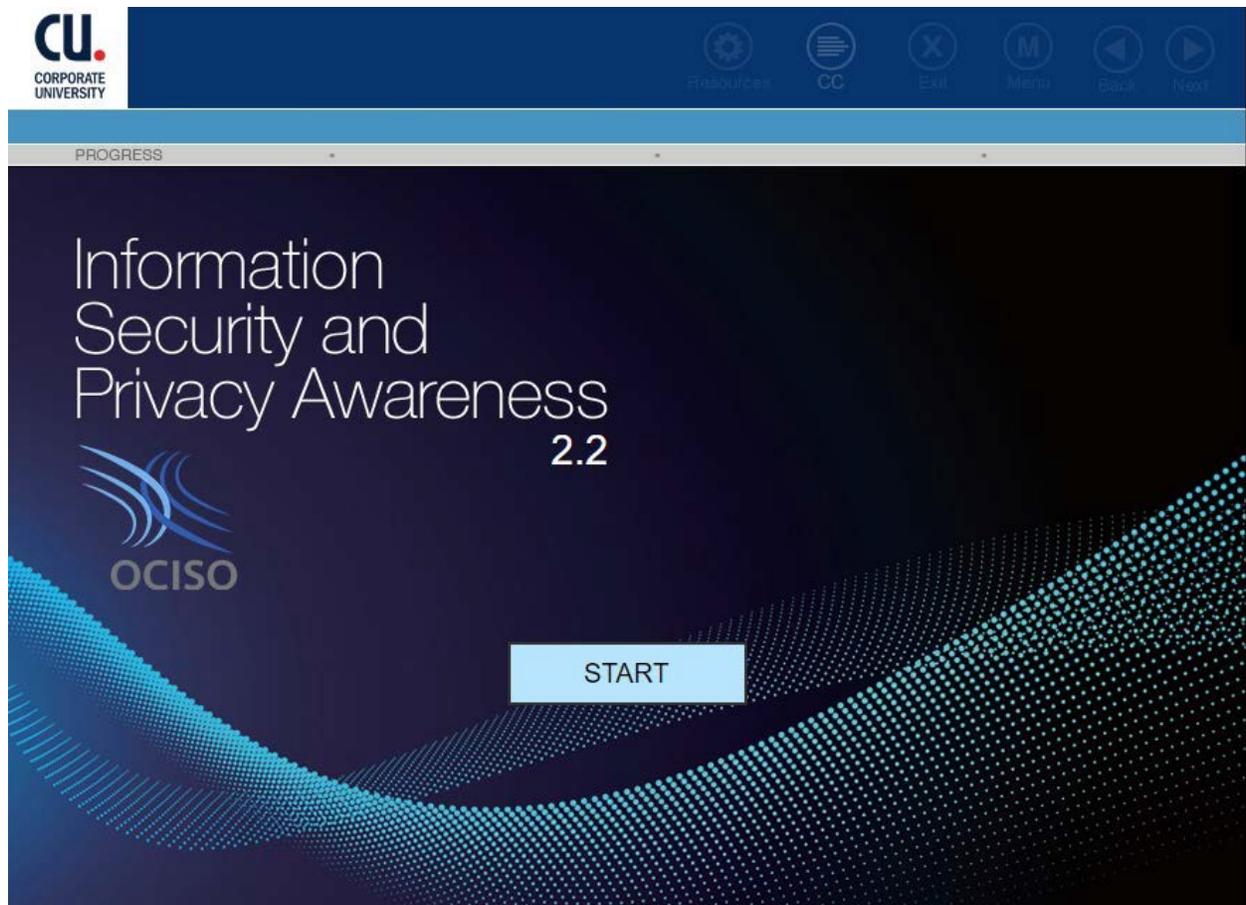


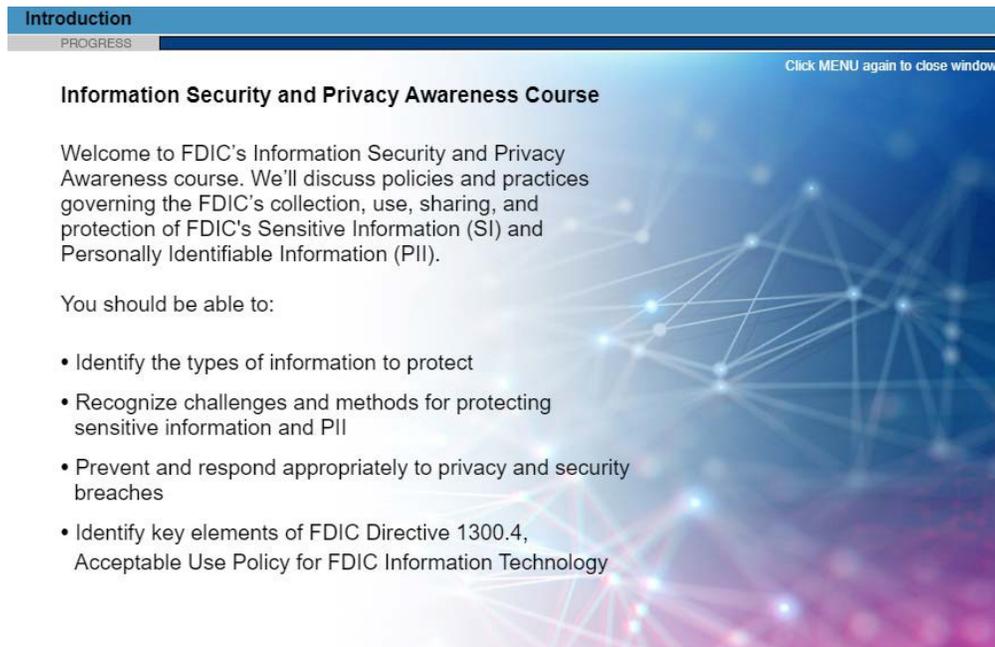


**CORPORATE
UNIVERSITY**

FDIC IT Security and Privacy Awareness



Information Security and Privacy Awareness 2.2

The image is a screenshot of a presentation slide. At the top left, there is a blue header bar with the word "Introduction" in white. Below it, a grey bar contains the word "PROGRESS" in white. In the top right corner, there is a small text prompt: "Click MENU again to close window". The main title of the slide is "Information Security and Privacy Awareness Course" in bold black text. Below the title, there is a paragraph of introductory text: "Welcome to FDIC's Information Security and Privacy Awareness course. We'll discuss policies and practices governing the FDIC's collection, use, sharing, and protection of FDIC's Sensitive Information (SI) and Personally Identifiable Information (PII)." This is followed by the phrase "You should be able to:" and a bulleted list of four items. The background of the slide features a network diagram with blue and purple nodes and connecting lines.

Information Security and Privacy Awareness Course

Welcome to FDIC's Information Security and Privacy Awareness course. We'll discuss policies and practices governing the FDIC's collection, use, sharing, and protection of FDIC's Sensitive Information (SI) and Personally Identifiable Information (PII).

You should be able to:

- Identify the types of information to protect
- Recognize challenges and methods for protecting sensitive information and PII
- Prevent and respond appropriately to privacy and security breaches
- Identify key elements of FDIC Directive 1300.4, Acceptable Use Policy for FDIC Information Technology

Information Security and Privacy Awareness Course

Welcome to FDIC's Information Security and Privacy Awareness course. During this training, we'll discuss policies and practices governing the FDIC's collection, use, sharing, and protection of FDIC's Sensitive Information (SI) and Personally Identifiable Information (PII). In addition, we will discuss FDIC's Acceptable Use Policy. You will learn how to maintain the confidentiality and integrity of the FDIC's network, systems, software, and data.

You should be able to:

- Identify the types of information to protect
- Recognize challenges and methods for protecting sensitive information and PII
- Prevent and respond appropriately to privacy and security breaches
- Identify key elements of FDIC Directive [1300.4, Acceptable use Policy for FDIC Information Technology](#)

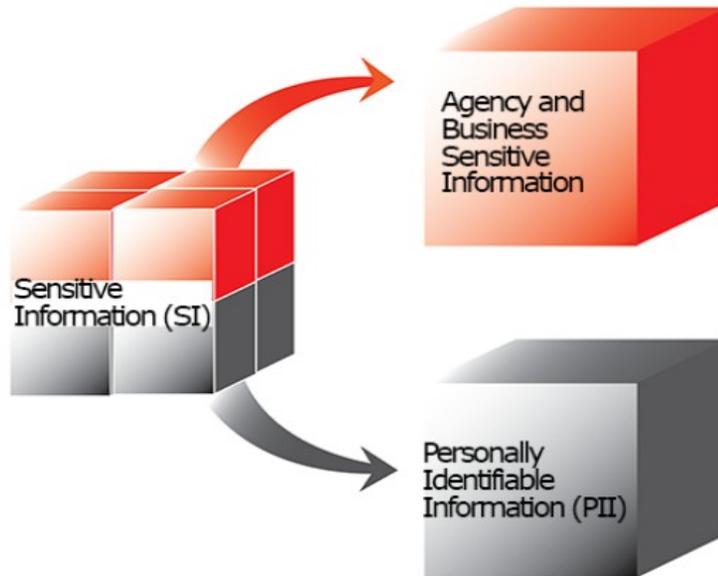
LESSON 1:

TYPES OF INFORMATION WE ARE PROTECTING

Lesson 1: Types of information we are protecting

PROGRESS

In accordance with FDIC Circular 1360.9 Protecting Sensitive Information, FDIC employees and contractors are required to protect all sensitive information collected or generated while working for the FDIC.



In accordance with FDIC Circular [1360.9 Protecting Sensitive Information](#), FDIC employees and contractors are required to protect all sensitive information collected or generated while working for the FDIC.

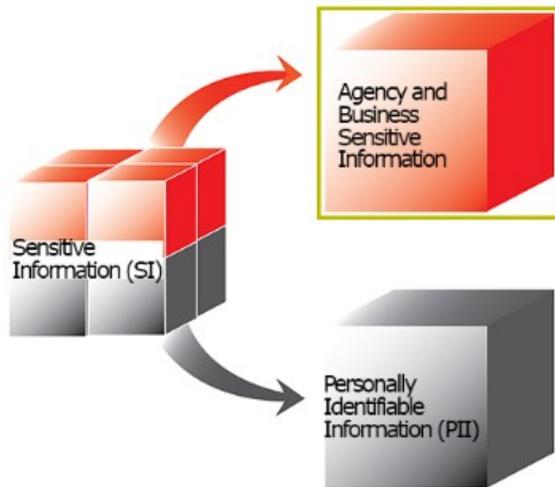
There are two main categories of Sensitive Information (SI):

- Agency and Business Sensitive information
- Personally Identifiable Information (PII)

Let's take a closer look at each type of information.

Lesson 1: Types of information we are protecting

PROGRESS

**Agency and Business Sensitive Information**

Examples of agency sensitive information include:

- Bank examination and bank closing information;
- Proprietary information provided to the Corporation by companies, organizations, or other agencies;
- Agency proprietary information that could disadvantage the agency in an ongoing negotiation;
- Attorney work product or attorney-client information;
- Certain law enforcement information or information about pending litigation;
- Security management information; and
- Information related to the FDIC's network or information technology that could be misused by malicious entities.

Agency and Business Sensitive Information

The first type is agency and business sensitive information, which if released inappropriately could harm or embarrass the FDIC, the financial institutions we supervise, or members of the public.

Examples of agency sensitive information include:

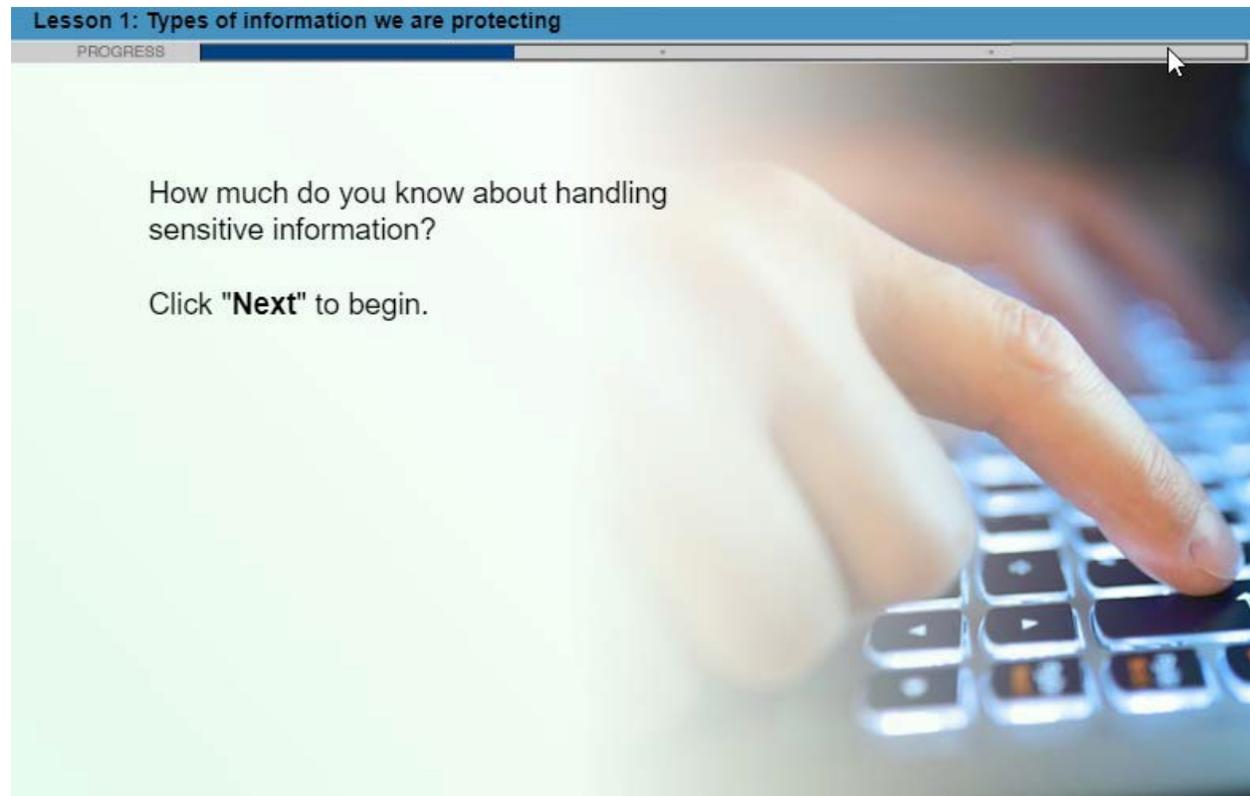
- Bank examination and bank closing information;
- Proprietary information provided to the Corporation by companies, organizations, or other agencies;
- Agency proprietary information that could disadvantage the agency in an ongoing negotiation;
- Attorney work product or attorney-client information;
- Certain law enforcement information or information about pending litigation;
- Security management information; and
- Information related to the FDIC's network or information technology that could be misused by malicious entities. (e.g., IP addresses, server names, firewall rules, encryption and authentication mechanisms, and network architecture pertaining to the FDIC).

Lesson 1: Types of information we are protecting

PROGRESS

How much do you know about handling sensitive information?

Click "**Next**" to begin.

A close-up photograph of a person's hand typing on a laptop keyboard. The background is blurred, showing the laptop screen and other parts of the keyboard. The lighting is soft, highlighting the texture of the keys and the skin of the hand.

How much do you know about handling sensitive information? Let's look at two scenarios. Click "Next" to begin.

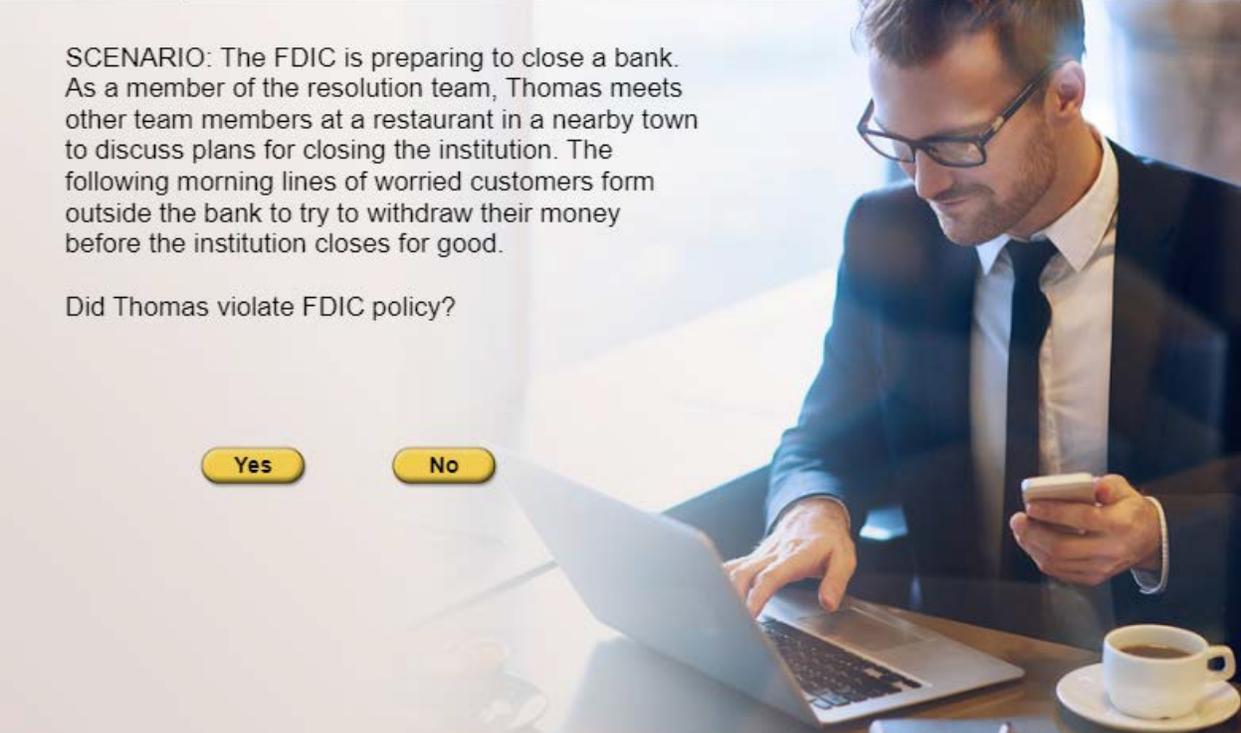
Lesson 1: Types of information we are protecting

PROGRESS

SCENARIO: The FDIC is preparing to close a bank. As a member of the resolution team, Thomas meets other team members at a restaurant in a nearby town to discuss plans for closing the institution. The following morning lines of worried customers form outside the bank to try to withdraw their money before the institution closes for good.

Did Thomas violate FDIC policy?

Yes No

A man in a dark suit, white shirt, and dark tie is sitting at a table in a restaurant. He is wearing glasses and has a beard. He is looking down at a smartphone in his left hand while his right hand is on a laptop keyboard. On the table in front of him is a white coffee cup on a saucer. The background is slightly blurred, showing a window and some interior decor.

Scenario: The FDIC is preparing to close a bank. As a member of the resolution team, Thomas meets other team members at a restaurant in a nearby town to discuss plans for closing the institution. The following morning lines of worried customers form outside the bank to try to withdraw their money before the institution closes for good.

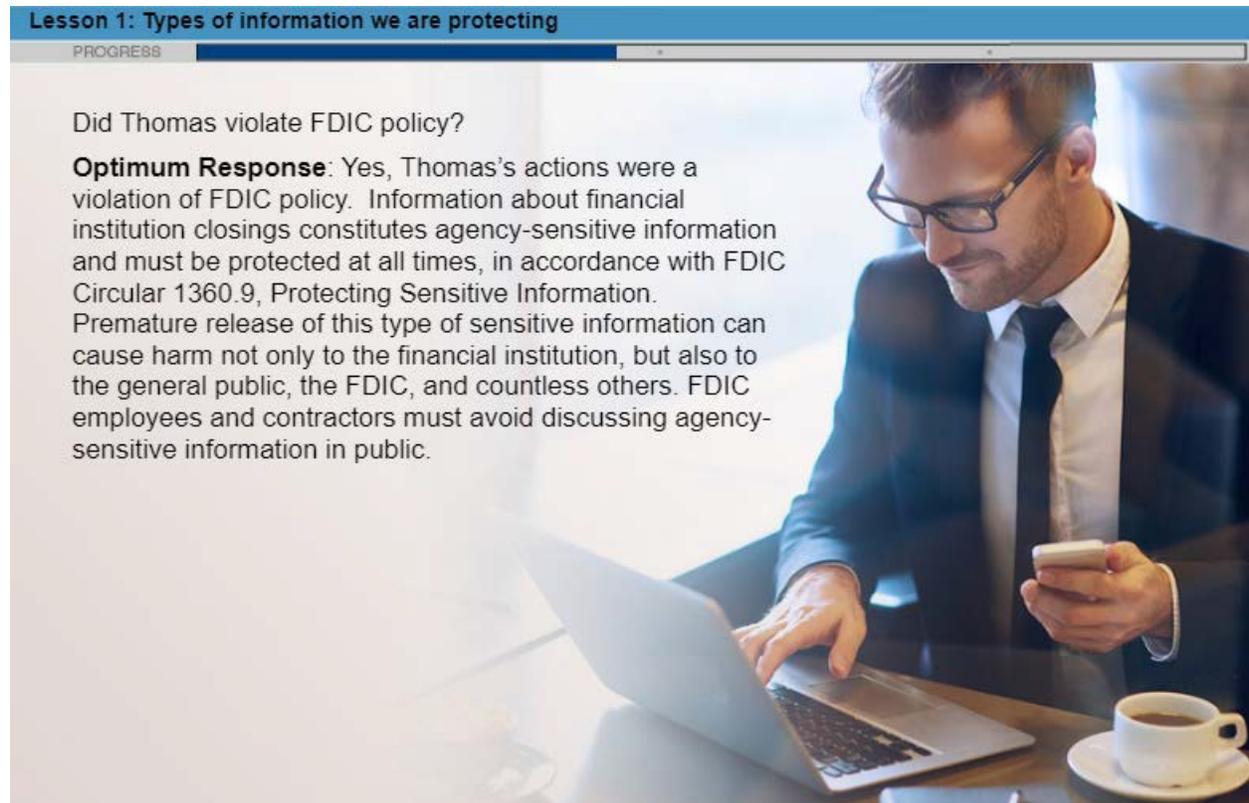
Did Thomas violate FDIC policy? Yes or No

Lesson 1: Types of information we are protecting

PROGRESS

Did Thomas violate FDIC policy?

Optimum Response: Yes, Thomas's actions were a violation of FDIC policy. Information about financial institution closings constitutes agency-sensitive information and must be protected at all times, in accordance with FDIC Circular 1360.9, Protecting Sensitive Information. Premature release of this type of sensitive information can cause harm not only to the financial institution, but also to the general public, the FDIC, and countless others. FDIC employees and contractors must avoid discussing agency-sensitive information in public.

A man in a dark suit, white shirt, and dark tie is sitting at a desk. He is wearing glasses and looking down at a smartphone in his left hand. His right hand is on the keyboard of a silver laptop. On the desk in front of him is a white coffee cup on a saucer. The background is a bright, out-of-focus office environment.

Did Thomas violate FDIC policy?

