

INTRODUCTION



FDIC Corporate University

Play Help Resources Transcript Exit Menu Back Next

Introduction

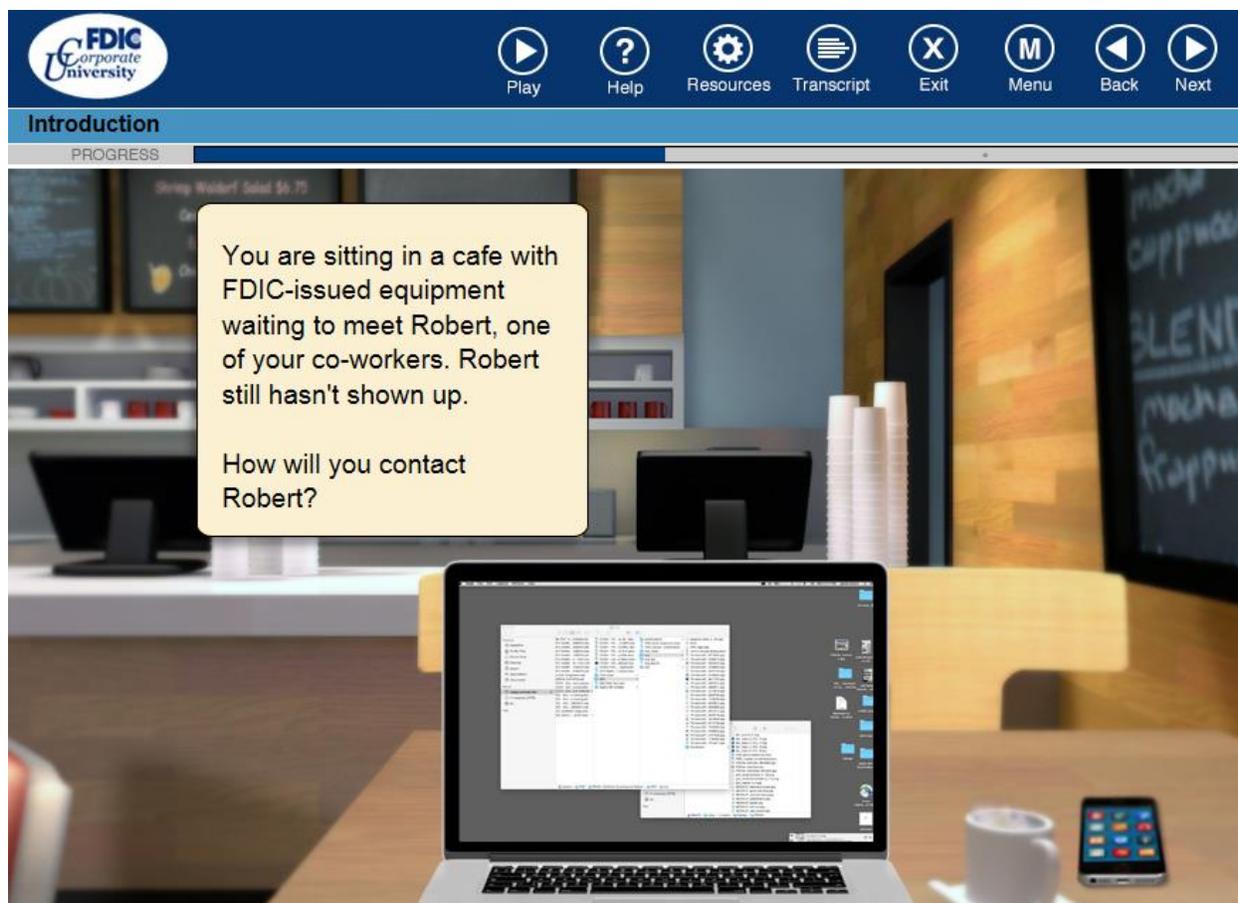
PROGRESS

Information Security and Privacy Awareness Course

We'll discuss:

- Collection
- Use
- Sharing
- Protection

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). You will learn how to maintain the confidentiality and integrity of the FDIC's network, systems, software, and data.



Before we begin, let's find out how you would handle the following scenario.