Optimum Response: Yes, Thomas's actions were a violation of FDIC policy. Information about financial institution closings constitutes agency-sensitive information and must be protected at all times, in accordance with FDIC Circular 1360.9, Protecting Sensitive Information. Premature release of this type of sensitive information can cause harm not only to the financial institution, but also to the general public, the FDIC, and countless others. FDIC employees and contractors must avoid discussing agency-sensitive information in public.

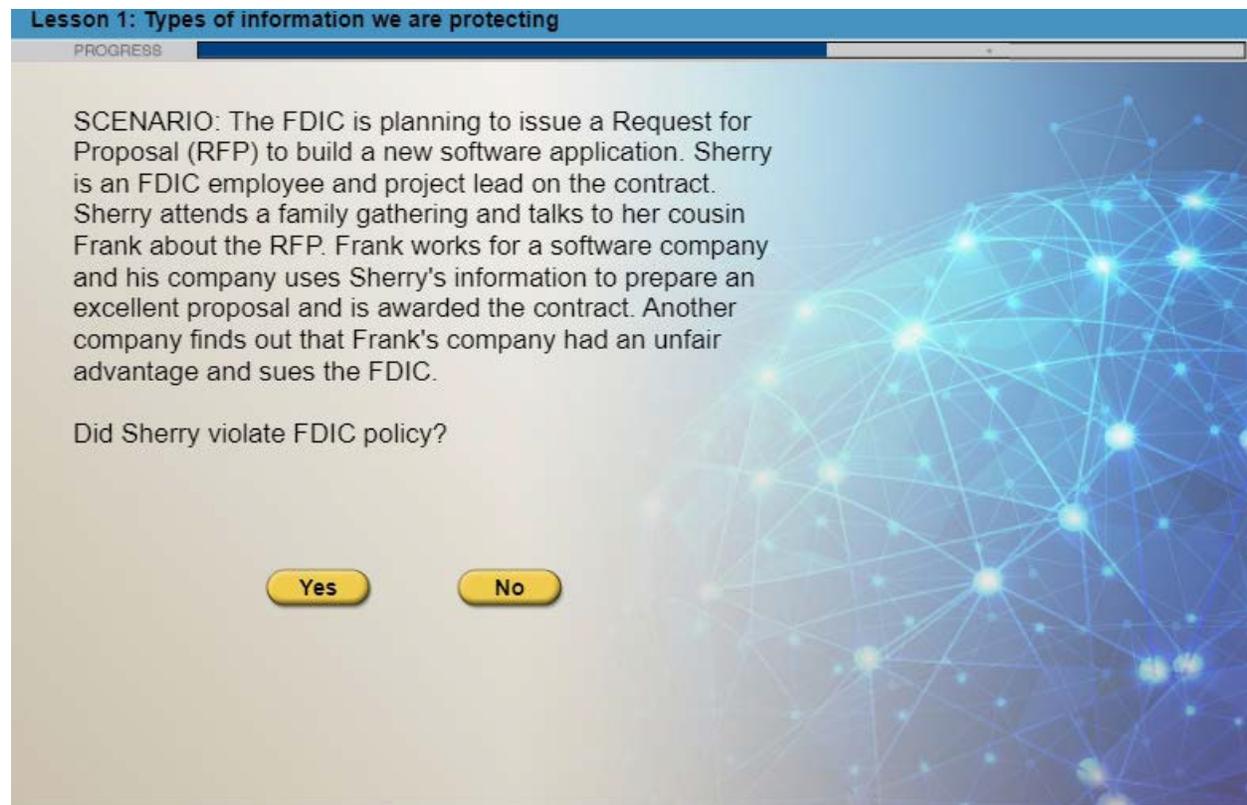
Lesson 1: Types of information we are protecting

PROGRESS

SCENARIO: The FDIC is planning to issue a Request for Proposal (RFP) to build a new software application. Sherry is an FDIC employee and project lead on the contract. Sherry attends a family gathering and talks to her cousin Frank about the RFP. Frank works for a software company and his company uses Sherry's information to prepare an excellent proposal and is awarded the contract. Another company finds out that Frank's company had an unfair advantage and sues the FDIC.

Did Sherry violate FDIC policy?

Yes No



Scenario: The FDIC is planning to issue a Request for Proposal (RFP) to build a new software application. Sherry is an FDIC employee and project lead on the contract. Sherry attends a family gathering and talks to her cousin Frank about the RFP. Frank works for a software company and his company uses Sherry's information to prepare an excellent proposal and is awarded the contract. Another company finds out that Frank's company had an unfair advantage and sues the FDIC.

Did Sherry violate FDIC policy? Yes or No

Lesson 1: Types of information we are protecting

PROGRESS

Did Sherry violate FDIC policy?

Optimum Response: Yes, Sherry's actions were a violation of FDIC Circular 1360.9, Protecting Sensitive Information. Information about the FDIC's plans for contracts or projects is considered agency-sensitive information and should not be discussed outside the organization before the RFP is released. This information ensures fairness in the awarding of contracts and protects the FDIC's reputation. It may also help protect the FDIC from litigation.

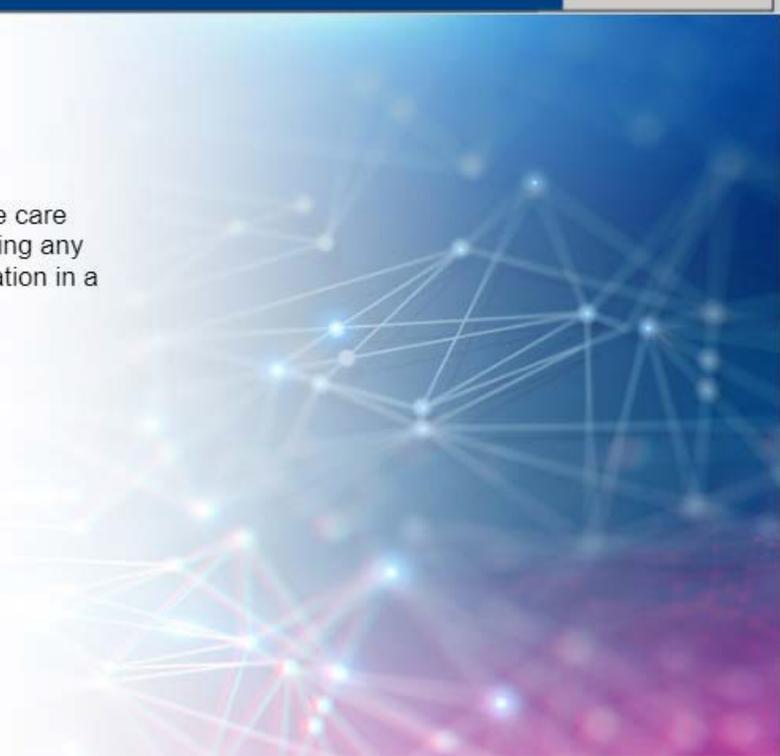


Did Sherry violate FDIC policy?

Optimum Response: Yes, Sherry's actions were a violation of FDIC Circular [1360.9, Protecting Sensitive Information](#). Information about the FDIC's plans for contracts or projects is considering agency-sensitive information and should not be discussed outside the organization before the RFP is released. This information ensures fairness in the awarding of contracts and protects the FDIC's reputation. It may also help protect the FDIC from litigation.

Lesson 1: Types of information we are protecting

PROGRESS

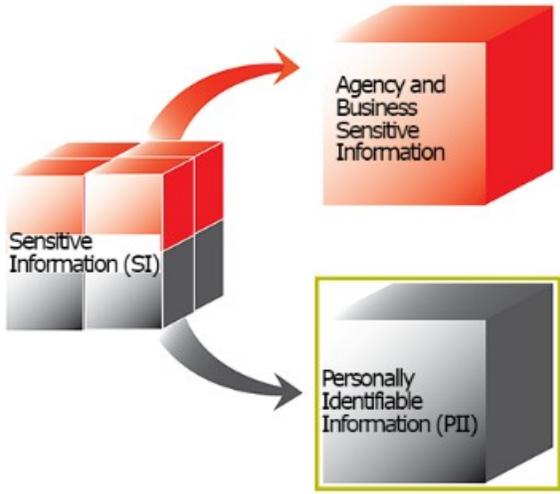


It is important to exercise care when discussing or sharing any agency sensitive information in a public setting.

As you learned, it is important to exercise care when discussing or sharing any agency sensitive information in a public setting.

Lesson 1: Types of information we are protecting

PROGRESS



Personally Identifiable Information (PII)

Examples of PII include:

- Full Names
- Home Addresses
- Telephone Numbers
- Email Addresses
- Financial Information

PII may be a single item or a combination of data elements, such as a full name combined with a credit card number or financial institution account number. PII may also be pieces of information, that when combined with other information, can be linked to a specific individual.

Personally Identifiable Information (PII)

The second type of information that requires additional care is Personally Identifiable Information (PII).

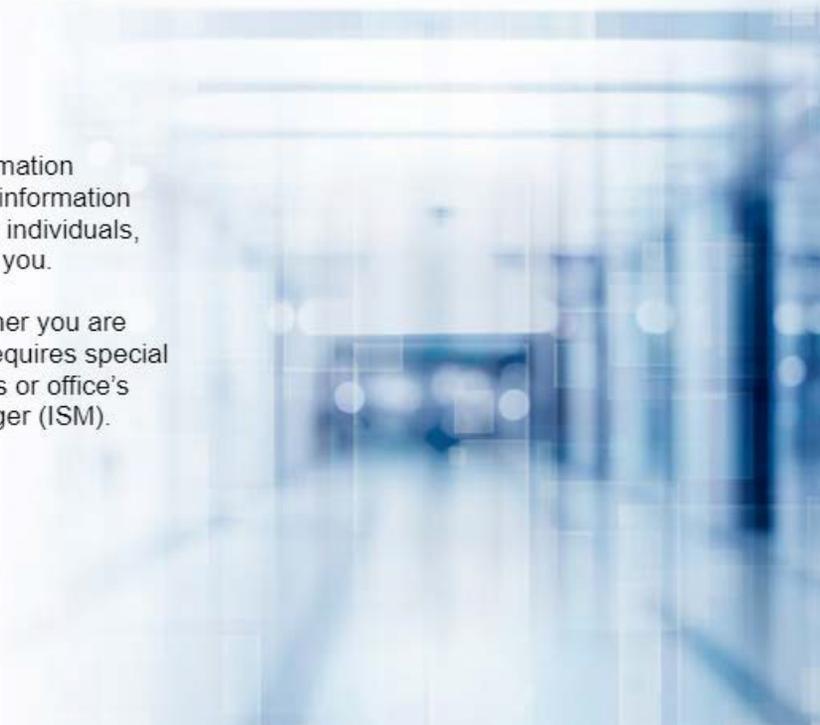
Examples of PII include:

- Full Names
- Home Addresses
- Telephone Numbers
- Email Addresses
- Financial Information
- Other personal data of FDIC employees, contractors, and visitors, as well as bank customer information

PII may be a single item or a combination of data elements, such as a full name combined with a credit card number or financial institution account number. PII may also be pieces of information, that when combined with other information, can be linked to a specific individual.

Lesson 1: Types of information we are protecting

PROGRESS



Mishandling sensitive information including agency sensitive information and PII, can cause harm to individuals, businesses, the FDIC, and you.

When in doubt about whether you are handling information that requires special care, contact your division's or office's Information Security Manager (ISM).

Keep in mind that mishandling sensitive information including agency sensitive information and PII, can cause harm to individuals, businesses, the FDIC, and you.

When in doubt about whether you are handling information that requires special care, contact your division's or office's Information Security Manager (ISM).

Lesson 2:

Why We Protect Agency Sensitive Information and PII

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

It is important to take special care with Agency Sensitive Information and PII in order to:

- 1) Comply with Federal laws, regulations, OMB circulars, and FDIC directives
- 2) Protect (a) the FDIC and the nation's financial system; (b) the public including bank customers; and (c) employees and contractors
- 3) Prevent an FDIC data breach
- 4) Avoid personal consequences for mishandling data

In Lesson 2, we will review why we protect sensitive information.

It is important to take special care with agency sensitive information and PII in order to:

- 1) Comply with Federal laws, regulations, Office of Management and Budget (OMB) circulars, and FDIC directives;
- 2) Protect (a) the FDIC and the nation's financial system; (b) the public including bank customers; (c) employees and contractors;
- 3) Prevent an FDIC data breach; and 4) Avoid personal consequences for mishandling data

Let's review each of these in more detail.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

1. Laws, Regulations and Policy Click on each button to learn more.

<input type="radio"/> The Privacy Act of 1974	The Privacy Act requires the FDIC to protect certain records containing PII (both electronic and in paper) and provide individuals with special privacy rights.
<input type="radio"/> E-Government Act of 2002	The E-Government Act requires FDIC to address information technology (IT) training, IT security, and the protection of personal privacy.
<input type="radio"/> Freedom of Information Act (FOIA)	The FOIA requires the FDIC to provide certain agency records to the public. However, there are several exceptions for agency sensitive information, personal and confidential PII, and business information.
<input checked="" type="radio"/> OMB Circulars/ Memoranda	The OMB provides the FDIC with policy and guidance to manage and protect information resources.

1. Laws, Regulations and Policy

There are a number of laws, regulations, and directives that guide FDIC's efforts to protect the security and privacy of information. The most relevant of these are:

The Privacy Act of 1974 requires the FDIC to protect certain records containing PII (both electronic and in paper) and provide individuals with special privacy rights.

E-Government Act of 2002 requires FDIC to address information technology (IT) training, IT security, and the protection of personal privacy.

The Freedom of Information Act (FOIA) requires the FDIC to provide certain agency records to the public. However, there are several exceptions for agency sensitive information, personal and confidential PII, and business information.

The OMB Circulars/Memoranda provides the FDIC with policy and guidance to manage and protect information resources.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

OCISO | FDIC.net | FDIC.gov

Office of the Chief Information Security Officer

Search OCISO Advanced Search

Home Awareness and Training Cybersecurity Program Privacy Program ISM Program About OCISO

OCISO > Home

Awareness and Training

Privacy/Cybersecurity Awareness
Building a Culture of Cybersecurity and Privacy within the FDIC

Privacy and Cybersecurity awareness training is an education process that teaches employees about Cybersecurity, Privacy, IT best practices, and even regulatory compliance. Below and via the Quick links employees can take training (online, computer-based, attend seminars, and obtain support materials) on a variety of IT, security, privacy and other business-related topics. OCISO's approach is to provide you with the right tools to create, grow and mature your understanding of Privacy and Cybersecurity awareness.

TRAINING

- ▶ Mandatory
- ▶ Corporate-wide
- ▶ Targeted
- ▶ Role-based
- ▶ External

AWARENESS QUICK LINKS

- ▶ Phishing Awareness Guidance

QUICK LINKS

- ▶ Awareness & Training
- ▶ FDIC Breach Response Plan
- ▶ CISO Home Page

SKILLPORT

FDICLEARN

REPORT AN INCIDENT

Click to view Security Related Directives

The FDIC has developed and implemented a number of security and privacy-related circulars and directives that are intended to help employees to protect: agency sensitive information, PII, and FDIC computer systems and networks. Visit the Office of the Chief Information Security Officer's (OCISO) website to review a wide variety of resources on information security and privacy, including directives and circulars. You should familiarize yourself with the information in FDIC Circular [1360.9, Protecting Sensitive Information](#).

[Security Related Directives](#)

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

2. Protect the FDIC, Public, and Personnel

The public trusts the FDIC to:

- insure deposits
- examine and supervise financial institutions
- manage receiverships

**2. Protect the FDIC, Public, and Personnel**

The public trusts the FDIC to insure deposits, examine and supervise financial institutions, and manage receiverships. In conducting our business, we protect sensitive bank customer data as well as FDIC employee and contractor information.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Protect the FDIC, Public, and Personnel

Click on each button to learn more.

- 

Protecting the Public

As an employee or contractor of the FDIC, you share the responsibility of protecting sensitive data and PII. While some data is collected from the financial institutions we supervise or close, some information is collected directly from the public. If any of this information falls into the wrong hands, it can be used to harm the financial institutions we supervise and regulate.
- 

Protecting FDIC employees

The FDIC collects and uses a wide range of PII from its employees during the hiring process and as part of administering payroll and benefits. Employees have the right to gain access to that information, and correct inaccurate information.
- 

Protecting Contractors

FDIC collects PII from its contractors during the background investigation process. Contractors have the right to gain access to that information, and correct inaccurate information.

Protect the FDIC, Public, and Personnel

Protecting the FDIC and the nation's financial system is an ongoing effort. As an employee or contractor of the FDIC, you share the responsibility of safeguarding agency sensitive information and PII from those seeking to harm us or the institutions we supervise and regulate.

Protecting the Public: As an employee or contractor of the FDIC, you share the responsibility of protecting sensitive data and PII. While some data is collected from the financial institutions we supervise or close, some information is collected directly from the public. If any of this information falls into the wrong hands, it can be used to harm the financial institutions we supervise and regulate.

Protecting FDIC Employees: The FDIC collects and uses a wide range of PII from its employees during the hiring process and as part of administering payroll and benefits. Employees have the right to gain access to that information, and correct inaccurate information.

Protecting Contractors: FDIC collects PII from its contractors during the background investigation process. Contractors have the right to gain access to that information, and correct inaccurate information.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

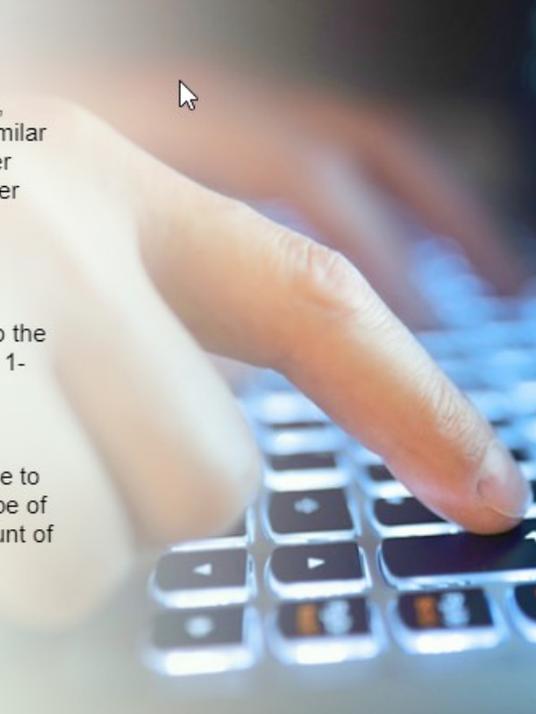
3. Breach

An occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for an other than authorized purpose.

How to Report a Breach

If you suspect or confirm a breach of personally identifiable information (PII), you must immediately report the incident to the DIT Help Desk/Security Operations Center (SOC) by calling 1-877-FDIC-999 or 1-877-334-2999, Option #5, and your Supervisor or Oversight Manager (OM).

You should provide all relevant information in the initial notice to the FDIC Help Desk/SOC, including but not limited to the type of data affected (e.g., name, SSN, address, etc.) and the amount of records or data affected.



3. Breach

An occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for an other than authorized purpose.

How to Report a Breach

If you suspect or confirm a breach of personally identifiable information (PII), you must immediately report the incident to the DIT Help Desk/Security Operations Center (SOC) by calling 1-877-FDIC-999 or 1-877-334-2999, Option #5, and your Supervisor or Oversight Manager (OM).

You should provide all relevant information in the initial notice to the FDIC Help Desk/SOC, including but not limited to the type of data affected (e.g., name, SSN, address, etc.) and the amount of records or data affected.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

3. Consequences of Privacy and Security Violations

Mishandling sensitive information while working on behalf of the FDIC may result in very real consequences for you. Depending on the circumstances and impact of the violation, you may be disciplined in accordance with the FDIC's normal disciplinary procedures, ranging from a verbal warning up to and including termination or separation of employment. Click the links to learn more about the guidelines that define Privacy and Security Violations.

[Privacy Violations](#)[Security Violations](#)**3. Consequences of Privacy and Security Violations**

Mishandling sensitive information while working on behalf of the FDIC may result in very real consequences for you. Depending on the circumstances and impact of the violation, you may be disciplined in accordance with the FDIC's normal disciplinary procedures, ranging from a verbal warning up to and including termination or separation of employment. Click the links to learn more about the guidelines that define Privacy and Security Violations.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Privacy Violations

There are criminal penalties addressed in the Privacy Act of 1974. They are based on knowingly and willfully:

- Obtaining records under false pretenses.
- Disclosing privacy data to any person not entitled to access.
- Maintaining a system of records without meeting public notice requirements.
- Penalties include a misdemeanor criminal charge and a fine of up to \$5000.

Under the Privacy Act, courts may also award civil penalties for:

- Unlawfully refusing to amend a record.
- Unlawfully refusing to grant access to a record.
- Failure to maintain accurate, relevant, timely, and complete information.
- Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect on the subject of the record.
- Penalties include: actual damages, payment of reasonable attorney's fees, and removal from employment.

Privacy Violations

There are criminal penalties addressed in the Privacy Act of 1974. They are based on knowingly and willfully:

- Obtaining records under false pretenses.
- Disclosing privacy data to any person not entitled to access.
- Maintaining a system of records without meeting public notice requirements.
- Penalties include a misdemeanor criminal charge and a fine of up to \$5000.

Under the Privacy Act, courts may also award civil penalties for:

- Unlawfully refusing to amend a record.
- Unlawfully refusing to grant access to a record.
- Failure to maintain accurate, relevant, timely, and complete information.
- Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect on the subject of the record.
- Penalties for these violations include: actual damages, payment of reasonable attorney's fees, and removal from employment.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Security Violations

Violations of security rules and regulations may result in a variety of serious consequences including permanent loss of data, identity theft, and unauthorized disclosure of data. Violations include:

- Using the logon credentials of another user.
- Transmitting sensitive data to a personal email address.
- Transmitting or providing sensitive data to an individual who is not authorized to receive it.
- Leaving sensitive data documents unsecured in your office or other unsecured areas.
- Storing sensitive data in an unprotected manner.
- Improperly disposing of sensitive data or documents.
- Improper use of government equipment or resources.
- Failing to report a security incident when you have firsthand knowledge of the event.

Security Violations

Violations of security rules and regulations may result in a variety of serious consequences including permanent loss of data, identity theft, and unauthorized disclosure of data. Violations include:

- Using the logon credentials of another user.
- Transmitting sensitive data to a personal email address.
- Transmitting or providing sensitive data to an individual who is not authorized to receive it.
- Leaving sensitive data documents unsecured in your office or other unsecured areas.
- Storing sensitive data in an unprotected manner.
- Improperly disposing of sensitive data or documents.
- Improper use of government equipment or resources.
- Failing to report a security incident when you have firsthand knowledge of the event.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Onboarding

When you started working at the FDIC, you agreed to adhere to confidentiality obligations.

Mishandling sensitive information including agency sensitive information and/or PII, is taken seriously.



Onboarding

When you started working at the FDIC, you agreed to adhere to confidential obligations. Mishandling sensitive information including agency sensitive information and/or PII, is taken seriously.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Leaving FDIC's Employment

The task of protecting information doesn't end with your employment:

- You will complete a pre-exit clearance process with your supervisor or oversight manager.
- As part of the pre-exit clearance process, you will be required to certify that you have returned all Corporation-owned equipment, documents, and confidential information to the FDIC and that you understand the obligation to maintain the confidentiality of any confidential information that you had access to while employed at the FDIC.
- You also will be notified of remedies available to the FDIC should you fail to comply with your obligations, and that any knowing and willful false statements that you make in providing the certifications or acknowledgements can be punished by fine or imprisonment, or both.

Leaving FDIC's Employment

The task of protecting information doesn't end with your employment:

- You will complete a pre-exit clearance process with your supervisor or oversight manager.
- As part of the pre-exit clearance process, you will be required to certify that you have returned all Corporation-owned equipment, documents, and confidential information to the FDIC and that you understand the obligation to maintain the confidentiality of any confidential information that you had access to while employed at the FDIC.
- You also will be notified of remedies available to the FDIC should you fail to comply with your obligations, and that any knowing and willful false statements that you make in providing the certifications or acknowledgements can be punished by fine or imprisonment, or both.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Protecting Agency Confidential Information and PII

You must take great care to protect information in order to:

- comply with laws and regulations
- follow FDIC circulars and directives
- prevent an FDIC data breach
- avoid personal consequences for mishandling data

Failure to protect this information or otherwise violating FDIC policies related to the protection of FDIC information can have serious negative consequences for individuals, the FDIC, and you.

The FDIC may seek any and all legal remedies available to it under the law, including breach of contract and injunctive relief from such court or courts as may have jurisdiction, and such relief shall be in addition to, and not in lieu of, other remedies, including possible criminal remedies.

Further, FDIC may seek to recover reasonable costs and attorney's fees in connection with obtaining any such relief for a breach.

Protecting Agency Confidential Information and PII

Protecting agency confidential Information and PII is an important responsibility. You must take great care to protect this information in order to:

- comply with laws and regulations;
- follow FDIC circulars and directives;
- prevent an FDIC data breach; and
- avoid personal consequences for mishandling data.

Failure to protect this information or otherwise violating FDIC policies related to the protection of FDIC information can have serious negative consequences for individuals, the FDIC, and you.

The FDIC may seek any, and all legal remedies available to it under the law, including breach of contract and injunctive relief from such court or courts as may have jurisdiction, and such relief shall be in addition to, and not in lieu of, other remedies, including possible criminal remedies.

Further, FDIC may seek to recover reasonable costs and attorney's fees in connection with obtaining any such relief for a breach.

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Protecting Agency Confidential Information and PII Cont.

If you remove FDIC nonpublic information without authorization, FDIC may seek to conduct reasonable searches of your personally-owned computers, electronic devices, and digital accounts containing FDIC nonpublic information.

You should not expect full and complete privacy in the contents of your personally-owned computers, electronic devices, and digital accounts if you violate or have violated FDIC policies and save or transmit, or have saved or transmitted, FDIC nonpublic information on/within them.

Violations of FDIC policy could be reported by the FDIC to future employers, to background investigators and/or to any professional licensing/credentialing bodies.

If you violate Corporate policies related to the protection of FDIC data, the FDIC has instituted a "Table of Penalties" that must be utilized to determine appropriate disciplinary action.

Click the button to review the Table of Penalties.

[Table of Penalties](#)

Protecting Agency Confidential Information and PII Cont.

In addition, if you remove FDIC nonpublic information without authorization, FDIC may seek to conduct reasonable searches of your personally-owned computers, electronic devices, and digital accounts containing FDIC nonpublic information.

You should not expect full and complete privacy in the contents of your personally-owned computers, electronic devices, and digital accounts if you violate or have violated FDIC policies and save or transmit, or have saved or transmitted, FDIC nonpublic information on/within them.

Violations of FDIC policy could be reported by the FDIC to future employers, to background investigators and/or to any professional licensing/credentialing bodies.

If you violate Corporate policies related to the protection of FDIC data, the FDIC has instituted a "[Table of Penalties](#)" that must be utilized to determine appropriate disciplinary action.

Lesson 3:

Challenges to Protecting

Agency Sensitive Information

and PII

Lesson 3: Challenges protecting Agency Sensitive Information and PII

PROGRESS

Challenges to Protecting Sensitive Information and PII

As an FDIC employee or contractor, you may have access to sensitive information.

It is important to protect sensitive information using all available means including:

- Electronic Protection
- Physical Protection
- Personal Conduct

Challenges to Protecting Sensitive Information and PII

Now let's look at the challenges we face protecting sensitive information, including agency sensitive information and PII. As an FDIC employee or contractor, you may have access to sensitive information. It is important to protect sensitive information using all available means including:

- **Electronic Protection** – Use of strong passwords, encryption, antivirus software, and appropriate use of FDIC IT systems and data;
- **Physical Protection** – Use proper storage and handling of paper copy materials, both in the office or off-site, and properly securing our workspace; and
- **Personal Conduct** – Use discretion when choosing to share information with others and making good choices when using FDIC IT resources.

Lesson 3: Challenges protecting Agency Sensitive Information and PII

PROGRESS

Challenges to Protecting Sensitive Information and PII

Let's review creating strong passwords and using FDIC IT systems appropriately.

You are about to enter a simulated scenario that will explore how to protect sensitive information throughout the information life cycle.

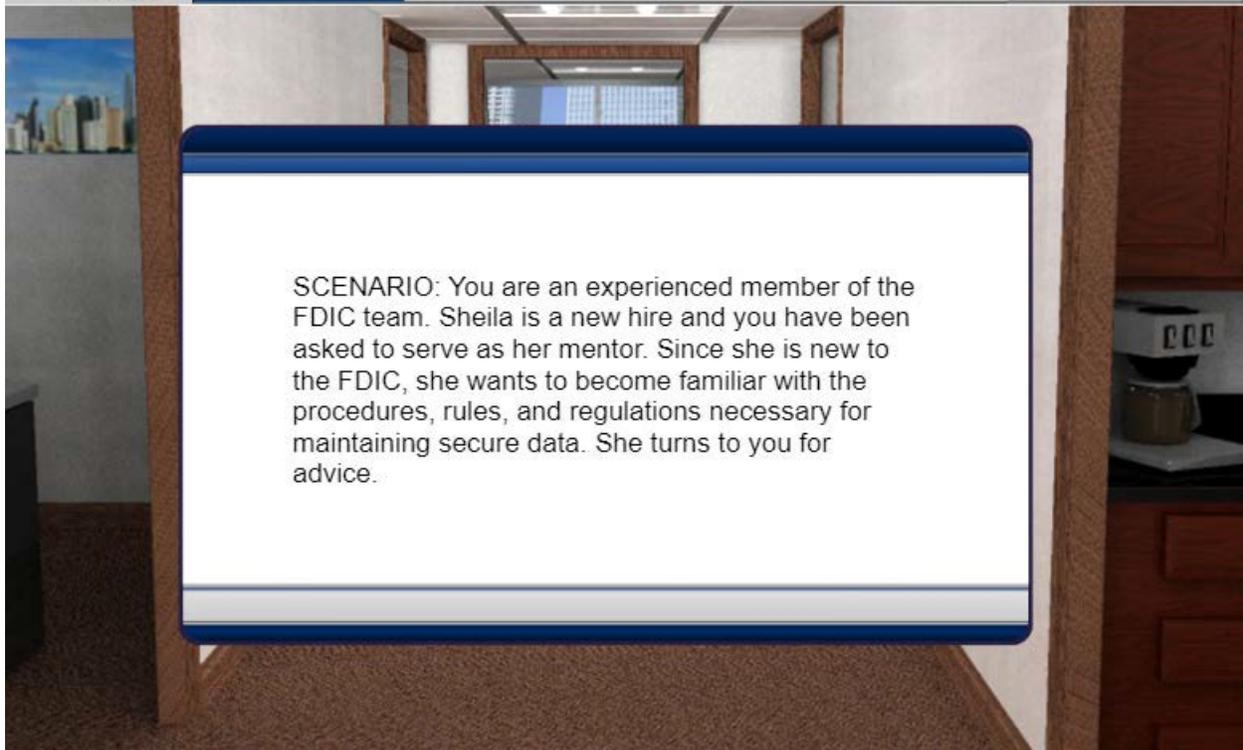
Select Next to begin.

Challenges to Protecting Sensitive Information and PII

Let's review creating strong passwords and using FDIC IT systems appropriately. You are about to enter a simulated scenario that will explore how to protect sensitive information throughout the information life cycle. Select Next to begin.

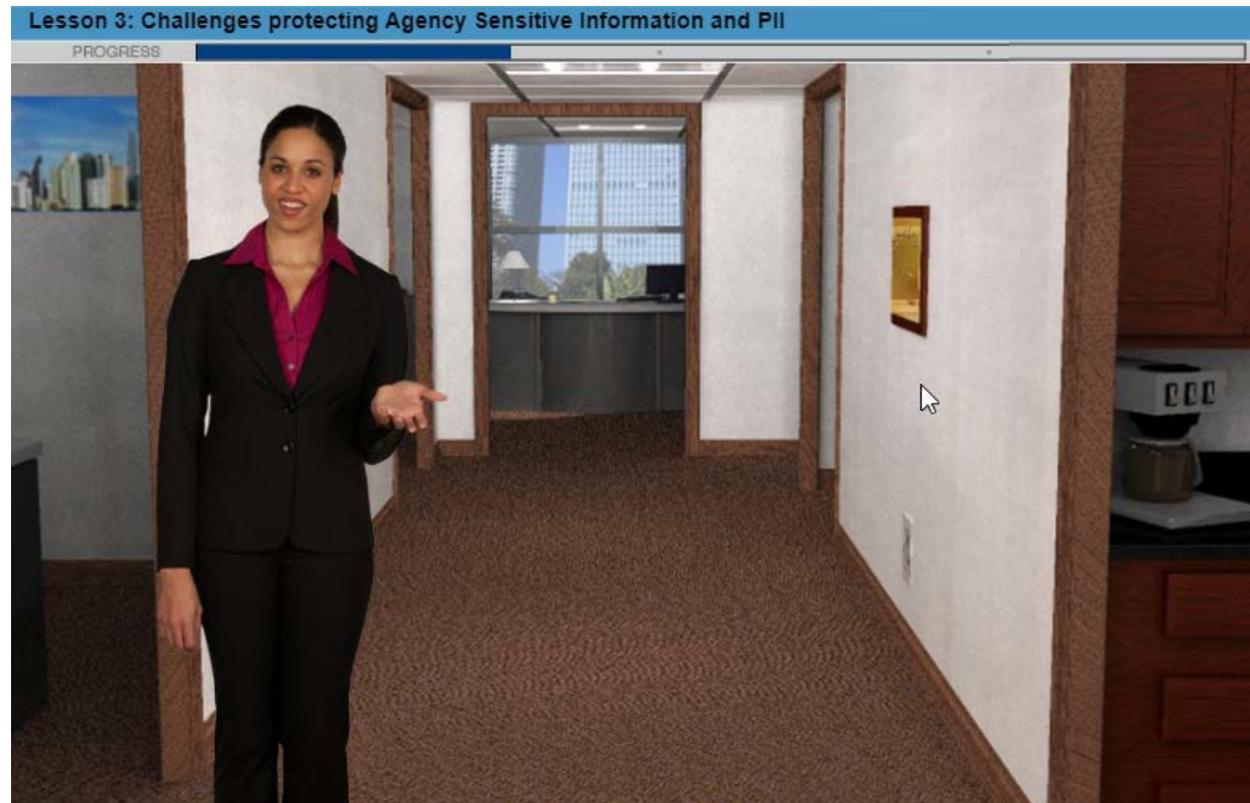
Lesson 3: Challenges protecting Agency Sensitive Information and PII

PROGRESS



SCENARIO: You are an experienced member of the FDIC team. Sheila is a new hire and you have been asked to serve as her mentor. Since she is new to the FDIC, she wants to become familiar with the procedures, rules, and regulations necessary for maintaining secure data. She turns to you for advice.

Scenario: You are an experienced member of the FDIC team. Sheila is a new hire and you have been asked to serve as her mentor. Since she is new to the FDIC, she wants to become familiar with the procedures, rules, and regulations necessary for maintaining secure data. She turns to you for advice.



Since our office is rolling out a new computer application, I need to select a new password. What do you recommend?

Lesson 3: Challenges protecting Agency Sensitive Information and PII

PROGRESS

Recommendations for a Strong Password**Strong Password SHOULD:**

- Have minimum length 8 characters (recommend 10-12 characters, 16 is the max)
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Contain at least one numerical and special character (e.g. 0-9, !@#\$%)
- Use a Passphrase adding a special character and number

Strong Password should NOT:

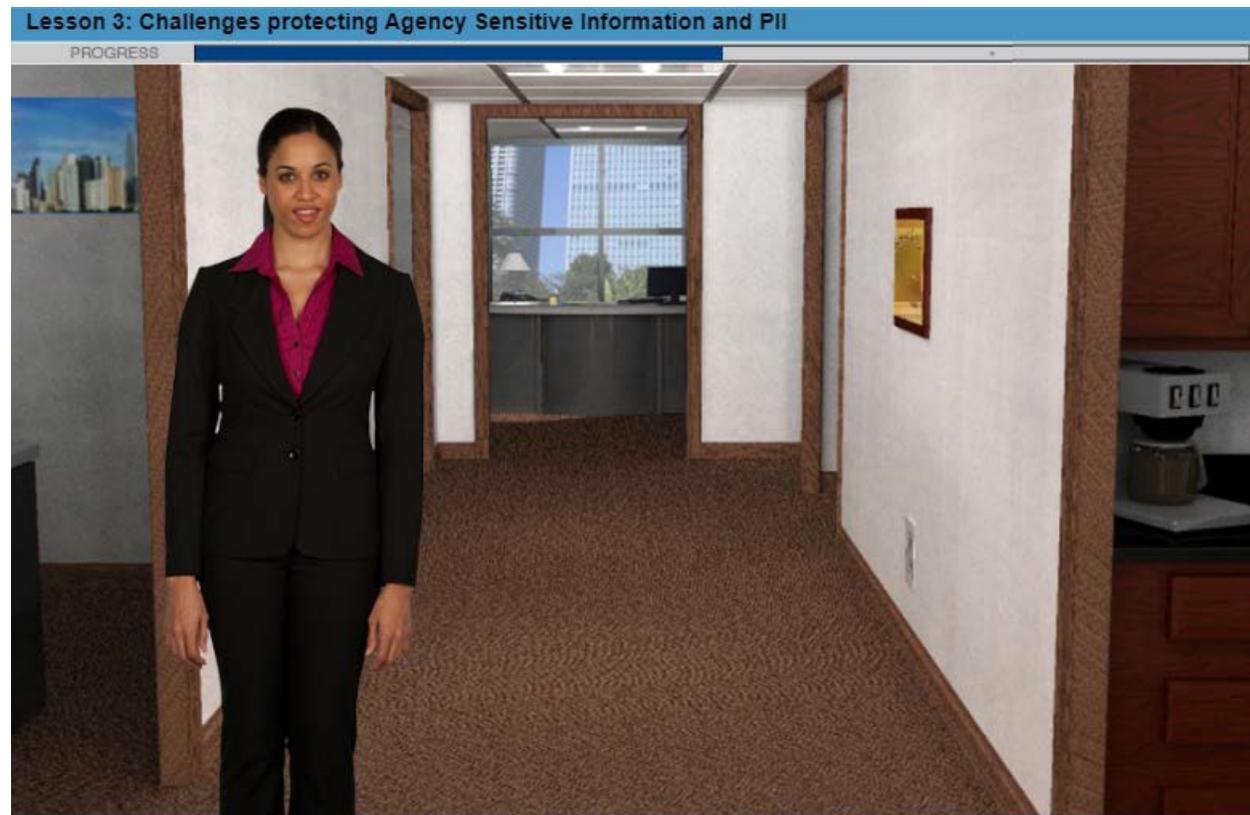
- Include any completed English words in a character string
- Have personal information such as User ID, family name, pet, birthday, etc.
- Spell a word with a number added to the beginning and the end

Recommendations for a Strong Password**Strong Password Should:**

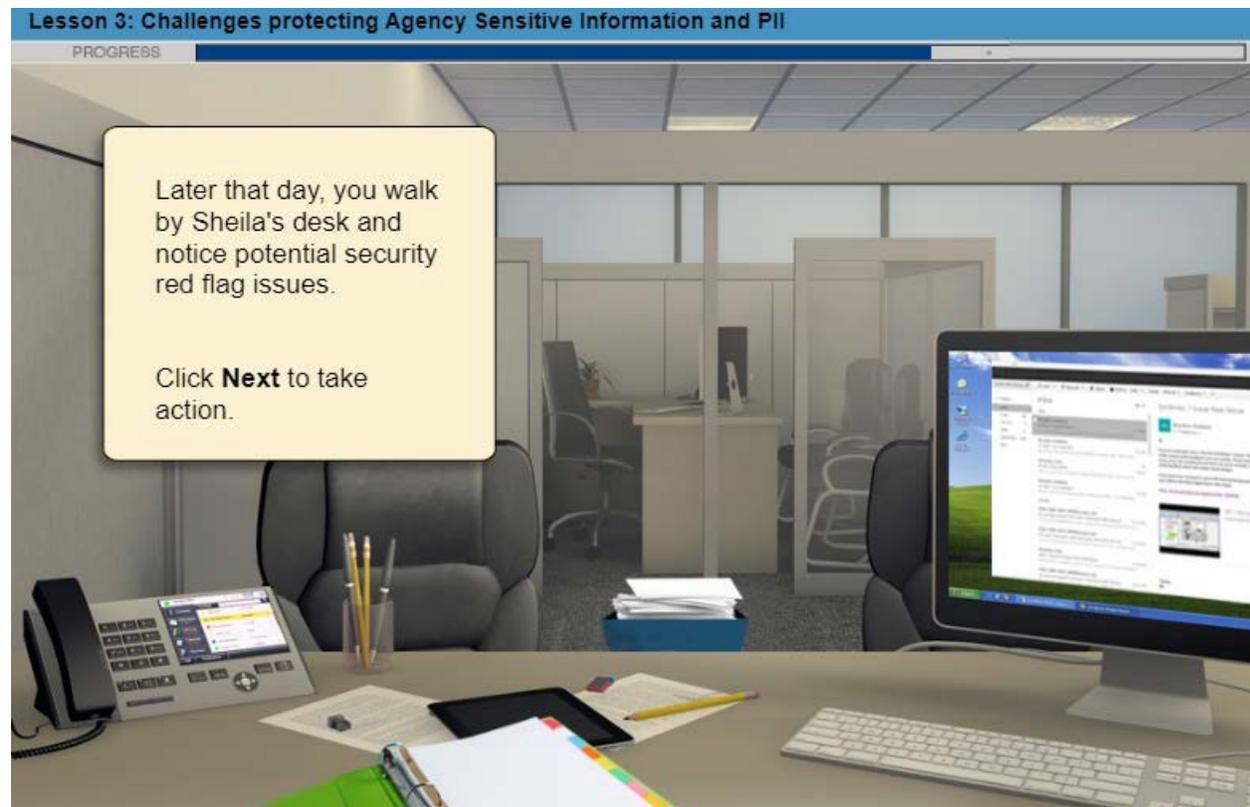
- Have minimum length 8 characters (recommend 10-12 characters, 16 is the max)
- Contain both upper and lowercase alphabetic characters (e.g., A-Z, a-z)
- Contain at least one numerical and special character (e.g., 0-9, !@#\$%)
- Use a Passphrase adding a special character and number

Strong Password should NOT:

- Include any completed English words in a character string
- Have personal information such as User ID, family name, pet, birthday, etc.
- Spell a word with a number added to the beginning and the end



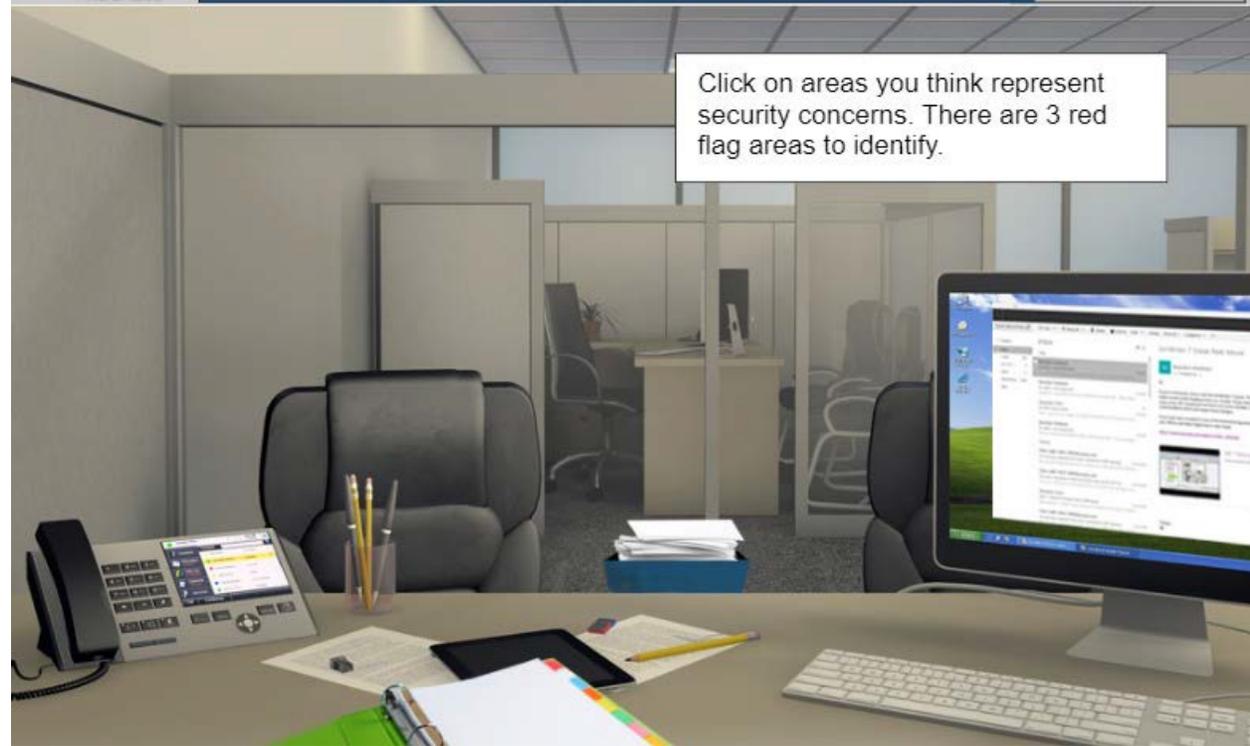
Ok. I'll use a longer password with letters, numbers and special characters. That's good to know. I'll work on creating a good, secure password right now. Thanks for your feedback.



Later that day, you walk by Sheila's desk and notice potential security red flag issues. Click Next to take action.