You are sitting in a cafe with your FDIC-issued equipment waiting to meet Robert, one of your co-workers. You like meeting at this venue because it offers large tables, plenty of coffee options, and available wi-fi. Robert still hasn't shown up. What is your best option to contact Robert?



Adhering to FDIC's standards for acceptable use of information technology, resources, and security can be challenging.

The FDIC takes information security and privacy seriously.

This training is intended to help you understand and comply with policies and practices.

You should be able to:

- Identify the types of information to protect
- Recognize the challenges and methods for protecting sensitive information
- Prevent and respond appropriately to privacy and security breaches

Actually, none of the options are correct. Adhering to FDIC's standards for acceptable use of information technology, resources, and security can be challenging. The FDIC takes information security and privacy seriously. This mandatory training is intended to help you understand and comply with policies and practices governing the protection and use of Sensitive Information (SI), including agency and business sensitive information and PII. This course will also help you maintain the confidentiality and integrity of the FDIC's network, systems, software, and data. By the end of the course you should also be able to:

- Identify the types of information to protect
- Recognize the challenges and methods for protecting sensitive information
- Prevent and respond appropriately to privacy and security breaches

LESSON 1:

TYPES OF INFORMATION WE ARE PROTECTING

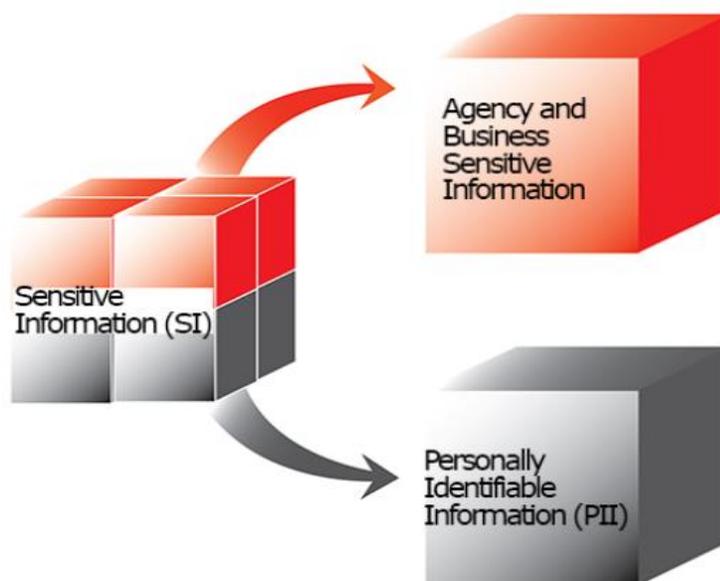
FDIC Corporate University

Play Help Resources Transcript Exit Menu Back Next

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 information:

- Agency and Business sensitive information; and
- Personally Identifiable Information (PII)

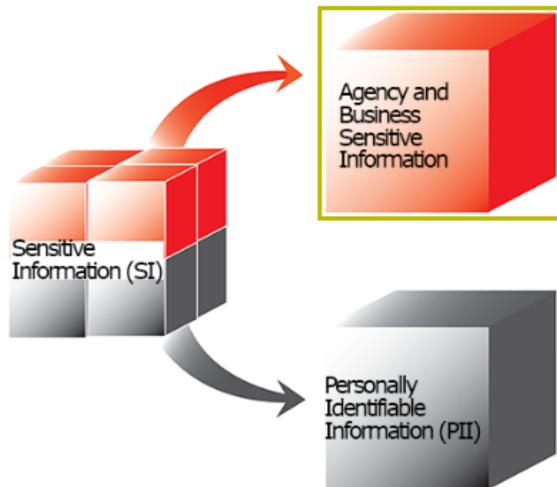
Let's take a closer look at each type of information.



Play
Help
Resources
Transcript
Exit
Menu
Back
Next

Lesson 1: Types of information we are protecting

PROGRESS



Agency and Business Sensitive Information

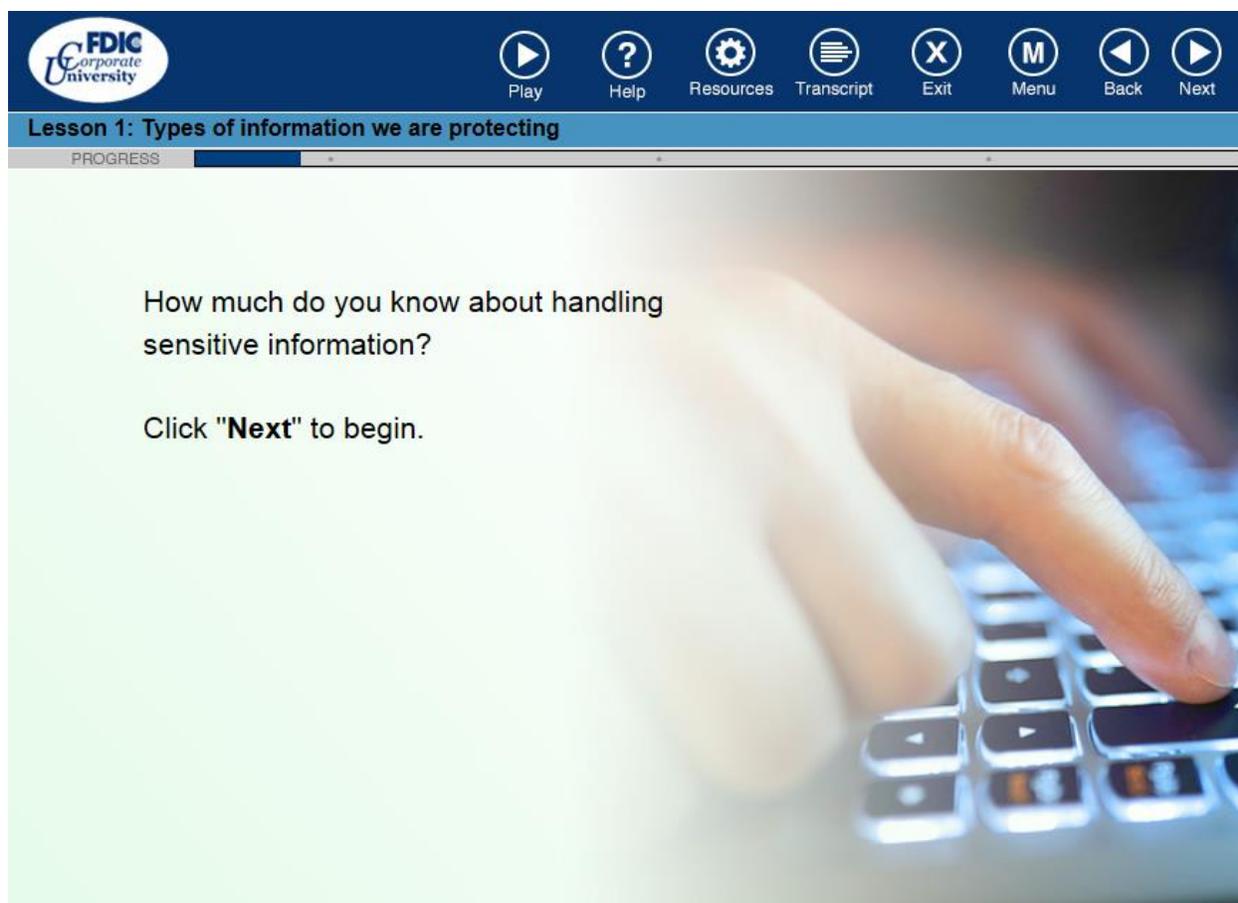
Examples of agency sensitive information include:

- 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
- Information related to FDIC's network or information technology that could be misused by malicious

....

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. Some 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.
- Information related to 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 FDIC).