Lesson 3: Challenges protecting Agency Sensitive Information and PII

PROGRESS

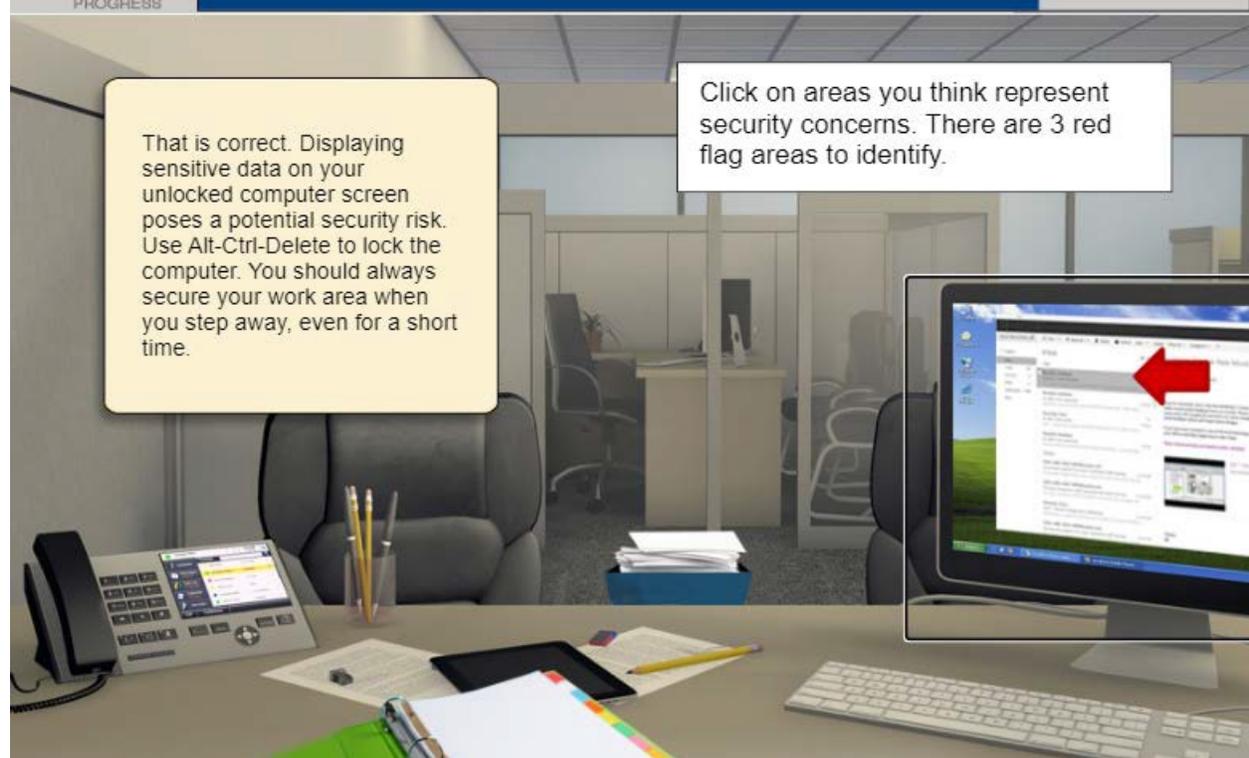


Click on areas you think represent security concerns. There are 3 red flag areas to identify.

Click on areas you think represent security concerns. There are 3 red flag areas to identify.

Lesson 3: Challenges protecting Agency Sensitive Information and PII

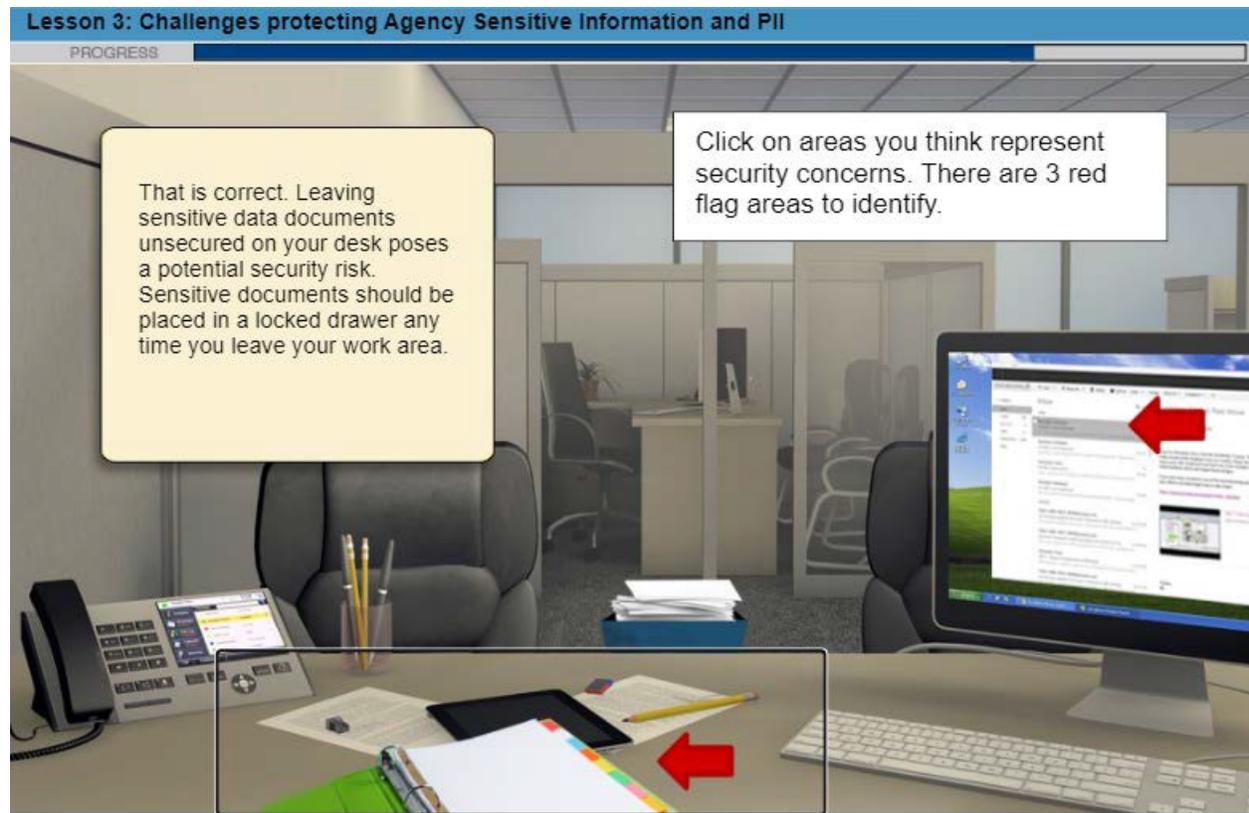
PROGRESS



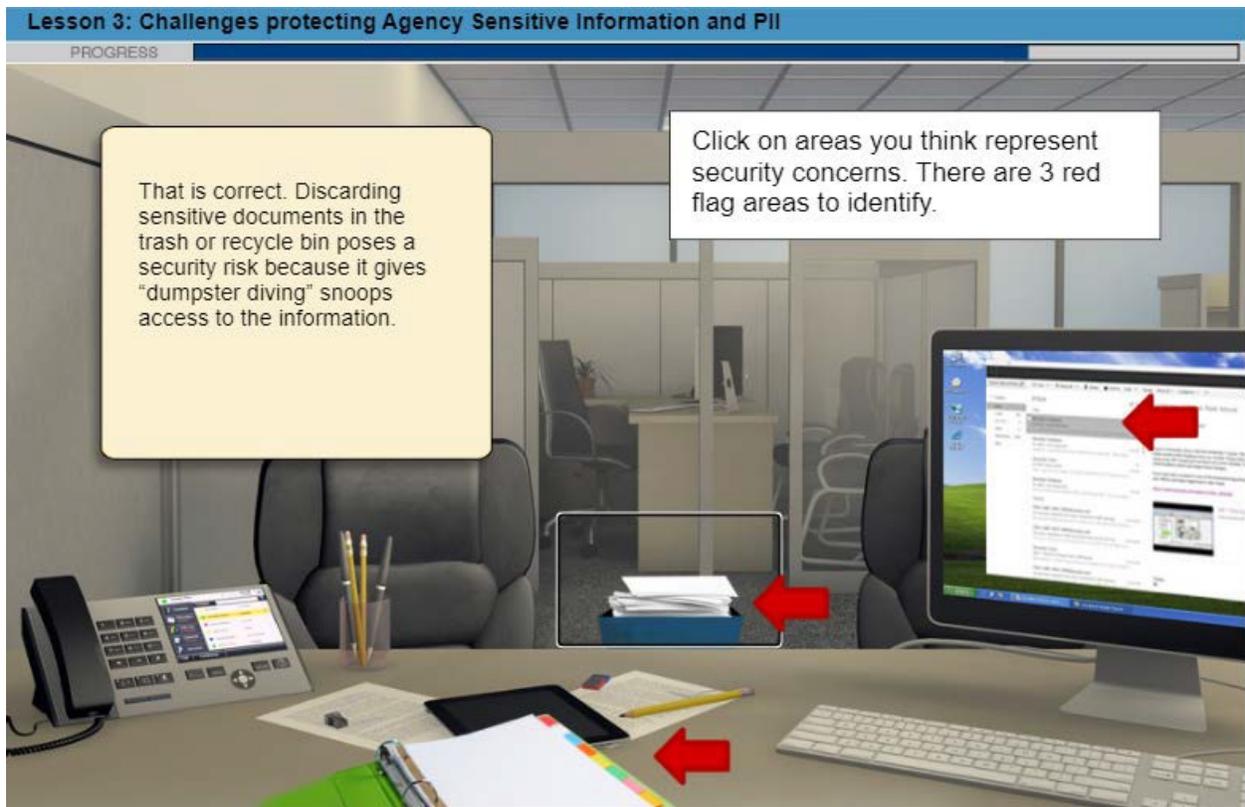
That is correct. Displaying sensitive data on your unlocked computer screen poses a potential security risk. Use Alt-Ctrl-Delete to lock the computer. You should always secure your work area when you step away, even for a short time.

Click on areas you think represent security concerns. There are 3 red flag areas to identify.

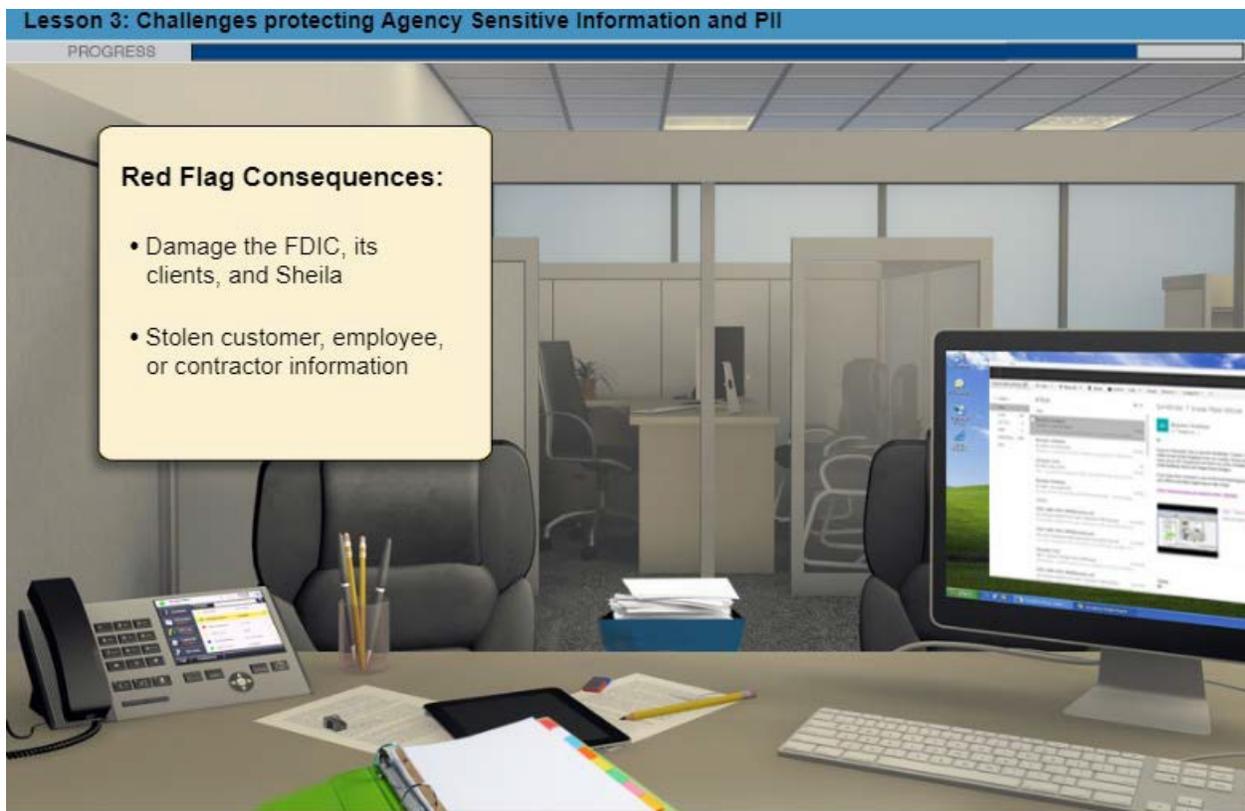
(Computer screen is selected.) That is correct. Displaying sensitive data on your unlocked computer screen poses a potential security risk. Use Alt-Ctrl-Delete to lock the computer. You should always secure your work area when you step away, even for a short time.



(Documents on the desk are selected.) That is correct. Leaving sensitive data documents unsecured on your desk poses a potential security risk. Sensitive documents should be placed in a locked drawer any time you leave your work area.



(Recycle bin documents are selected.) This is correct. Discarding sensitive documents in the trash or recycle bin poses a security risk because it gives "dumpster diving" snoops access to the information.



You discuss the red flag concerns with Sheila and explain their potential consequences, including how the release of sensitive information could seriously damage the FDIC, its clients, and even Sheila herself. She could have had bank customer, employee, or contractor information stolen, and be reprimanded or even terminated from her position. Sheila thanks you for the feedback and promises to be more organized and careful.

Red Flag Consequences:

- Damage the FDIC, its clients, and Sheila
- Stolen customer, employee, or contractor information

Lesson 3: Challenges protecting Agency Sensitive Information and PII

PROGRESS



Electronic protection, physical protection, and personal conduct are all necessary to ensure protection of information throughout its life cycle.

As you just experienced, electronic protection, physical protection, and personal conduct are all necessary to ensure the protection of information throughout its life cycle, from its initial collection to its ultimate disposal or destruction.

Lesson 4:

Protecting Information

Throughout the Lifecycle

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

This lesson reviews phases throughout the information life cycle.

If you have questions about any of the information life cycle phases, talk with your supervisor or your division ISM. You may also contact FDIC's Privacy Program at privacy@fdic.gov.

Image Description: Collection/Creation leads to Use, Maintenance, Sharing/Disclosure, Storage; which leads to Disposal



This lesson reviews phases throughout the information life cycle.

Protecting data can be challenging. It is important to know how to protect information throughout the entire life cycle – from the time data is initially collected to its ultimate disposal or destruction. Consider the information you work with every day. If you have questions about any of the information life cycle phases, talk with your supervisor or your division ISM. You may also contact FDIC's Privacy Program at privacy@fdic.gov.

Image Description: Collection/Creation leads to Use, Maintenance, Sharing/Disclosure, Storage; which lead to Disposal.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Collection and Creation

We collect and create data for specific business purposes from:

- employees
- contractors
- financial institutions
- members of the general public

Special requirements:

- The type of information being collected;
- The intended purpose and use of information to be collected;
- The number of members of the public being asked for this information;
- The nature of the information collection (whether the collection is paper-based or web-based; and
- Whether the collection of information requires a new or modified Privacy Act of System Records Notice.

Disposal

Collection and Creation

As part of our jobs, we collect and create data for specific business purposes from employees, contractors, financial institutions, or members of the general public. In general, we should only collect or create the minimum amount of information needed to carry out the mission of the FDIC.

Special requirements may govern the collection of information depending on:

- The type of information being collected;
- The intended purpose and use of information to be collected;
- The number of members of the public being asked for this information;
- The nature of the information collection (whether the collection is paper-based or web-based); and
- Whether the collection of information requires a new or modified Privacy Act of System Records Notice.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Use

If you are uncertain about the uses of the information you work with every day, talk with your supervisor, or your division Information Security Manager (ISM).

You can also contact FDIC's Privacy Program by emailing privacy@fdic.gov.

Click "**Next**" to review ISM listing

Use

The use of information refers to the appropriate handling and sharing of sensitive information and PII in accordance with authorized legal or business requirements. You are responsible for knowing who is authorized to access sensitive information before you disclose it. If you are uncertain about the uses of the information you work with every day, talk with your supervisor, your division Information Security Manager (ISM) or contact FDIC's Privacy Program by emailing privacy@fdic.gov.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Role of Information Security Manager (ISM)

FDIC's Information Security Management (ISM) Program is designed to increase the effectiveness of the corporation's cybersecurity risk management program.

Divisional Information Security Managers (ISMs) ensure an enterprise-wide approach to information security and privacy serving as advisors throughout the corporation to leverage security management tools and technical expertise.

[Click to review ISM list](#)**Role of Information Security Manager (ISM)**

FDIC's Information Security Management (ISM) Program is designed to increase the effectiveness of the corporation's cybersecurity risk management program.

Divisional Information Security Managers (ISMs) ensure an enterprise-wide approach to information security and privacy serving as advisors throughout the corporation to leverage security management tools and technical expertise.

[Click to review ISM list.](#)

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Click "Next" when you are ready to advance.

Sharing and Disclosure

There are special rules governing the sharing of sensitive information or PII to other parties.

Click on each item to learn more about the Privacy Act of 1974 and the Freedom of Information Act (FOIA).

The Privacy Act of 1974

The Freedom of Information Act (FOIA)

The image is a screenshot of a training module slide. At the top, there is a blue header bar with the text "Lesson 4: Protecting information throughout the lifecycle". Below the header, there is a progress bar with the word "PROGRESS" on the left. The main content area has a light beige background with a blurred image of a stack of papers. The text on the slide includes a title "Sharing and Disclosure", a paragraph about special rules for sensitive information, an instruction to click on items to learn more, and two blue buttons labeled "The Privacy Act of 1974" and "The Freedom of Information Act (FOIA)".

Sharing and Disclosure

There are special rules governing the sharing of sensitive information or PII to other parties. Click on each item to learn more about the Privacy Act of 1974 and the Freedom of Information Act (FOIA).

Lesson 4: Protecting information throughout the lifecycle

PROGRESS



The Privacy Act of 1974

The Privacy Act specifies that we cannot disclose by any means of communication any information from a Privacy Act system of records unless the subject of the record provides you with a written request, or prior written consent.

The Privacy Act also provides individuals with some control and rights over the information the government collects on them. These include the right to request whether a system contains records about themselves and to request access and amendments to their records.

Questions concerning whether certain records are covered by the Privacy Act should be emailed to privacy@fdic.gov or directed to the FDIC Legal Office (FOIA/Privacy Act Group).

The Privacy Act of 1974

The Privacy Act of 1974 specifies that we cannot disclose by any means of communication (e.g., conversationally or by email) any information from a Privacy Act system of records unless the subject of the record provides you with a written request, or prior written consent.

The Privacy Act also provides individuals with some control and rights over the information the government collects on them. These include the right to request whether a system contains records about themselves and to request access and amendments to their records.

Questions concerning whether certain records are covered by the Privacy Act should be emailed to privacy@fdic.gov or directed to the FDIC Legal Office (FOIA/Privacy Act Group).

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

The Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA) requires agencies to provide agency records to requesters, except for material that is exempt from disclosure.

Any FOIA request must immediately be brought to the attention of the FDIC's Legal Division. You must also refer the inquirer to the FDIC's FOIA website.

[FDIC's FOIA Requests](#)

The Freedom of Information Act (FOIA)

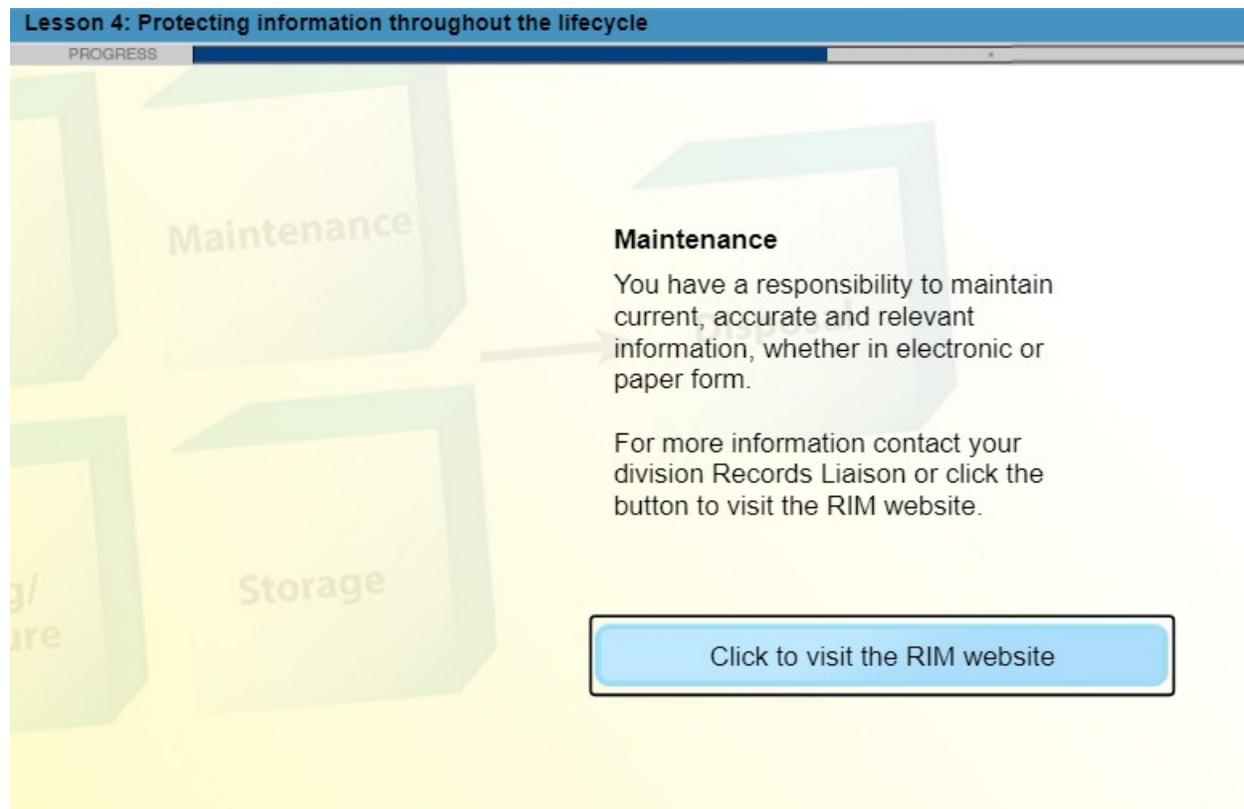
The Freedom of Information Act (FOIA) requires agencies to provide agency records to requesters, except for material that is exempt from disclosure.

Any FOIA request, which may be in writing, must immediately be brought to the attention of the FDIC's Legal Division. You must also refer the inquirer to the FDIC's FOIA website.

[FDIC's FOIA Requests](#)

Lesson 4: Protecting information throughout the lifecycle

PROGRESS



Maintenance

You have a responsibility to maintain current, accurate and relevant information, whether in electronic or paper form.

For more information contact your division Records Liaison or click the button to visit the RIM website.

Click to visit the RIM website

Maintenance

As an FDIC employee or contractor, you have a responsibility to maintain current, accurate and relevant information, whether in electronic or paper form. The overall goal is to comply with the law, while still achieving business objectives. Avoid saving redundant or outdated data that is not required by law. For more information contact your division Records Liaison or visit the [RIM website](#).