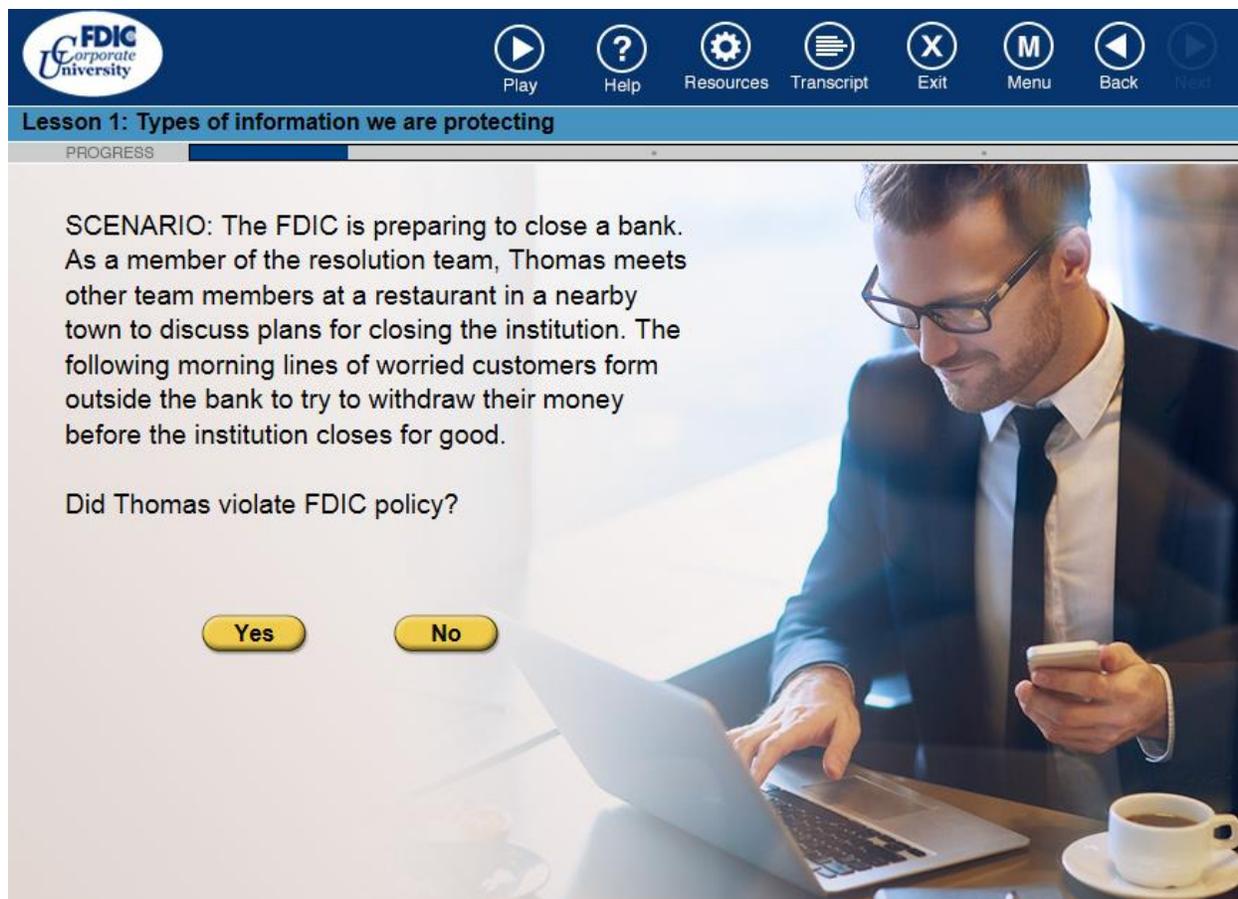
The screenshot shows a user interface for a learning module. At the top left is the logo for FDIC Corporate University. To the right of the logo is a navigation bar with icons for Play, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below the navigation bar is a blue header with the text "Lesson 1: Types of information we are protecting". Underneath the header is a progress bar labeled "PROGRESS". The main content area has a light green background and contains the following text:

How much do you know about handling sensitive information?

Click "**Next**" to begin.

The background of the main content area is a blurred image of a hand typing on a laptop keyboard.

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



FDIC
Corporate
University

Play Help Resources Transcript Exit Menu Back Next

Lesson 1: Types of information we are protecting

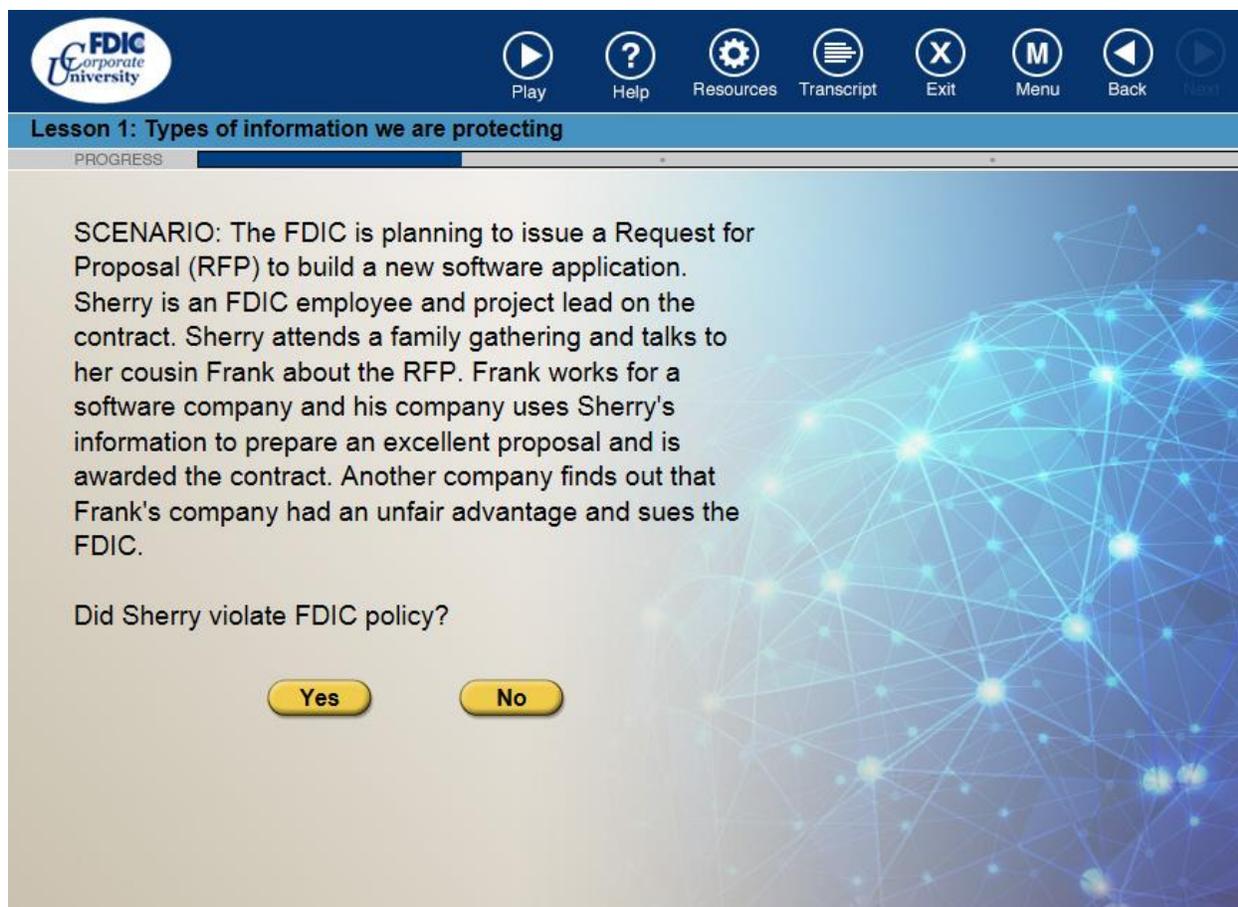
PROGRESS

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

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?