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Maintenance

Paper copies

Electronic copies

Storage

You must properly secure information to help prevent accidental loss or dissemination. Failing to secure records properly may result in a Computer Security Incident Response Team (CSIRT) incident, and cause harm to an individual or the FDIC.

Click the links for more information about storing paper and electronic copies.

Storage

You must properly secure information to help prevent accidental loss or dissemination. Failing to secure records properly may result in a Computer Security Incident Response Team (CSIRT) incident, and cause harm to an individual or the FDIC.

Click on the links for more information about storing paper and electronic copies.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Storing Paper Copies

- Avoid making paper copies of agency sensitive information or PII whenever possible.
- Store paper copies of agency sensitive information or PII in a locked drawer or file cabinet, and make sure they are secure any time you leave your desk. Never leave agency sensitive data or PII at home or in your vehicle.
- Printed agency sensitive information at home should never be left out unattended; documents should be in a locked drawer or file cabinet.
- Agency sensitive information that is being transported in a vehicle should always be out of sight, and vehicle locked if unattended.
- Use caution with printers and copiers. Leaving an original on the copier or sending a print job to the wrong printer can lead to improper disclosure of data.

Storing Paper Copies

- Avoid making paper copies of agency sensitive information or PII whenever possible. You'll have less paper to keep track of and potentially misplace.
- Store paper copies of agency sensitive information or PII in a locked drawer or file cabinet, and make sure they are secure any time you leave your desk. Never leave agency sensitive data or PII at home or in your vehicle.
- Printed agency sensitive information at home should never be left out unattended; documents should be in a locked drawer or file cabinet.
- Agency sensitive information that is being transported in a vehicle should always be out of sight, and vehicle locked if unattended.
- Use caution with printers and copiers. Leaving an original on the copier or sending a print job to the wrong printer can lead to improper disclosure of data.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Storing Electronic Copies

- Personal email accounts (Gmail or Hotmail) should never be used for transmitting or receiving any sensitive FDIC business-related information.
- Only make electronic copies of information from the network that is relevant to your task.
- Do not download any data from any FDIC-furnished equipment to removable media (USB storage device or CD/DVD). This is prohibited. Refer to the Acceptable Use Policy for a list of exceptions.
- Protect electronic copies of data from production databases as carefully as you would the originals.
- Only authorized equipment and services furnished by the FDIC (or by contractor personnel if stated in the terms of the contract) may be connected to FDIC IT resources in an FDIC facility or at a financial institution. FDIC employees and contractors are allowed to access limited corporate applications through personally owned devices (smart devices, tablet computing devices, or laptop computers) and may connect such devices remotely via the Internet to the designated FDIC Remote Access systems. Personally-owned devices that are not furnished by the FDIC may also connect to the FDIC Guest Wi-Fi Network.
- The FDIC automatically scans for malware. Individuals should also be vigilant and install malware protection software on their personal devices to prevent attacks.
- When dealing with agency sensitive information or PII, encrypt or password - protect your files.

Storing Electronic Copies

- Personal email accounts (e.g., Gmail or Hotmail) should never be used for transmitting or receiving any sensitive FDIC business-related information.
- Only make electronic copies of information from the network that is relevant to your task.
- Do not download any data from any FDIC-furnished equipment to removable media (USB storage device or CD/DVD). This is prohibited. Refer to the Acceptable Use Policy for a list of exceptions.
- Protect electronic copies of data from production databases as carefully as you would the originals.
- Only authorized equipment and services furnished by the FDIC (or by contractor personnel if stated in the terms of the contract) may be connected to FDIC IT resources in an FDIC facility or at a financial institution. FDIC employees and contractors are allowed to access limited corporate applications through personally owned devices (smart devices, tablet computing devices, or laptop computers) and may connect such devices remotely via the internet to the designated FDIC Remote Access systems. Personally owned devices that are not furnished by the FDIC may also connect to the FDIC Guest Wi-Fi Network.
- The FDIC automatically scans for malware. Individuals should also be vigilant and install malware protection software on their personal devices to prevent attacks.

- When dealing with agency sensitive information or PII, encrypt or password – protect your files.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Storage - Encryption

You should never store unencrypted sensitive information in an easily accessible place.

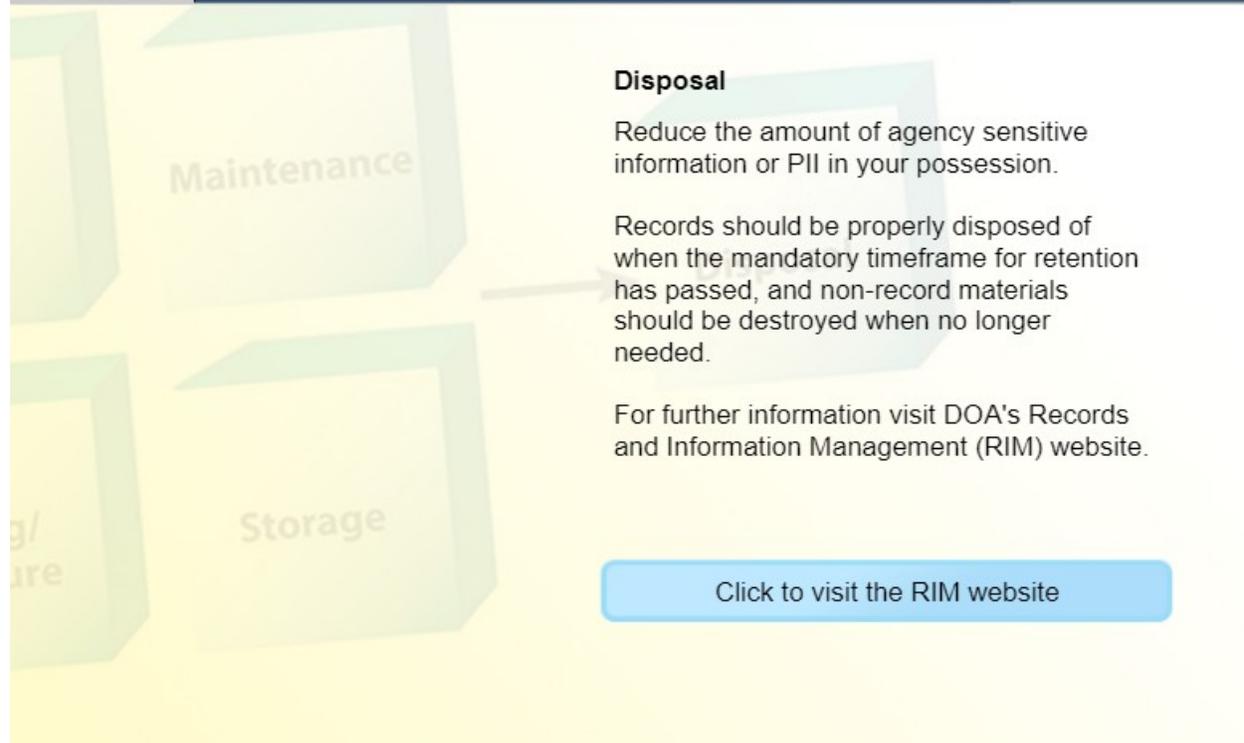
Downloading any files from FDIC-furnished equipment is prohibited. If you have a business requirement that can only be met by using removable media, please refer to FDIC, 1300.4 Directive for the approval authority and process.

Storage – Encryption

The importance of encrypting or password protecting sensitive files cannot be overstated. All FDIC-issued devices are automatically encrypted. However, you must take steps to encrypt sensitive data or PII sent via internal or external email. You should never store unencrypted sensitive information in an easily accessible place. Downloading any files from FDIC-furnished equipment is prohibited. If you have a business requirement that can only be met by using removable media, please refer to FDIC, 1300.4 Directive for the approval authority and process.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS



Disposal

Reduce the amount of agency sensitive information or PII in your possession.

Records should be properly disposed of when the mandatory timeframe for retention has passed, and non-record materials should be destroyed when no longer needed.

For further information visit DOA's Records and Information Management (RIM) website.

Click to visit the RIM website

Disposal

Reduce the amount of agency sensitive information or PII in your possession. Records should be properly disposed of when the mandatory timeframe for retention has passed, and non-record materials should be destroyed when no longer needed. For further information, visit DOA's [Records and Information Management \(RIM\) website](#).

Lesson 5:

Recognize How to Protect Sensitive Information and PII

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

You are the key to security and privacy.



OCISO

The image shows a presentation slide with a blue header and a white central box. The header contains the text 'Lesson 5: Recognize how to protect sensitive information and PII' and a progress bar labeled 'PROGRESS'. The central box contains the text 'You are the key to security and privacy.' above the OCISO logo, which consists of stylized blue lines forming a circular shape above the text 'OCISO' in bold, dark grey letters. The background of the slide is a blue and purple network diagram.

Typically, the strongest link in data protection and security is the user. You are the key to security and privacy. Now let's discuss important ways you can protect information.

Lesson 5: Recognize how to protect sensitive information and PII

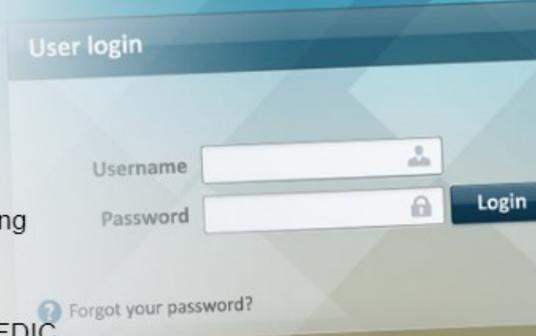
PROGRESS

Access Control

Using another person's identity to access information or to make changes to data is both an ethical and cybersecurity violation, and never acceptable.

To help safeguard your data, consider these guidelines:

- Don't share your password with others.
- Do not share your PIV card or PIN with others.
- Do not allow others to access FDIC systems using your identity.
- Do not write down your password.
- Never allow friends and family members to use FDIC IT Resources (e.g. sharing Wi-Fi/MiFi device).

A screenshot of a user login interface. It features a title bar that says "User login". Below the title bar are two input fields: "Username" with a person icon and "Password" with a lock icon. To the right of the password field is a "Login" button. Below the password field is a link that says "Forgot your password?".

Access Control

Using another person's identity to access information or to make changes to data is both an ethical and cybersecurity violation, and never acceptable.

To help safeguard your data, consider these guidelines;

- Don't share your password with others.
- Do not share your PIV card or PIN with others.
- Do not allow others to access FDIC systems using your identity.
- Do not write down your password.
- Never allow friends and family members to use FDIC IT Resources (e.g., sharing WI-FI/MIFI device).

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Phishing

Form of social engineering used to steal sensitive information.

Attackers will send crafted emails to people within an organization. The email appears to be from someone trustworthy, like your bank, credit card company, or some other entity with which you may have a business relationship.

Clicking the link takes the user to the fake site, which asks for some form of personal information or logon credentials. Sometimes the link can be concealed beneath clickable content, like a video play button.

FDIC is concerned hackers may gain access to information systems.

**Phishing**

Phishing is a form of social engineering used to steal sensitive information. Frequently, attackers will send crafted emails to people within an organization. The email appears to be from someone trustworthy, like your bank, credit card company, or some other entity with which you may have a business relationship. The email will usually include a link to an “officially-looking” website that is actually a fake site operated by the attacker.

Clicking the link takes the user to the fake site, which asks for some form of personal information or logon credentials. Sometimes the link can be concealed beneath clickable content, like a video play button. The attackers use information provided to access the victim’s account or sometimes, the victim’s computer.

While the FDIC is concerned with the safety and security of its employees’ and contractors’ personal financial information, the FDIC is extremely concerned if a hacker gains access to FDIC information systems when an employee or contractor accidentally provides their logon credentials. Attackers regularly update their methods to get past defenses to reach your inbox. We need your help identifying these emails to protect FDIC information.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Phishing Attacks

How to avoid being a victim?

- Do not click on hyperlinks within the suspicious unexpected email.
- Do not download files that are attached to a suspicious unexpected email.
- Do not provide personal information or information about your organization.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Do not give sensitive information to anyone who is not authorized to have it and doesn't have a business need for it.

Phishing Attacks

How to avoid being a victim?

- Do not click on hyperlinks within the suspicious unexpected email.
- Do not download files that are attached to a suspicious unexpected email.
- Do not provide personal information or information about your organization.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Do not give sensitive information to anyone who is not authorized to have it and doesn't have a business need for it.

While malicious websites may look very similar to a legitimate site, understand that the URL may use a variation in spelling or a different domain.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Common Phishing Indicators

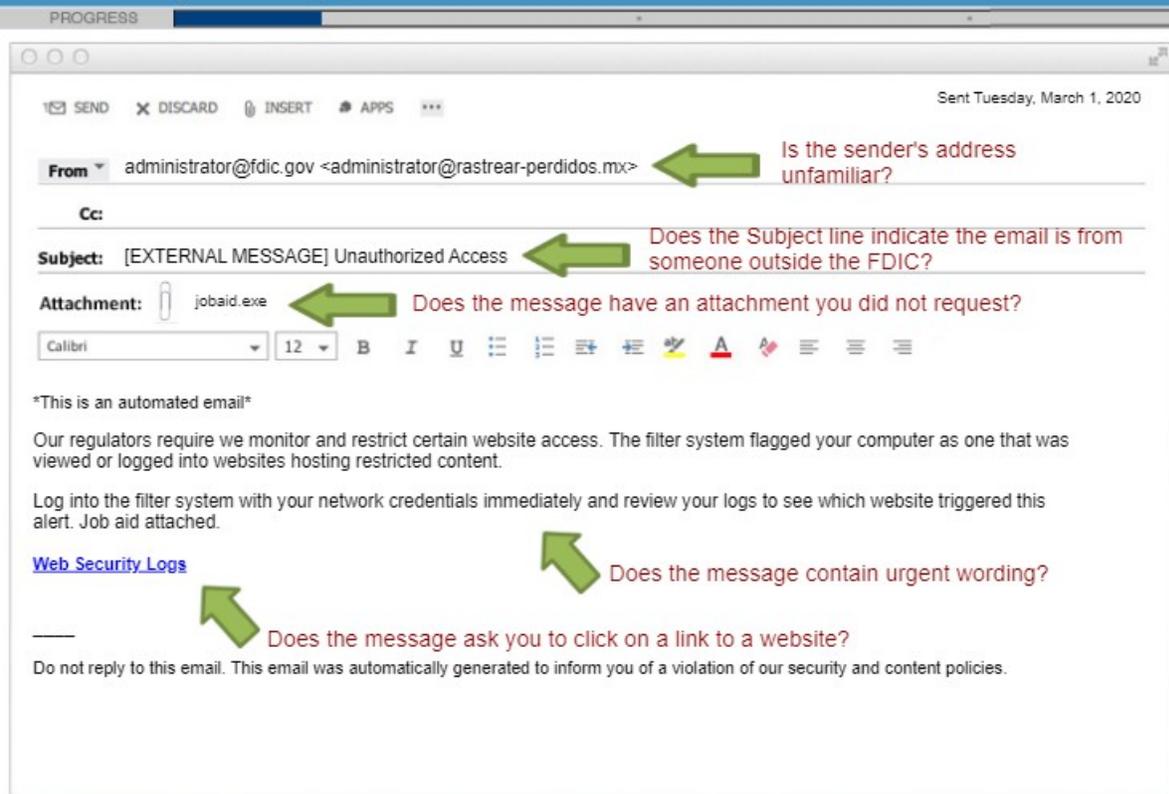
- Unknown sender address
- [External Message] in the Subject Line
- Generic greeting
- Call for "Immediate Action"
- Different link destination (Mouse over email link to determine if destination is different than what is presented)
- Unexpected attachment
- Requests personal information
- Includes grammar and spelling errors



Common Phishing Indicators

- Unknown sender address
- [External Message] in the Subject Line
- Generic greeting
- Call for "Immediate Action"
- Different link destination (Mouse over email link to determine if destination is different than what is presented)
- Unexpected attachment
- Requests personal information
- Includes grammar and spelling errors

Lesson 5: Recognize how to protect sensitive information and PII

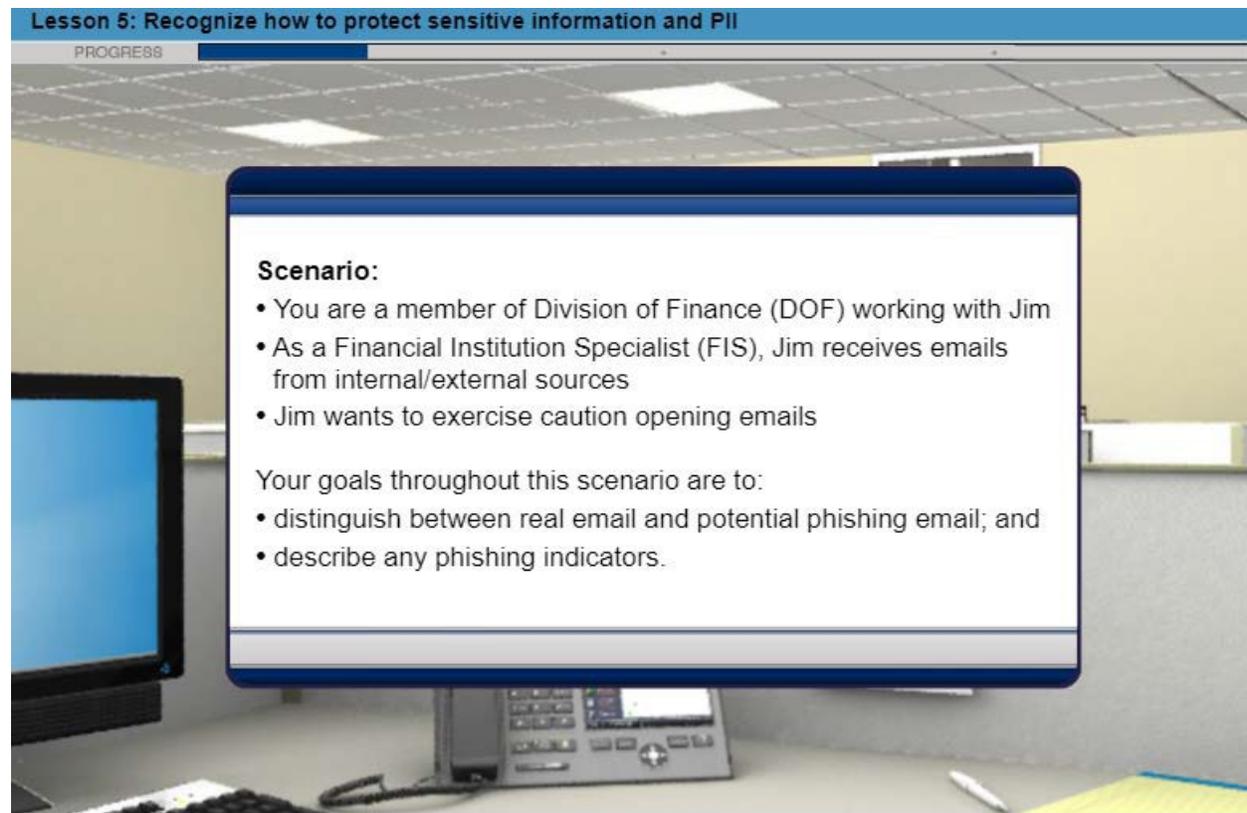


Let's review common clues to help identify a fraudulent phishing email.

- Is the sender's address unfamiliar?
- Does the subject line begin with "External Message"?
- Does the message content contain a generic greeting?
- Is the message written with poor or awkward grammar?
- Does the message ask you to click on a link to a website?
- Does the message ask you to provide your user name and password or other login credentials?
- Does the message contain urgent wording?
- Does the message have an attachment you did not request?
- Does the message body contain only an image?
- Does the message make promises that seem too good to be true?
- Is the message content signed by an individual or an organization you do not know?

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



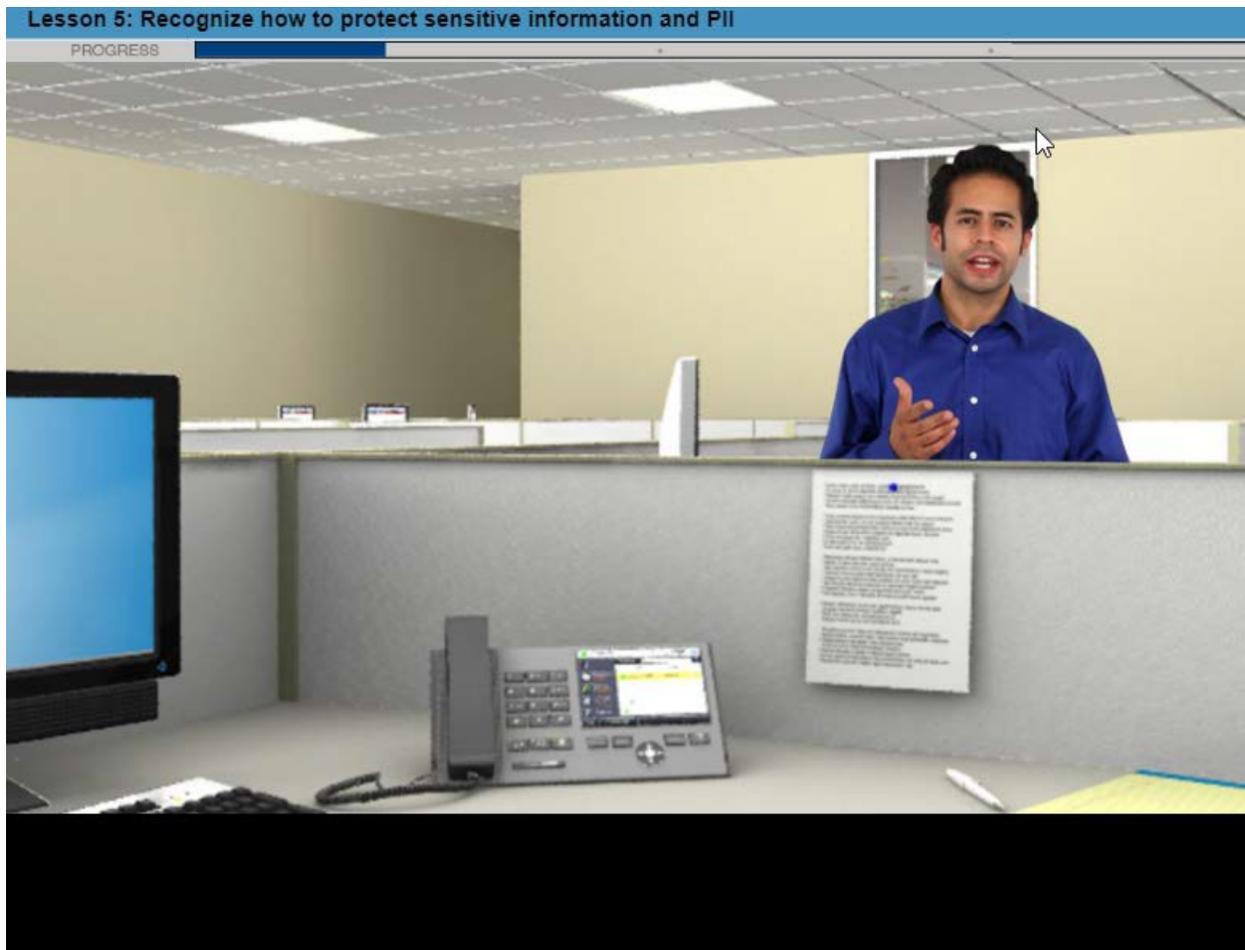
Scenario:

- You are a member of Division of Finance (DOF) working with Jim
- As a Financial Institution Specialist (FIS), Jim receives emails from internal/external sources
- Jim wants to exercise caution opening emails

Your goals throughout this scenario are to:

- distinguish between real email and potential phishing email; and
- describe any phishing indicators.

Scenario: You will now enter a simulated scenario about phishing emails. In this scenario, you are a member of Division of Finance (DOF) working with Jim who joined the FDIC about 6 months ago. As a Financial Institution Specialist (FIS), Jim receives emails from internal/external sources. Jim wants to exercise caution opening emails. Your goals throughout this scenario are to distinguish between real email and potential phishing email; and describe any phishing indicators.



Since I am new here, I'm still trying to get familiar with the Information Security Policy, so I have some questions. I recently received an email and I'm not sure if it's a real or phishing email. Is this a Phish or a Real email?

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Sent Tuesday, March 1, 2020

From: IT Security <itsecurity@fdic.com>

Cc:

Subject: [EXTERNAL MESSAGE] Security Notice

Attachment: Password Review

Calibri 12 B I U

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security
Federal Deposit Insurance Agency

Is this email Phish or Real?

It looks like a phishing email.

I think it's a real email.

SUBMIT

From: IT Security itsecurity@fdic.com – Sent Tuesday, March 1, 2020

Subject: [EXTERNAL MESSAGE] Security Notice

Attachment: Password Review

IMPORTANT SECURITY NOTICE

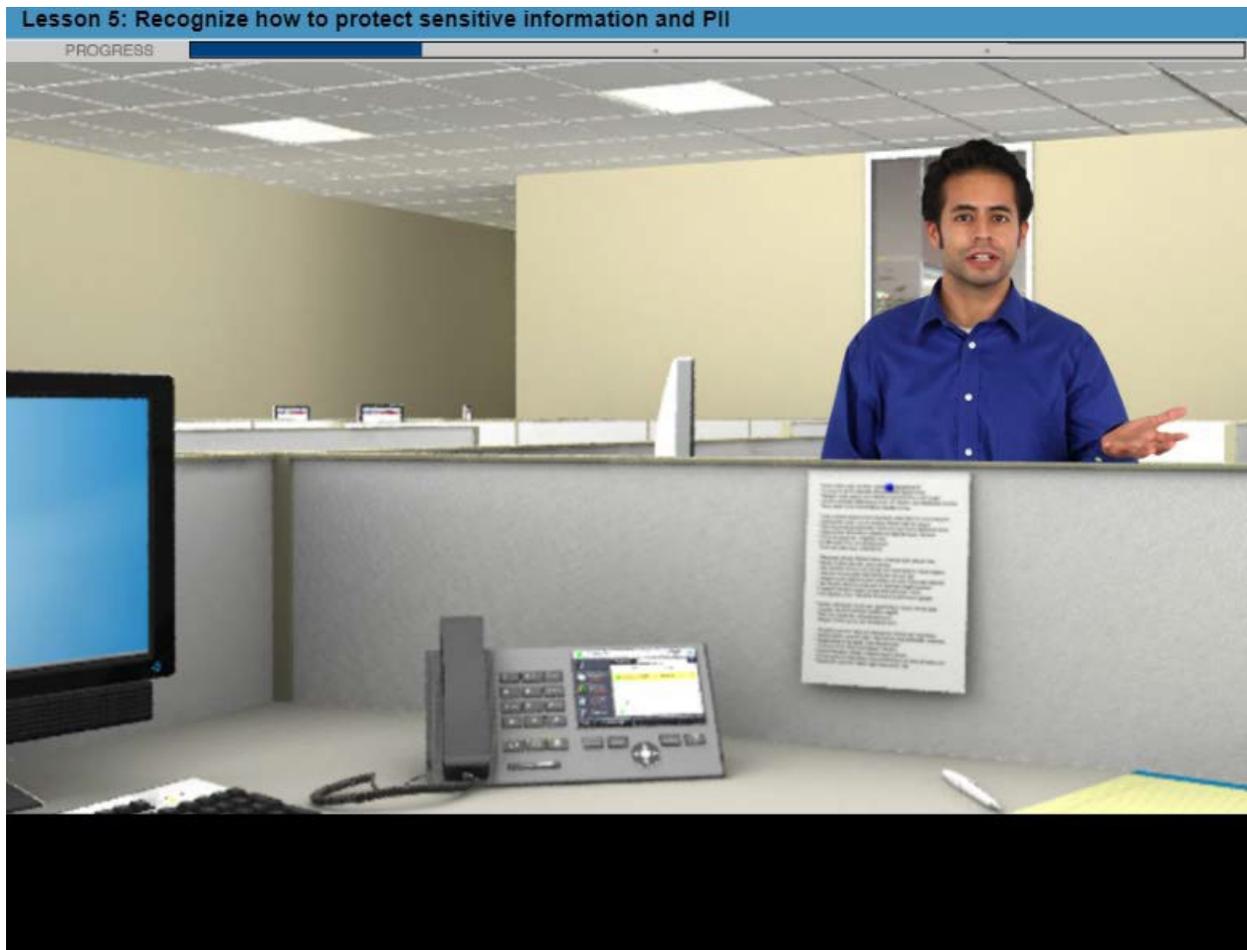
Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security

Federal Deposit Insurance Agency

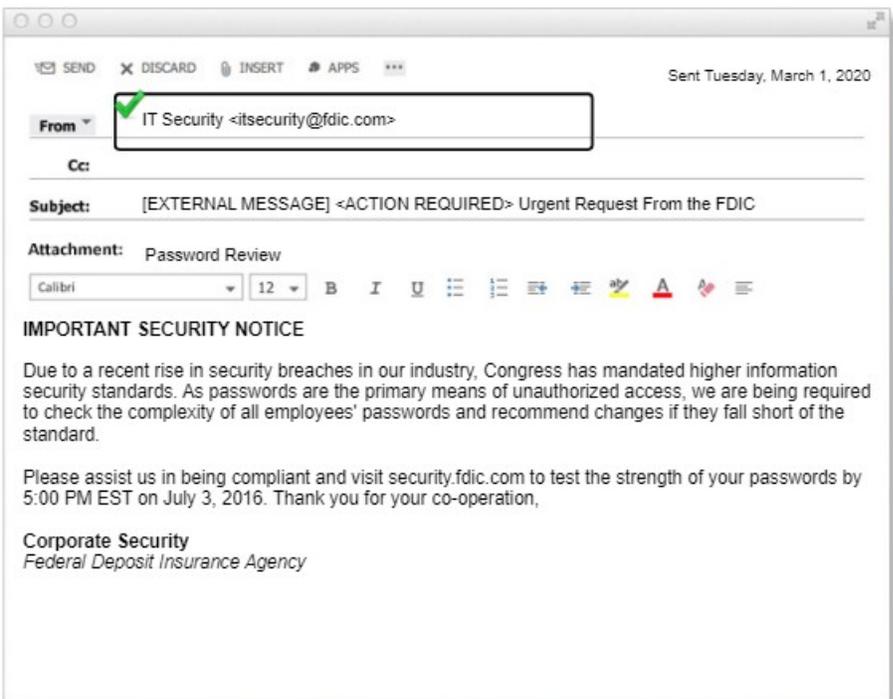
Is this email Phish or Real? *It looks like phishing email is selected.*



Is it? Can you show me what makes it a phishing email?

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



Instructions:
Click the part of the email that is a phishing indicator.
There are 5 indicators in this email.

FEEDBACK:
That's correct.
It's important to identify the domain address.
The email is coming from "fdic.com" instead of "fdic.gov".

From: IT Security <itsecurity@fdic.com>

Cc:

Subject: [EXTERNAL MESSAGE] <ACTION REQUIRED> Urgent Request From the FDIC

Attachment: Password Review

Calibri 12 B I U

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security
Federal Deposit Insurance Agency

From: IT Security itsecurity@fdic.com – Sent Tuesday, March 1, 2020

Subject: [EXTERNAL MESSAGE] Security Notice

Attachment: Password Review

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security

Federal Deposit Insurance Agency

Instructions: Click the part of the email that is a phishing indicator.

Domain Name is selected.

Feedback: That's correct. It's important to identify the domain address. The email is coming from "fdic.com" instead of "fdic.gov".

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Instructions:
Click the part of the email that is a phishing indicator.
There are 5 indicators in this email.

FEEDBACK:
That's correct.
It is important to identify the sender of the email. This email is signed "Federal Deposit Insurance Agency" instead of "Federal Deposit Insurance Corporation."

From: IT Security itsecurity@fdic.com – Sent Tuesday, March 1, 2020

Subject: [EXTERNAL MESSAGE] Security Notice

Attachment: Password Review

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security

Federal Deposit Insurance Agency

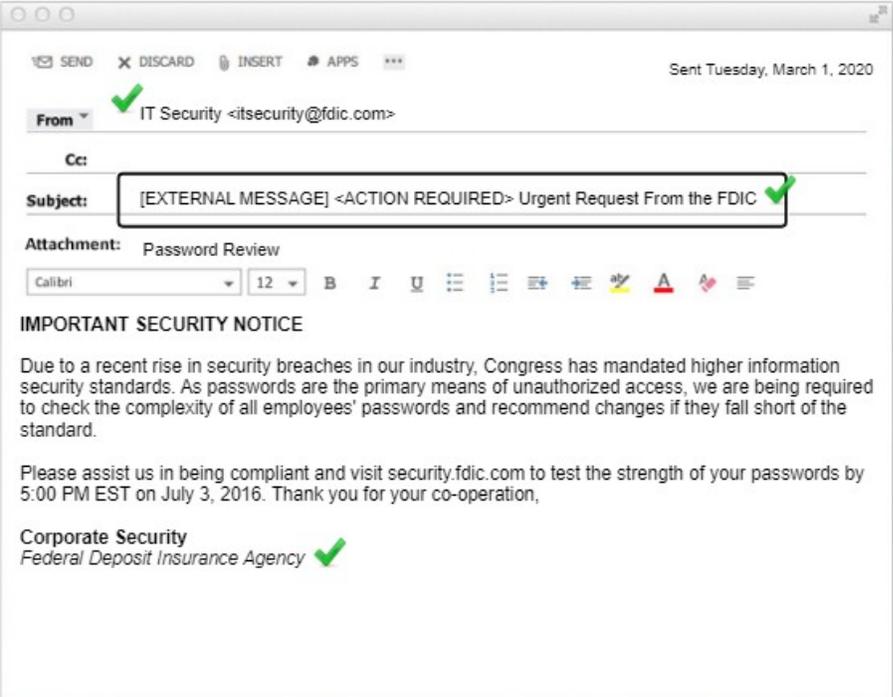
Instructions: Click the part of the email that is a phishing indicator.

Sender name is selected.

Feedback: That's correct. It is important to identify the sender of the email. This email is signed "Federal Deposit Insurance Agency" instead of "Federal Deposit Insurance Corporation."

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



Sent Tuesday, March 1, 2020

From: IT Security <itsecurity@fdic.com>

Cc:

Subject: [EXTERNAL MESSAGE] <ACTION REQUIRED> Urgent Request From the FDIC

Attachment: Password Review

Calibri 12 B I U

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security
Federal Deposit Insurance Agency

Instructions:
Click the part of the email that is a phishing indicator.
There are 5 indicators in this email.

FEEDBACK:
That's correct.
The "[EXTERNAL MESSAGE]" tag in the subject line indicates the email originated from outside the FDIC.

From: IT Security itsecurity@fdic.com – Sent Tuesday, March 1, 2020

Subject: [EXTERNAL MESSAGE] Security Notice

Attachment: Password Review

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security

Federal Deposit Insurance Agency

Instructions: Click the part of the email that is a phishing indicator.

Subject line is selected.

Feedback: That's correct. The "[EXTERNAL MESSAGE]" tag in the subject line indicates the email originated from outside the FDIC.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Instructions:
Click the part of the email that is a phishing indicator.
There are 5 indicators in this email.

FEEDBACK: That's correct. It is important to identify the domain of any links in an email. The link in this email directs you to "fdic.com" instead of "fdic.gov."

From: IT Security itsecurity@fdic.com – Sent Tuesday, March 1, 2020

Subject: [EXTERNAL MESSAGE] Security Notice

Attachment: Password Review

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security

Federal Deposit Insurance Agency

Instructions: Click the part of the email that is a phishing indicator.

Link in the email is selected.

Feedback: That's correct. It is important to identify the domain of any links in an email. The link in this email directs you to "fdic.com" instead of "fdic.gov."

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Instructions:
Click the part of the email that is a phishing indicator.
 There are 5 indicators in this email.

FEEDBACK:
 That's correct.
 The email is dated March 1, 2020, and in the email is the request for information by July 3, 2016.

From: IT Security itsecurity@fdic.com – Sent Tuesday, March 1, 2020

Subject: [EXTERNAL MESSAGE] Security Notice

Attachment: Password Review

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

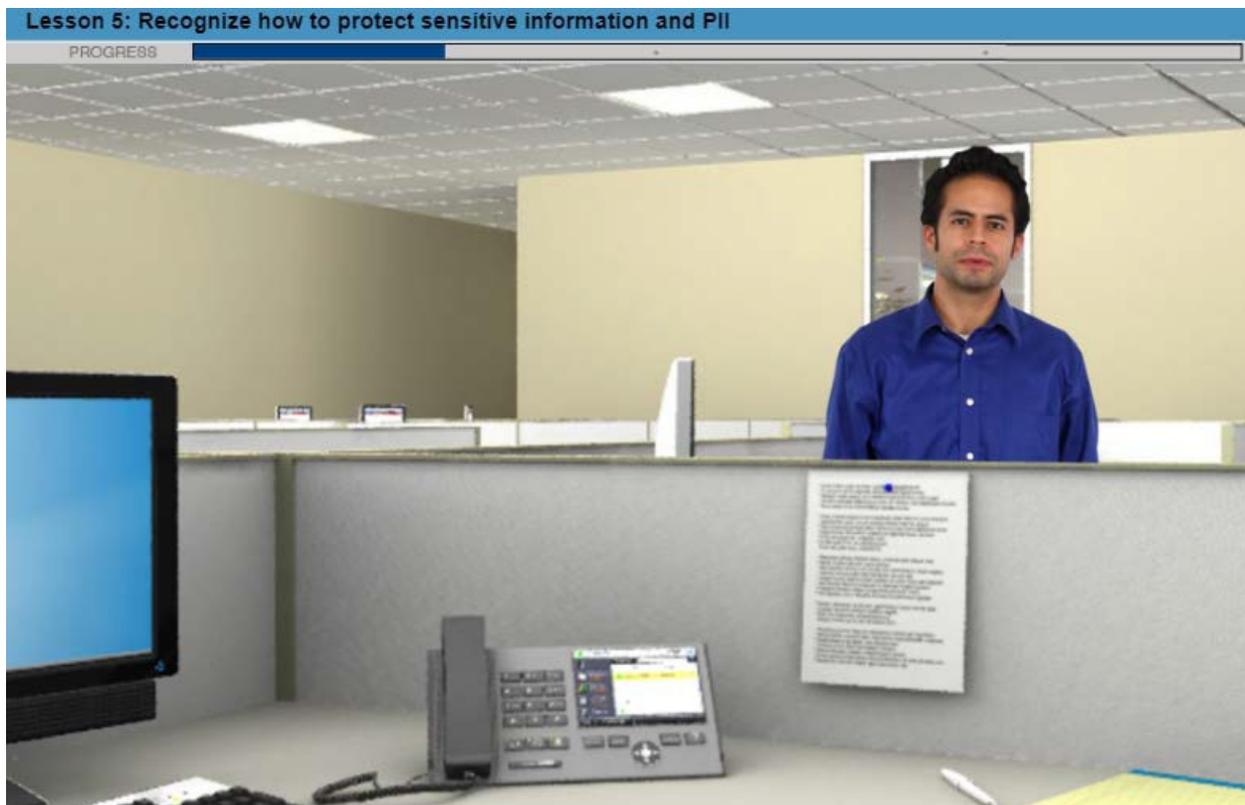
Corporate Security

Federal Deposit Insurance Agency

Instructions: Click the part of the email that is a phishing indicator.

The date of the email is selected.

Feedback: That's correct. The email is dated March 1, 2020, and in the email is the request for information by July 3, 2016.

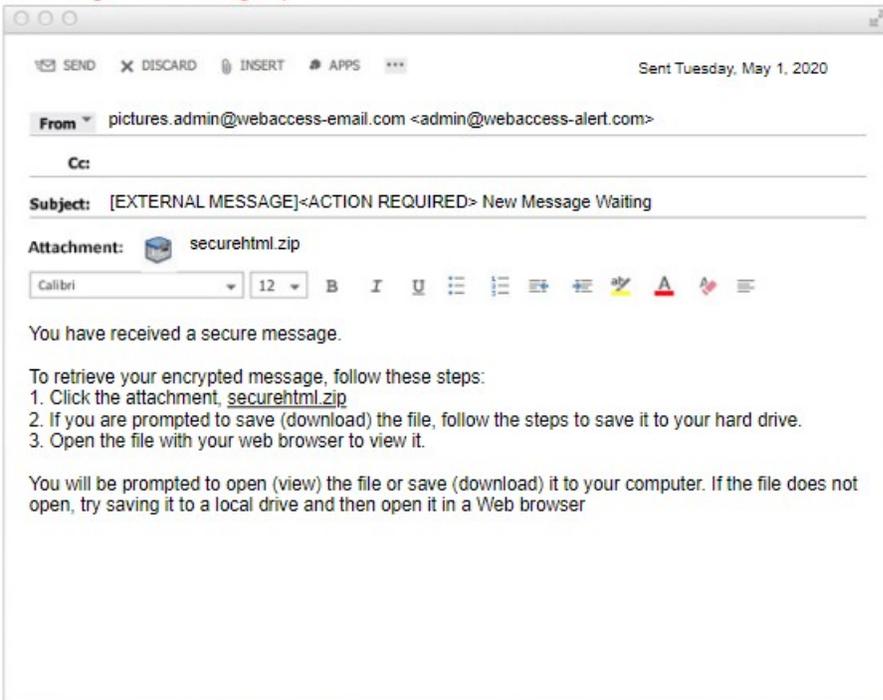


Here's another email. Richard mentioned that he received a similar message and is sure it's a phishing email. Is this a Phish or a Real email?

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

This message was sent with High importance



Is this email
Phish or Real?

✓ I think it's a phishing email.

It looks like a real email.

SUBMIT

From: pictures.admin@webaccess-email.com<admin@webaccess-alter.com> - Sent Tuesday, May 1, 2020

Subject: [EXTERNAL MESSAGE]<ACTION REQUIRED>New message Waiting

Attachment: securehtml.zip

You have received a secure message.

To retrieve your encrypted message, follow these steps:

1. Click the attachment, [securehtml.zip](#)
2. If you are prompted to save (download) the file, follow the steps to save it to your hard drive.
3. Open the file with your web browser to view it.

You will be prompted to open (view) the file or save (download) it to your computer. If the file does not open, try saving it to a local drive and then open it in a Web browser

Is this email Phish or Real? *I think it's a phishing email is selected.*

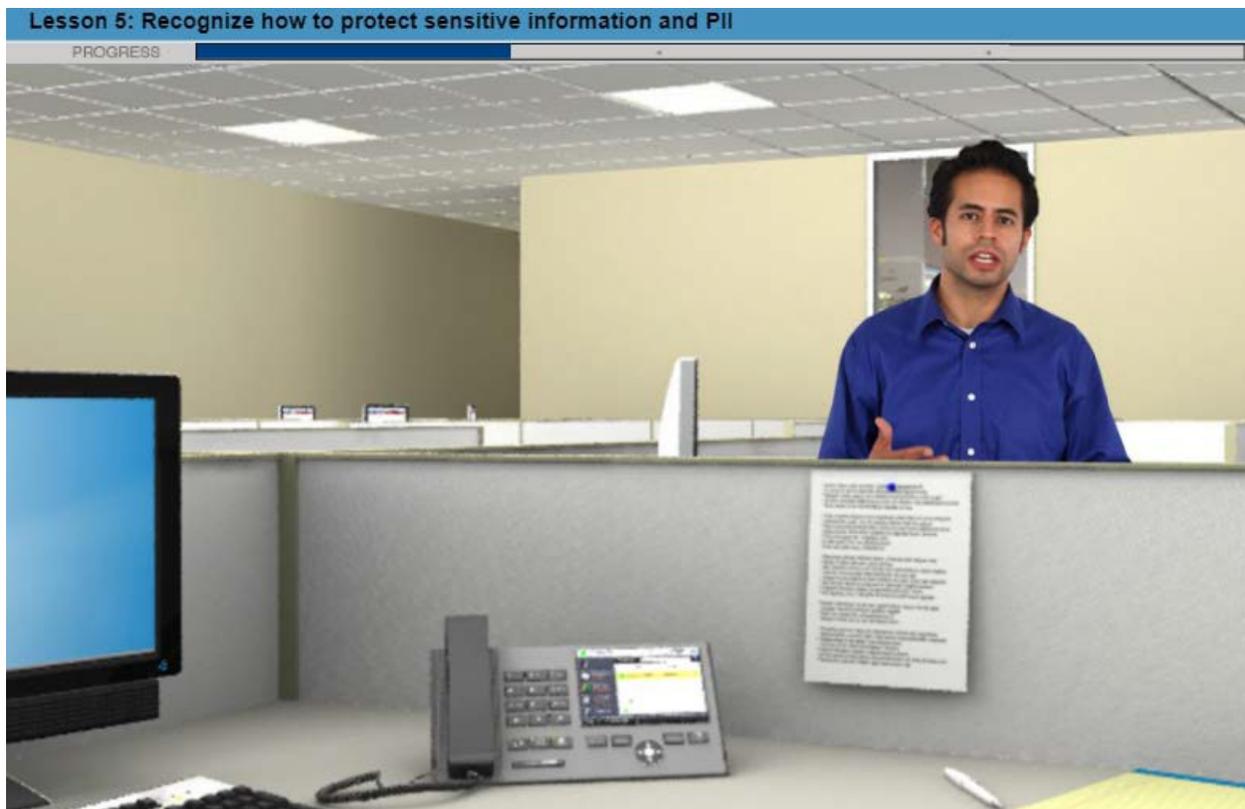
Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

 Feedback: That's correct. This email is coming from an unknown email address. Note the "[EXTERNAL MESSAGE]" tag in the Subject line. Although in the contents it mentions that it is a secure encrypted message, the attachment is an illegitimate file.



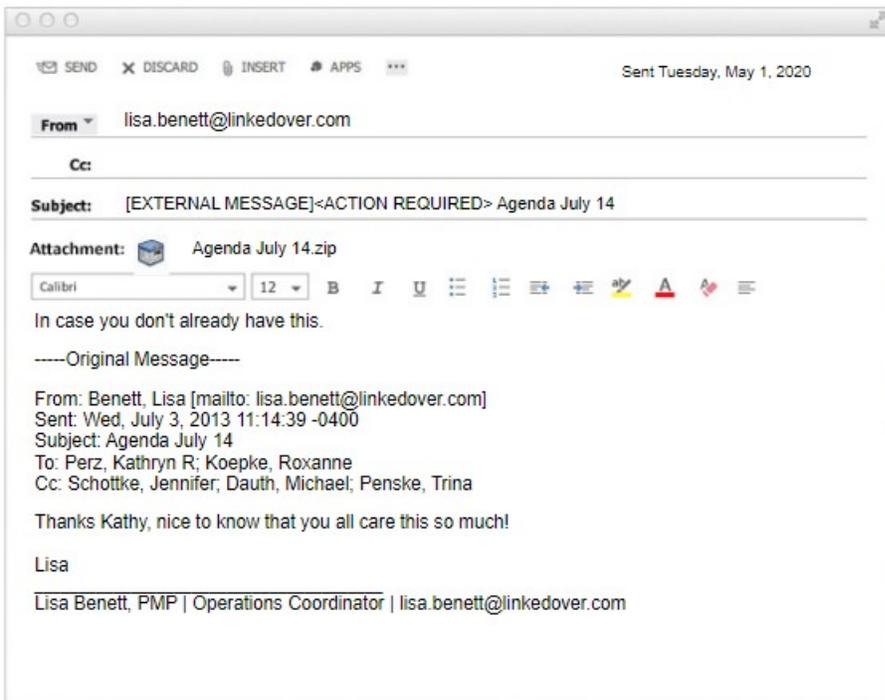
Feedback: That's correct. This email is coming from an unknown email address. Note the "[EXTERNAL MESSAGE]" tag in the Subject line. Although in the contents it mentions that it is a secure encrypted message, the attachment is an illegitimate file.



That is great information to keep in mind. I wouldn't have thought about the risks of opening an attachment in an email from an unknown source. I have one more email for you to review. Do you think this is a phishing email?

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



Is this email
Phish or Real?

It looks like a phishing email.

I think it's a real email.

From: lisa.benett@linkedover.com- Sent Tuesday, May 1, 2020

Subject: [EXTERNAL MESSAGE]<ACTION REQUIRED> Agenda July 14

Attachment: Agenda July 14.zip

In case you don't already have this.

---Original Message---

From: Benett, Lisa [mailto:lisa.benett@linkedover.com]

Sent: Wed, July 3, 2013 11:14:39-0400

Subject: Agenda July 14

To: Perz, Kathryn R; Koepke, Roxanne

Cc: Schottke, Jennifer; Dauth, Michael; Penske, Trina

Thanks Kathy, nice to know that you all care this so much!

Lisa

Lisa Benett, PMP | Operations Coordinator | lisa.benett@linkedover.com

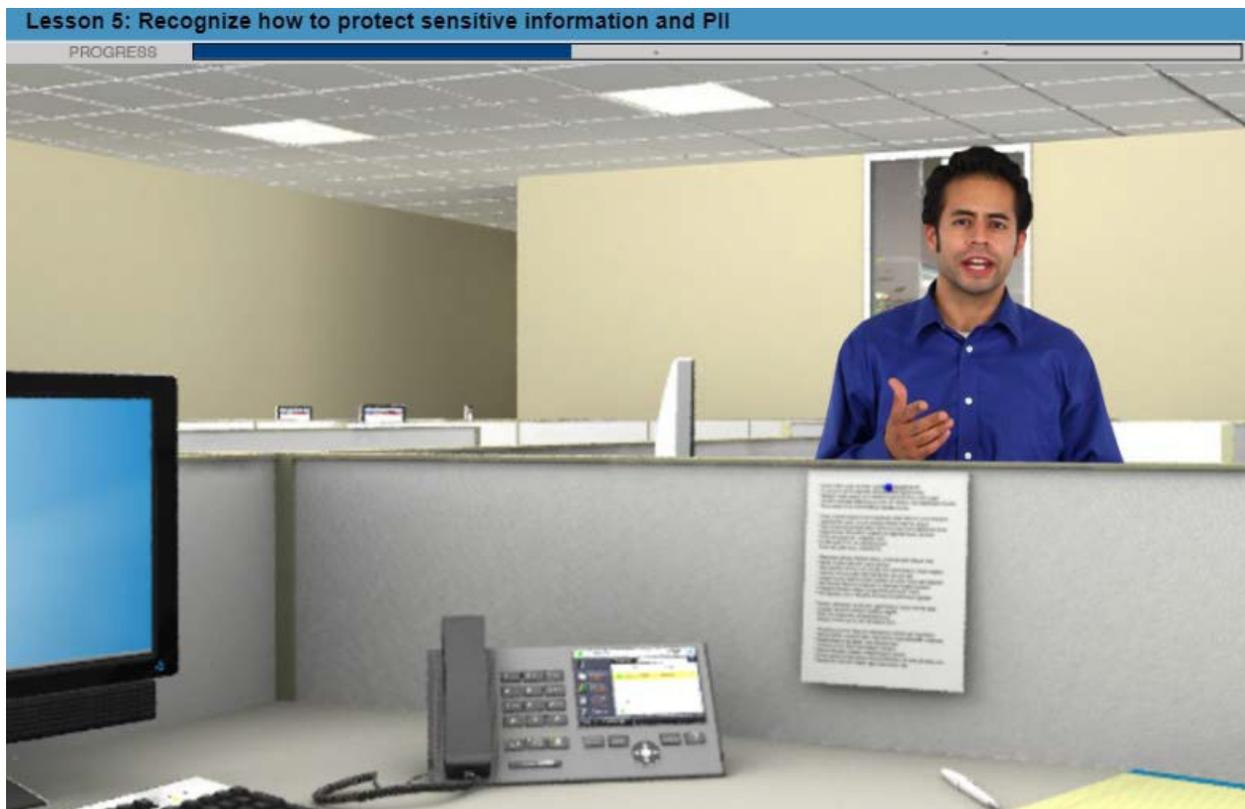
Is this email Phish or Real? *It looks like a phishing email is selected.*

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

 Feedback: That's correct. This email is coming from an unknown email address. Note the "[EXTERNAL MESSAGE]" tag in the Subject line. This tag indicates the message originates from outside the FDIC. Also, the attachment is an illegitimate file.

Feedback: That's correct. This email is coming from an unknown email address. Note the "[EXTERNAL MESSAGE]" tag in the Subject line. This tag indicates the message originates from outside the FDIC. Also, the attachment is an illegitimate file.



That's good to know. I really learned something about phishing emails. I'll be sure to keep an eye out for all the indicators you mentioned every time I checked my emails. Thank you for your help.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Recognize Phishing Attempts

Successfully recognizing phishing emails is critical to maintaining secure communication.

Common clues to look for include:

- An unfamiliar sender address
- [EXTERNAL MESSAGE] in the Subject line
- A generic greeting
- Call for immediate action
- Different link destination
- Unexpected attachments
- Request for personal information
- Grammar/Spelling errors

**Recognize Phishing Attempts**

Being able to recognize phishing emails is critical to maintaining secure communication. Since this topic is so important and affects nearly every FDIC employee and contractor, let's review key points about phishing. To avoid or minimize these losses, you must be able to recognize phishing attempts. Remember that you are the FDIC's best defense against phishing attacks.

Common clues to look for include:

- An unfamiliar sender address
- [EXTERNAL MESSAGE] in Subject line
- A generic greeting
- Call for immediate action
- Different link destination
- Unexpected attachments
- Request for personal information
- Grammar/Spelling errors

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

File Home Send / Receive Folder View Enterprise Vault McAfee E-mail Scan Live Meeting Service Adobe PDF

New E-mail Items New Delete Reply Reply All Forward More CSS Training To Manager Team E-mail Move Rules OneNote Assign Policy Follow Up Find a Contact Address Book Filter E-mail Report Phishing PhishMe

From: IT Security <itsecurity@fdic.com>

Cc:

Subject: [EXTERNAL MESSAGE] Security Notice

Calibri 12 B I U [List Icons]

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

Corporate Security
Federal Deposit Insurance Agency

To Report Phishing:

- Highlight the email
- Click "Report Phishing" button to automatically forward to FDIC's security operations

From: IT Security itsecurity@fdic.com

Subject: [EXTERNAL MESSAGE] Security Notice

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary means of unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standard.

Please assist us in being compliant and visit security.fdic.com to test the strength of your passwords by 5:00 PM EST on July 3, 2016. Thank you for your co-operation,

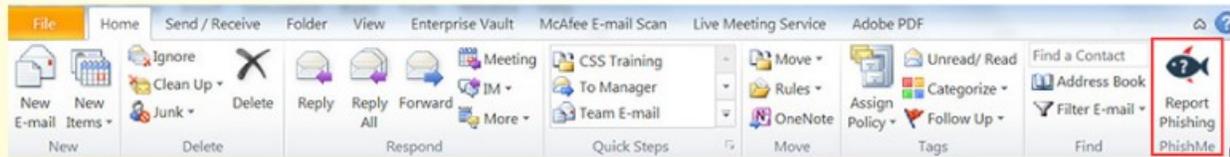
Corporate Security

Federal Deposit Insurance Agency

To Report Phishing: Highlight the email. Click "Report Phishing" button to automatically forward to FDIC's security operations.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

**Report Phishing**

- You may also click the “Report Phishing” button even if you have already opened the email
- Periodically delete these messages from your Junk Email folder
- This feature should not be used to report spam emails
- Contact the DIT Help Desk for assistance if you do not see the “Report Phishing” button in Outlook

Report Phishing

- You may also click the “Report Phishing” button even if you have already opened the email.
- Periodically delete these messages from your Junk Email folder.
- This feature should not be used to report spam emails.
- Contact the DIT Help Desk for assistance if you do not see the “Report Phishing” button in Outlook.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Acceptable Use Policy for FDIC Information Technology

The purpose of the FDIC's Acceptable Use Policy is to establish the acceptable behavior of employees, contractors, and authorized visitors to ensure the protection and integrity of the FDIC's computer systems and information assets.

To ensure that personal use does not interfere with normal business activities, please remember these key policies:

- Secure your portable FDIC-furnished devices at all times
- Never share your password, PIV card, or PIN with anyone
- Always lock your screen when you leave your computer or device if unattended
- Never use your FDIC-furnished device for any illegal or inappropriate activity
- Never send text messages using either FDIC-furnished or personally owned IT resources, while operating an FDIC-owned, -leased, or -rented motor vehicle
- Never send text messages while operating a privately owned vehicle on official FDIC business
- Never download any information from any FDIC IT device to a removable media, unless explicitly authorized by your Division or Office Director and the FDIC CIO
- Never install or use unauthorized software or services designed to share data
- Never use non-FDIC email accounts to transmit or receive FDIC information; and
- Never allow friends and family member's access to FDIC- furnished equipment

Acceptable Use Policy for FDIC Information Technology

The purpose of the FDIC's Acceptable Use Policy is to establish the acceptable behavior of employees, contractors, and authorized visitors to ensure the protection and integrity of the FDIC's computer systems and information assets.

To ensure that personal use does not interfere with normal business activities, please remember these key policies:

- Secure your portable FDIC-furnished devices at all times.
- Never share your password, PIV card, or PIN with anyone.
- Always lock your screen when you leave your computer or device if unattended.
- Never use your FDIC-furnished device for any illegal or inappropriate activity.
- Never send text messages using either FDIC-furnished or personally owned IT resources, while operating an FDIC-owned, -leased, or -rented motor vehicle.
- Never send text messages while operating a privately owned vehicle on official FDIC business.
- Never download any information from any FDIC IT device to a removable media, unless explicitly authorized by your Division or Office Director and the FDIC CIO.
- Never install or use unauthorized software or services designed to share data.
- Never use non-FDIC email accounts to transmit or receive FDIC information.
- Never allow friends or family member's access to FDIC- furnished equipment.

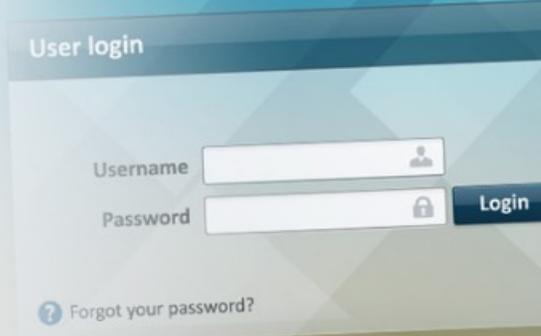
Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Email Cautions

- Do not email agency sensitive information or PII to your personal email account.
- Send sensitive information electronically only when required. Email messages containing sensitive information shall always be encrypted using an FDIC-approved encryption product.
- Use care when opening weblinks and email attachments.

As a reminder, FDIC employees and contractors are no longer permitted to copy data to removable media.



The screenshot shows a 'User login' form with two input fields: 'Username' and 'Password'. The 'Username' field has a person icon on the right, and the 'Password' field has a lock icon. A 'Login' button is to the right of the password field. Below the fields is a link that says 'Forgot your password?' with a question mark icon.

Email Cautions

FDIC employees and contractors must use official FDIC email accounts when transmitting or receiving FDIC information and must use care when opening web links and email attachments, particularly “executable files.”

- Do not email agency sensitive information or PII to your personal email account.
- Send sensitive information electronically only when required. Email messages containing sensitive information shall always be encrypted using an FDIC-approved encryption product.
- Use care when opening weblinks and email attachments.
- As a reminder, FDIC employees and contractors are no longer permitted to copy data to removable media.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Encryption Tools – Emails and Attachments

Click each option to review its definition.



Azure Information Protection (AIP) is Microsoft's digital rights management tool, used for encrypting and decrypting email at the FDIC. FDIC's version of AIP offers two templates for protecting email to FDIC internal users:

- FDIC-Information Protection "Encrypt" – Apply this template to allow FDIC email recipients to: View, Open, Read, Save, Edit Content, Edit, View Rights, Allow Macros, Forward, Print, Reply, and Reply All to the message.
- FDIC-Information Protection "Encrypt-Restricted" – Apply this template to allow FDIC email recipients to ONLY: View, Open, Read, Reply, and Reply All to the message. (The "Encrypt-Restricted" template does not allow recipients to Forward, Save, Copy, Print, Print Screen, or use the Snipping Tool.)

The determination of when to use each template will be up to the business. There are no FDIC-wide guidelines at this time for when to use each level of encryption.

Encryption Tools – Emails and Attachments

Click each to review its definition.

- AIP
- Zix Secure E-mail
- PK Zip
- GlobalScape

Azure Information Protection (AIP): is Microsoft's digital rights management tool, used for encrypting and decrypting email at the FDIC. FDIC's version of AIP offers two templates for protecting email to FDIC internal users:

- FDIC-Information Protection "Encrypt" – Apply this template to allow FDIC email recipients to: View, Open, Read, Save, Edit Content, Edit, View Rights, Allow Macros, Forward, Print, Reply, and Reply All to the message.
- FDIC-Information Protection "Encrypt-Restricted" – Apply this template to allow FDIC email recipients to ONLY: view, Open, Read, Reply, and Reply All to the message. (The "Encrypt-Restricted" template does not allow recipients to Forward, Save, Copy, Print, Print Screen, or use the Snipping Tool.)

The determination of when to use each template will be up to the business. There is no FDIC-wide guidelines at this time for when to use each level of encryption.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Encryption Tools – Emails and Attachments

Click each option to review its definition.



Zix secure e-mail is an FDIC Secure email Service which allows FDIC employees to communicate confidential and sensitive business information through a secure channel with individuals outside the FDIC (external users only).

Zix Secure E-mail: is an FDIC Secure email Service which allows FDIC employees to communicate confidential and sensitive business information through a secure channel with individuals outside the FDIC (external users only).

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Encryption Tools – Emails and Attachments

Click each option to review its definition.



The standard FDIC desktop and laptop have been configured with PK Zip, a software utility that allows for the encryption of .zip files. Encrypted .zip files may be sent both internally or externally (such as to outside vendors or contractors) as attachments in email.

PK Zip: The standard FDIC desktop and laptop have been configured with PK Zip, a software utility that allows for the encryption of .zip files. Encrypted .zip files may be sent both internally or externally (such as to outside vendors or contractors) as attachments in email.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Encryption Tools – Emails and Attachments

Click each option to review its definition.

AIP

Zix Secure E-mail

PK Zip

GlobalScape

GlobalScape is used to transmit large files up to 10 Gb and is externally hosted. Recipients receive a link to access files. Access can be requested through ARCS.

GlobalScape: is used to transmit large files up to 10 Gb and is externally hosted. Recipients receive a link to access files. Access can be requested through ARCS.

Lesson 5: Recognize how to protect sensitive information and PII

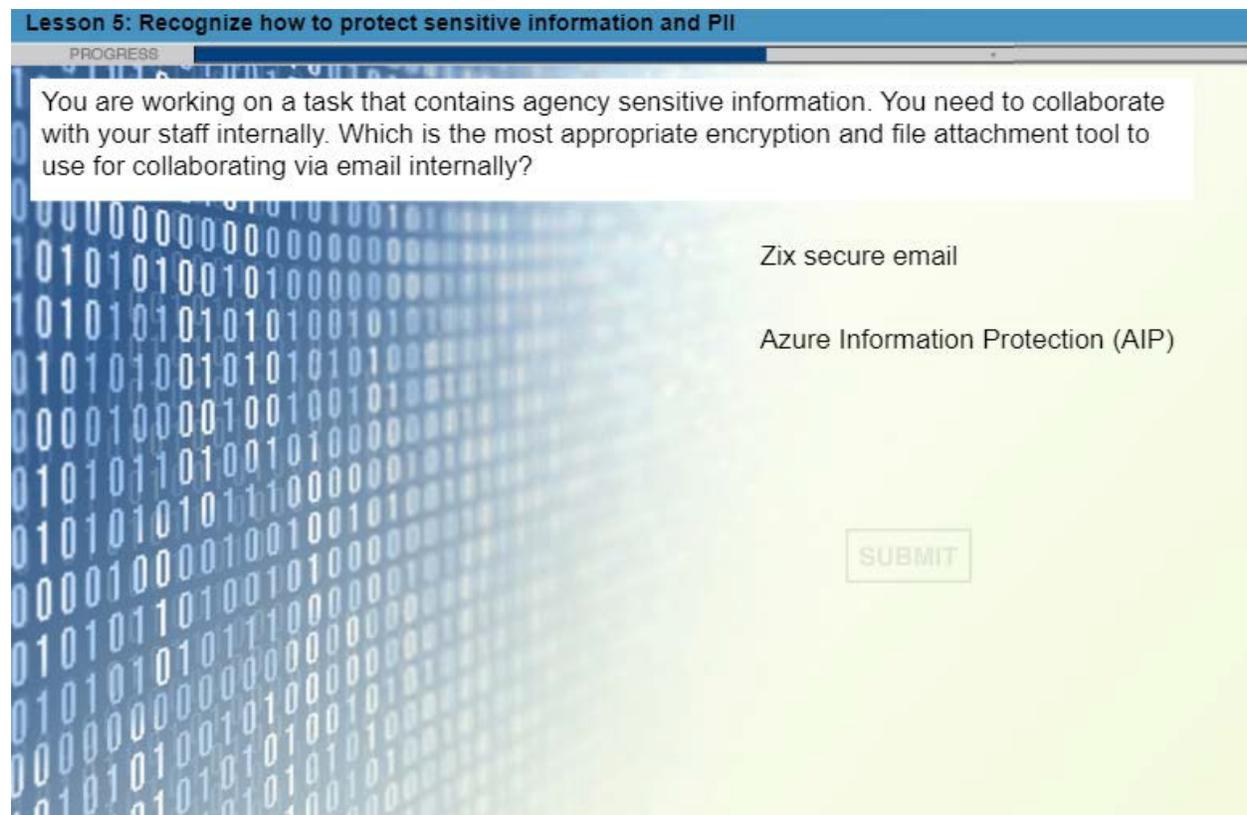
PROGRESS

You are working on a task that contains agency sensitive information. You need to collaborate with your staff internally. Which is the most appropriate encryption and file attachment tool to use for collaborating via email internally?

Zix secure email

Azure Information Protection (AIP)

SUBMIT

The image is a screenshot of a quiz interface. At the top, there is a blue header bar with the text "Lesson 5: Recognize how to protect sensitive information and PII". Below this is a progress bar labeled "PROGRESS". The main content area has a light green background with a blue binary code pattern on the left side. A white text box contains the question: "You are working on a task that contains agency sensitive information. You need to collaborate with your staff internally. Which is the most appropriate encryption and file attachment tool to use for collaborating via email internally?". Below the question, there are two radio button options: "Zix secure email" and "Azure Information Protection (AIP)". At the bottom right of the options, there is a "SUBMIT" button.

You are working on a task that contains agency sensitive information. You need to collaborate with your staff internally. Which is the most appropriate encryption and file attachment tool to use for collaborating via email internally?

Choices:

- Zix secure email
- Azure Information Protection (AIP)

Azure Information Protection (AIP) is selected.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



Feedback: That's correct. You should use the Azure Information Protection (AIP) tool for sending emails containing SI internally to other FDIC staff.

The image shows a feedback message on a yellow background with several faint speech bubble icons. The message is preceded by a green bar icon, indicating a correct answer.

Feedback: That's correct. You should use the Azure Information Protection (AIP) tool for sending emails containing SI internally to other FDIC staff.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Why is AIP the most appropriate tool?

- a. It allows you to securely exchange confidential and sensitive information with other users inside the FDIC.
- b. It allows FDIC employees to communicate confidential and sensitive business information through a secure channel with individuals outside the FDIC (external users only).
- c. Although the email is not encrypted the file attachment is encrypted to the email.

SUBMIT

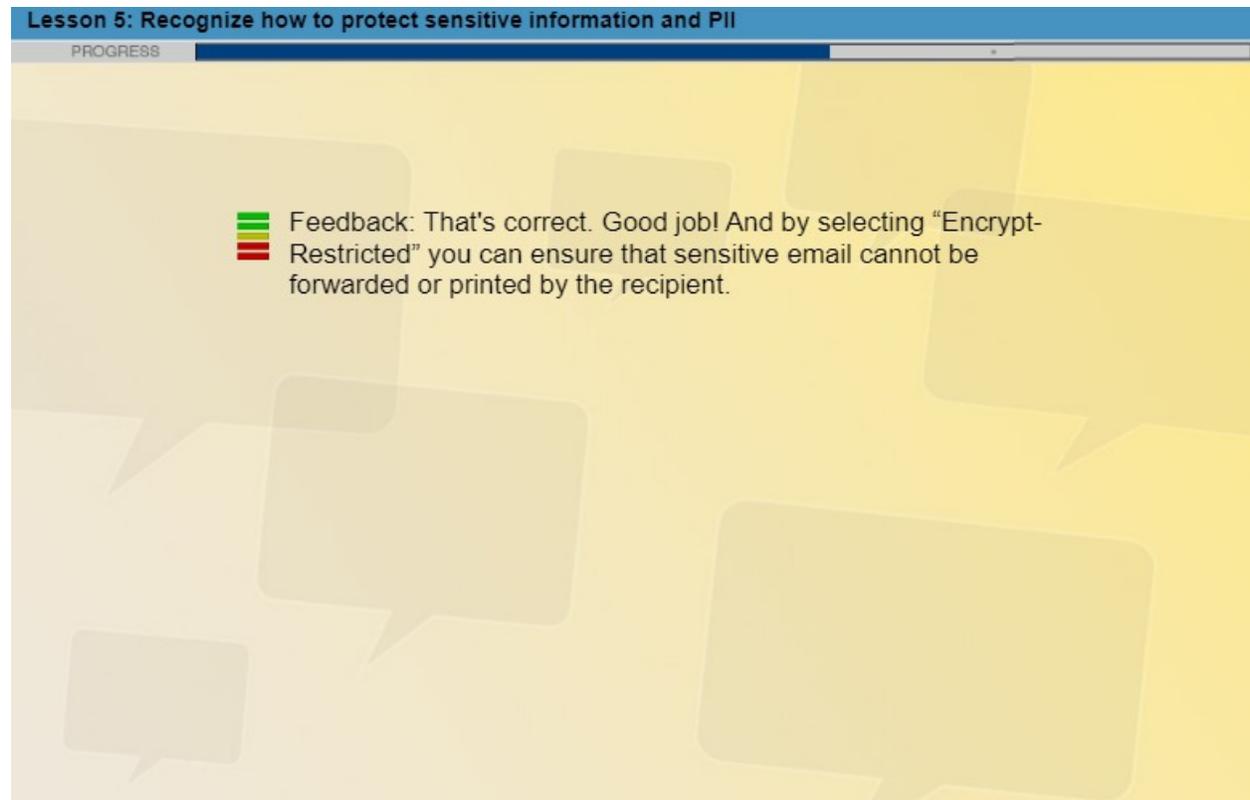
Why is AIP the most appropriate tool?

- a. It allows you to securely exchange confidential and sensitive information with other users inside the FDIC.
- b. It allows FDIC employees to communicate confidential and sensitive business information through a secure channel with individuals outside the FDIC (external users only).
- c. Although the email is not encrypted the file attachment is encrypted to the email.

A is selected.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



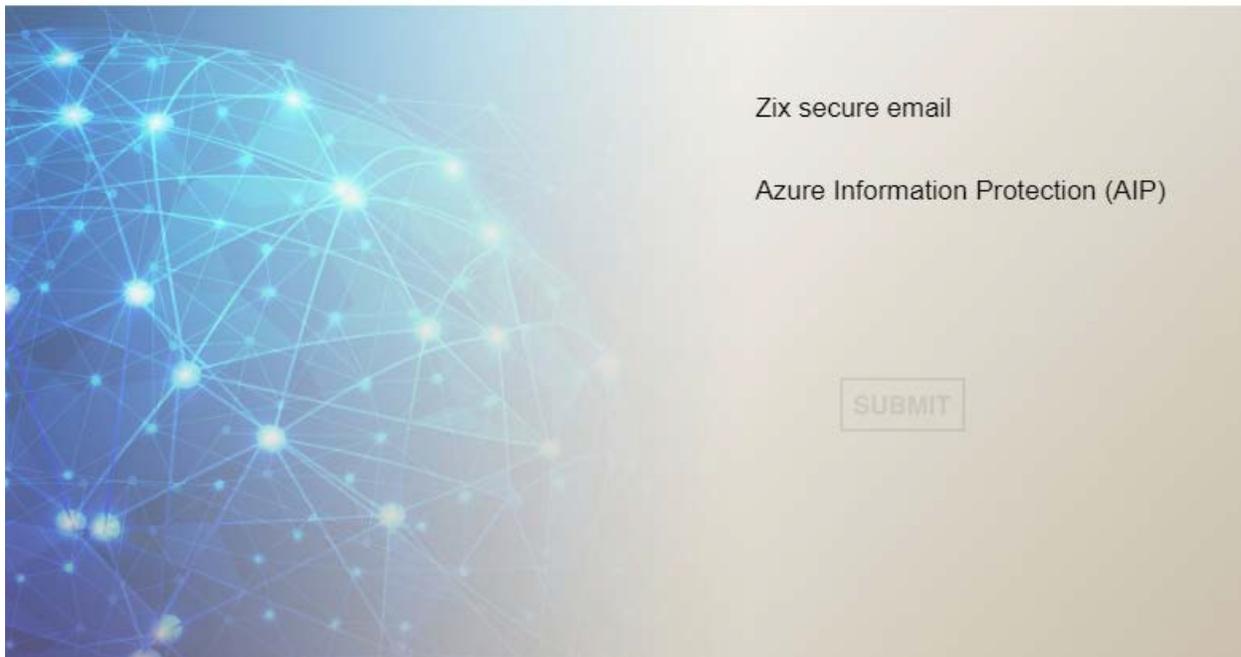
Feedback: That's correct. Good job! And by selecting "Encrypt-Restricted" you can ensure that sensitive email cannot be forwarded or printed by the recipient.

Feedback: That's correct. Good job! And by selecting "Encrypt-Restricted" you can ensure that sensitive email cannot be forwarded or printed by the recipient.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Which is the most appropriate tool to use for collaborating via email with another Federal regulator?



Zix secure email

Azure Information Protection (AIP)

SUBMIT

Which is the most appropriate tool to use for collaborating via email with another Federal regulator?

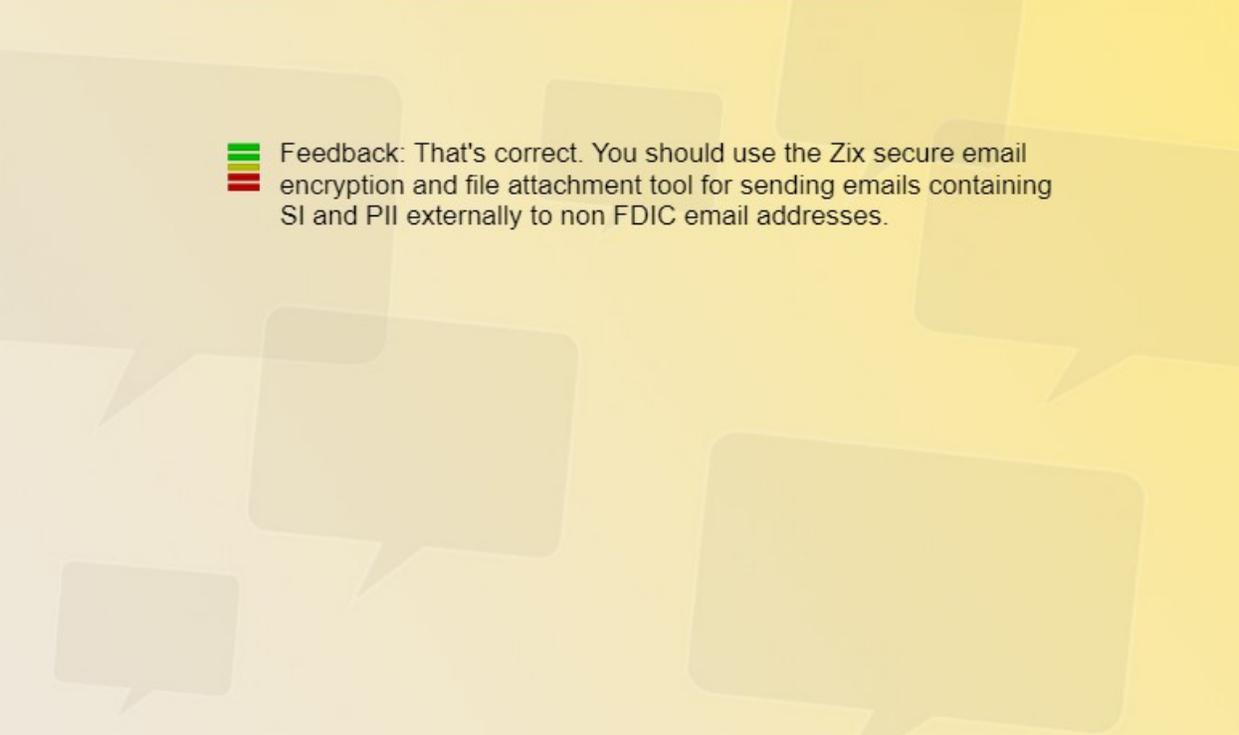
- Zix secure email
- Azure Information Protection (AIP)

Zix secure email is selected

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

 Feedback: That's correct. You should use the Zix secure email encryption and file attachment tool for sending emails containing SI and PII externally to non FDIC email addresses.



Feedback: That's correct. You should use the Zix secure email encryption and file attachment tool for sending emails containing SI and PII externally to non FDIC email addresses.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Malicious Software and Viruses

Symptoms to look for:

- Does your computer demonstrate reduced responsiveness or sudden loss of power?
- Is there unusual activity on the hard drive?
- Does your computer crash frequently?
- Has your antivirus software been disabled?
- Do others report receiving unusual messages from you?

Malicious Software and Viruses

There are several symptoms to look for to determine if your computer is infected with malicious software or a virus. Symptoms to look for:

- Does your computer demonstrate reduced responsiveness or sudden loss of power?
- Is there unusual activity on the hard drive?
- Does your computer crash frequently?
- Has your antivirus software been disabled?
- Do others report receiving unusual messages from you?

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Malicious Software and Viruses

Steps to follow if you suspect an infection:

1. Stop working on your computer.
2. Do NOT turn off your computer or unplug it.
3. Do nothing that will change the current operating status of your computer.
4. Call CSIRT immediately at 877-791-3377 or email fdic-csirt@fdic.gov

Malicious Software and Viruses

Steps to follow if you suspect an infection:

1. Stop working on your computer.
2. Do NOT turn off your computer or unplug it.
3. Do nothing that will change the current operating status of your computer.
4. Call CSIRT immediately at 877-791-3377 or email fdic-csirt@fdic.gov.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Security of FDIC's Network

Click on each item to learn more.

Wireless Restrictions

Wireless networks: Although the use of public Hotspots and Wi-Fi is acceptable, the FDIC encourages authorized users to connect to the FDIC network through FDIC-issued equipment and services, or from a personally-owned device through the designated FDIC Remote Access systems.

Software Limitations

Software installations: You are not permitted to install software on network computers unless it has been approved by DIT and appears in "FDIC Software Portal." You may not download or install software programs from the Internet that are not approved by the FDIC. This limitation applies to peer-to-peer (P2P), instant messaging (IM), and groupware programs.

Security of FDIC's Network**Wireless Restrictions**

Wireless networks: Although the use of public Hotspots and Wi-Fi is acceptable, the FDIC encourages authorized users to connect to the FDIC network through FDIC-issued equipment and services, or from a personally-owned device through the designated FDIC Remote Access systems.

Software Limitations

Software installations: You are not permitted to install software on network computers unless it has been approved by DIT and appears in "FDIC Software Portal." You may not download or install software programs from the Internet that are not approved by the FDIC. This limitation applies to peer-to-peer (P2P), instant messaging (IM), and groupware programs.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



Information Security Away from the Office

Whether you are on travel status or teleworking, it is important to take precautions to protect agency sensitive information, PII, and FDIC computer resources.

- Do not transport, or remove from the office, sensitive information without prior management approval.
- Protect all FDIC records and data against unauthorized disclosure, access, mutilation, and destruction.

Information Security Away from the Office

Whether you are on travel status or teleworking, it is important to take precautions to protect agency sensitive information, PII, and FDIC computer resources.

- Do not transport, or remove from the office, sensitive information without prior management approval.
- Protect all FDIC records and data against unauthorized disclosure, access, mutilation, and destruction.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



FDIC Telework Program

If you have been approved to telework, consider the security of your home environment.

- Always get management approval before removing agency sensitive information or PII from the workplace.
- Report any suspected loss or interception of data immediately.
- Misuse of the network or remote access privileges while teleworking can result in the compromise of identities, passwords, and agency sensitive or privacy data.

Click the button to review FDIC Telework Program Directive 2121.1.

[FDIC Telework Program Directive](#)

FDIC Telework Program

If you have been approved to telework, consider the security of your home environment.

- Always get management approval before removing agency sensitive information or PII from the workplace.
- Report any suspected loss or interception of data immediately.
- Misuse of the network or remote access privileges while teleworking can result in the compromise of identities, passwords, and agency sensitive or privacy data.

[FDIC Telework Program Directive](#)

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Wireless Network Safety

FDIC-provided equipment must be used to access or process FDIC information.

It is permissible to use a personally owned mobile device as a hotspot for your FDIC-furnished laptop or iPad.

Using the employee's personal cellular service provider is at the expense of the employee unless explicitly authorized by other FDIC policies.

Wireless Network Safety

FDIC-provided equipment must be used to access or process FDIC information. It is permissible to use a personally owned mobile device as a hotspot for your FDIC-furnished laptop or iPad. Using the employee's personal cellular service provider is at the expense of the employee unless explicitly authorized by other FDIC policies.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Wireless Devices

The FDIC provides IT resources for the purpose of conducting official business in support of the FDIC's mission.

Authorized users of FDIC IT services are required to use these resources consistent with applicable policies.

Sharing FDIC IT resources (iPad, laptops, iPhone, MiFi or iPhone/iPad hotspots) with friends or family is in violation of FDIC Directive 1300.4, Acceptable Use Policy for FDIC Information Technology. Doing so may subject an employee to disciplinary action.

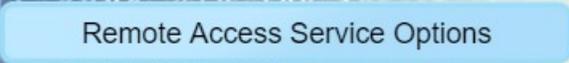
Wireless Devices

The FDIC provides IT resources for the purpose of conducting official business in support of the FDIC's mission. Authorized users of FDIC IT services are required to use these resources consistent with applicable policies.

Sharing FDIC IT resources (iPad, laptops, iPhone, MiFi or iPhone/iPad hotspots) with friends or family is in violation of FDIC Directive [1300.4, Acceptable Use Policy for FDIC Information Technology](#). Doing so may subject an employee to disciplinary action.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS



Remote Access

Remote access is available to authorized FDIC employees, contractors, and external entities with a valid need to access the FDIC network.

Remote access to the FDIC network should only be done for FDIC-related business and not compromise the security of FDIC systems or data.

FDIC employees and contractors are allowed to access limited corporate applications through non-FDIC IT devices.

Only FDIC-furnished IT equipment will have access to complete corporate network remotely.

Official FDIC business must only be conducted using FDIC-provided equipment. Remote users must comply with all FDIC policies and directives.

Employees and contractors must use FDIC furnished equipment/email accounts for transmitting and receiving FDIC information.

Click the button for a list of remote access options.

Remote Access

Remote access is available to authorized FDIC employees, contractors, and external entities with a valid need to access the FDIC network.

Remote access to the FDIC network should only be done for FDIC-related business and not compromise the security of FDIC systems or data.

FDIC employees and contractors are allowed to access limited corporate applications through non-FDIC IT devices.

Only FDIC-furnished IT equipment will have access to complete corporate network remotely.

Official FDIC business must only be conducted using FDIC-provided equipment. Remote users must comply with all FDIC policies and directives.

Employees and contractors must use FDIC furnished equipment/email accounts for transmitting and receiving FDIC information.

[Remote Access Service Options](#)

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Good Practices of Physical Security

Failing to follow good practices can lead to:

- **Accidental Loss** – Spilling food or drinks on a computer, or being careless with portable media can lead to permanent loss.
- **Theft** – Failing to take proper measures can lead to the theft of physical media or systems holding key data.
- **Accidental Disclosure** – Improperly transferring information because it was included in media or sending FDIC official business to a non-FDIC - issued device via email can compromise data and cause serious security and privacy situations.

**Good Practices of Physical Security**

While we have good security guards at entry points and fire suppression systems to help keep us safe, you are an important part of physical security at the FDIC. Using good practices for physical security allows you to minimize risks to security and privacy.

Failing to follow good practices can lead to:

Accidental Loss – Spilling food or drinks on a computer, or being careless with portable media can lead to permanent loss.

Theft – Failing to take proper measures can lead to the theft of physical media or systems holding key data.

Accidental Disclosure – Improperly transferring information because it was included in media or sending FDIC official business to a non-FDIC – issued device via email can compromise data and cause serious security and privacy situations.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

What if Equipment is Damaged, Lost, or Stolen?

The Computer Security Incident Response Team (CSIRT) operates 24 hours a day, seven days a week.

If your equipment has been damaged, lost, or stolen, contact CSIRT:

Call 877-FDIC-999
(877-334-2999) or *999

Email fdic-csirt@FDIC.gov

What if Equipment is Damaged, Lost, or Stolen?

In spite of our best efforts, equipment can be damaged, lost, or stolen. The Computer Security Incident Response Team (CSIRT) operates 24 hours a day, seven days a week to respond to computer threats.

If your equipment has been damaged, lost, or stolen, contact CSIRT:

- Call 877-FDIC-999
- (877-334-2999) or *999
- Email fdic-csirt@FDIC.gov

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Preparing to Ship Sensitive Information

Sensitive information must be shipped in accordance with FDIC Circular 3130.5.

Whenever sensitive information is shipped, it must be both secure and traceable.

Click the link for more information about Division of Administration's (DOA) Packaging Guidelines for Shipping Sensitive Information.

[Guidelines for Shipping Sensitive Information](#)



Preparing to Ship Sensitive Information

Shipping agency sensitive information or PII can present some special physical security challenges. Sensitive information must be shipped in accordance with FDIC Circular 3130.5 and the guidance contained in the FDIC Express Mail Job Aid.

Whenever sensitive information is shipped, it must be both secure and traceable. You must create a list of items containing sensitive information that will be included in the package, and maintain that list in a separate location in case of loss.

The list must contain sufficient details so that, if information were lost or misplaced, it could be reconstructed and other appropriate action can be taken.

Click the link for more information about Division of Administration's (DOA) Packaging Guidelines for Shipping Sensitive Information.

[Guidelines for Shipping Sensitive Information](#)

Conclusion

Conclusion

PROGRESS

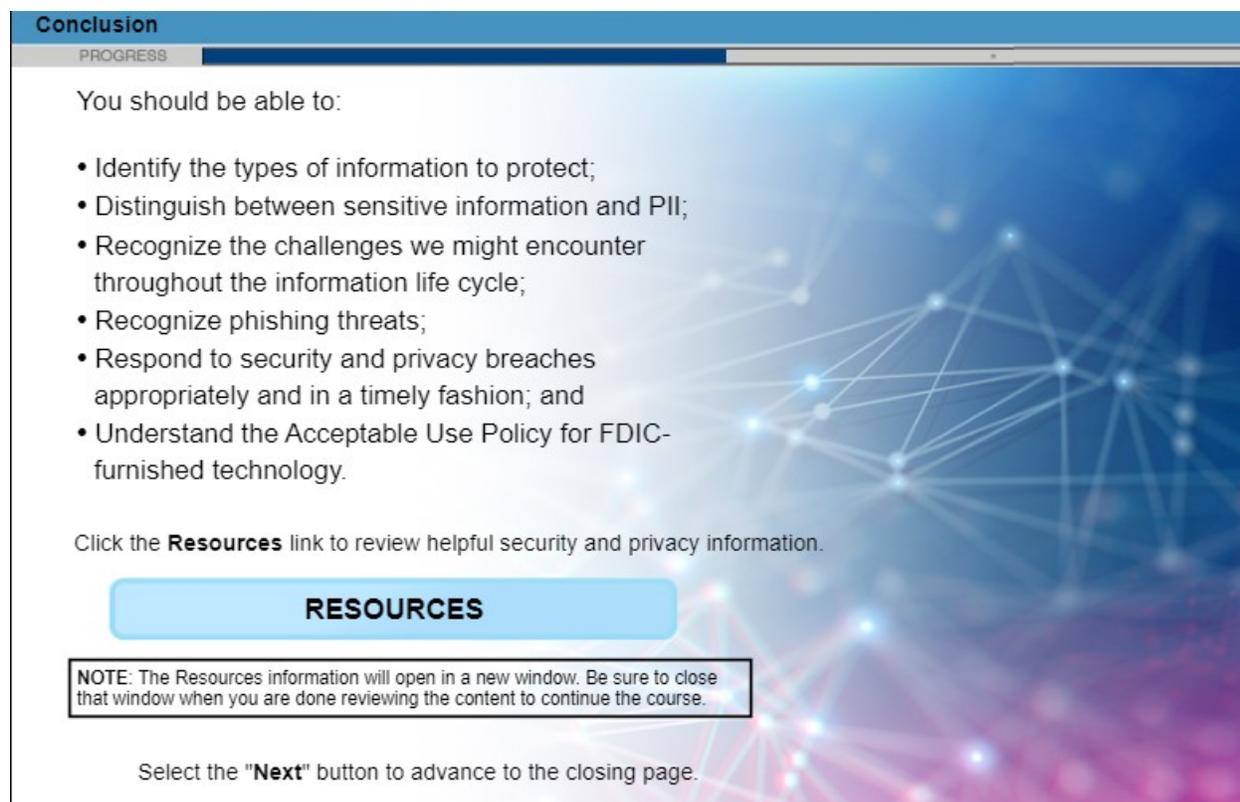
Depending on the circumstances, authorized users who violate the provisions of the Acceptable Use Policy may be subject to disciplinary action up to and including removal from federal service or from their contract.

Click on the button to review FDIC Directive 1300.4 - Acceptable Use Policy for FDIC Information Technology

Acceptable Use Policy for FDIC Information Technology

In spite of our best intentions, at times we fail to protect the FDIC network, applications, and data. Keep in mind that, depending on the circumstances, authorized users who violate the provisions of the Acceptable Use Policy may be subject to disciplinary action up to and including removal from federal service or from their contract.

Click on the button to review FDIC Directive [1300.4, Acceptable Use Policy for FDIC Information Technology](#).



Conclusion

PROGRESS

You should be able to:

- Identify the types of information to protect;
- Distinguish between sensitive information and PII;
- Recognize the challenges we might encounter throughout the information life cycle;
- Recognize phishing threats;
- Respond to security and privacy breaches appropriately and in a timely fashion; and
- Understand the Acceptable Use Policy for FDIC-furnished technology.

Click the **Resources** link to review helpful security and privacy information.

RESOURCES

NOTE: The Resources information will open in a new window. Be sure to close that window when you are done reviewing the content to continue the course.

Select the "**Next**" button to advance to the closing page.

As you just learned, the protection of the FDIC network and data, including sensitive information and PII, is everyone's responsibility. Remember that you are the key to security!

Now that you have completed this course, you should be able to:

- Identify the types of information to protect;
- Distinguish between sensitive information and PII;
- Recognize the challenges we might encounter throughout the information life cycle;
- Recognize phishing threats;
- Respond to security and privacy breaches appropriately and in a timely fashion; and
- Understand the Acceptable Use Policy for FDIC-furnished technology.

Click the [Resources](#) link to review helpful security and privacy information.

Conclusion

PROGRESS

Information Security and Privacy Awareness User Agreement

By checking this box, I understand and agree to comply with the rules of behavior as described in this training, and acknowledge that I am responsible for adhering to FDIC Directive 1300.4, Acceptable Use Policy for Information Technology. I also understand that authorized users who violate the provisions of FDIC Directive 1300.4 may be subject to disciplinary action up to and including removal from federal service or from their contract.

Information Security and Privacy Awareness User Agreement

By checking this box, I understand and agree to comply with the rules of behavior as described in this training, and acknowledge that I am responsible for adhering to FDIC Directive [1300.4, Acceptable Use Policy for Information Technology](#). I also understand that authorized users who violate the provisions of FDIC Directive 1300.4 may be subject to disciplinary action up to and including removal from federal service or from their contract.

Conclusion

PROGRESS

Congratulations!

You have completed this course.

Click **DONE** to exit the course. Your transcript in FDICLearn will reflect your completion of this course.



DONE

Congratulations!

You have completed this course.

Click "DONE" to exit the course. Your transcript in FDICLearn will reflect your completion of this course.

Thank you for participation and attention to this important information.