FDIC
Corporate
University

Play Help Resources Transcript Exit Menu Back Next

Lesson 1: Types of information we are protecting

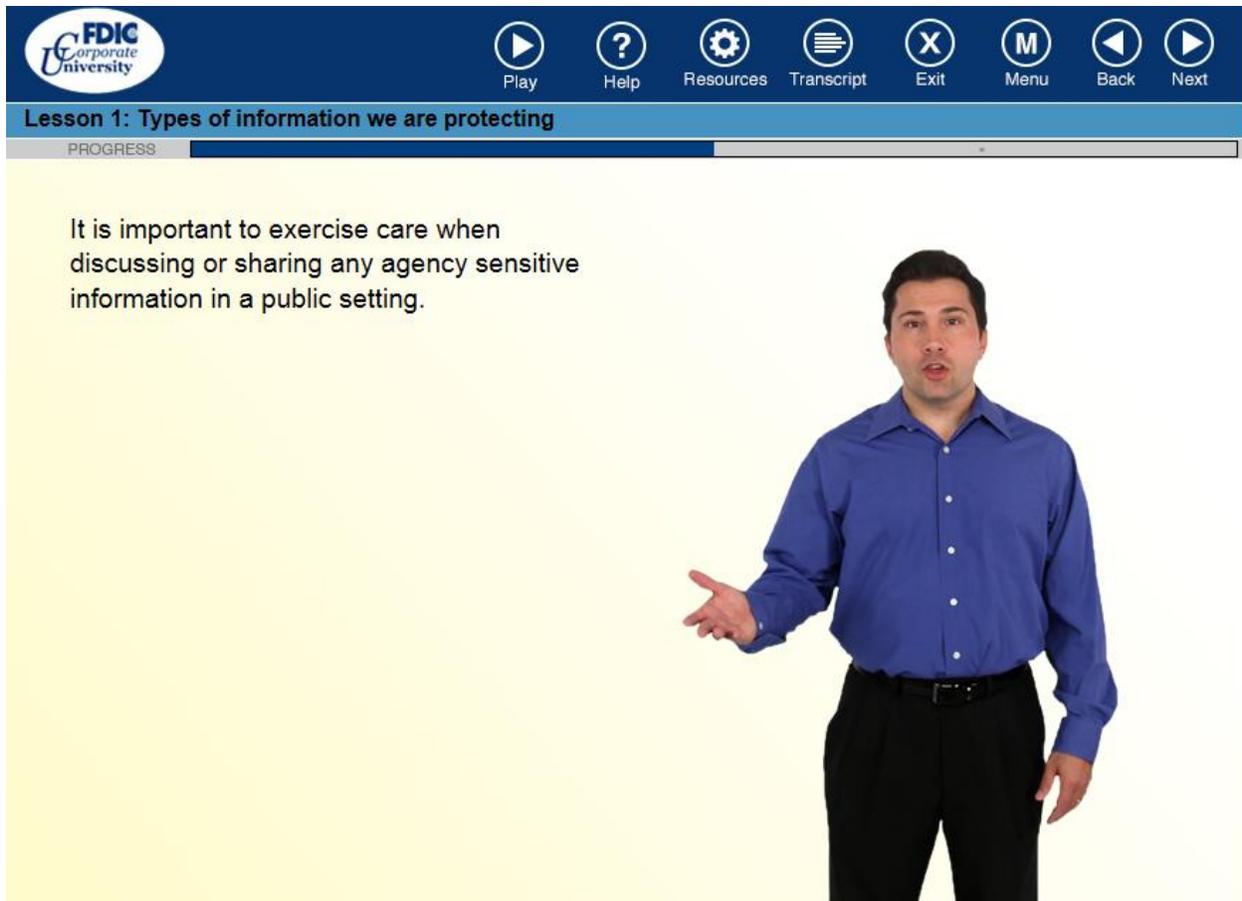
PROGRESS

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

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?



FDIC
Corporate
University

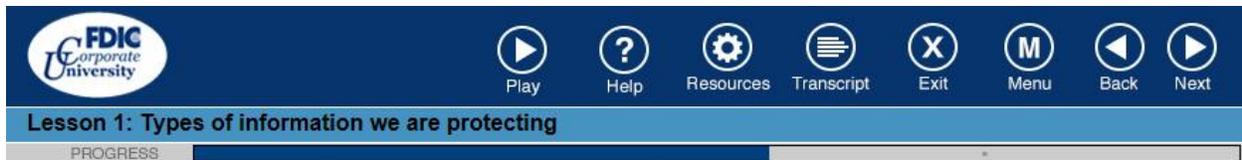
Play Help Resources Transcript Exit Menu Back Next

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

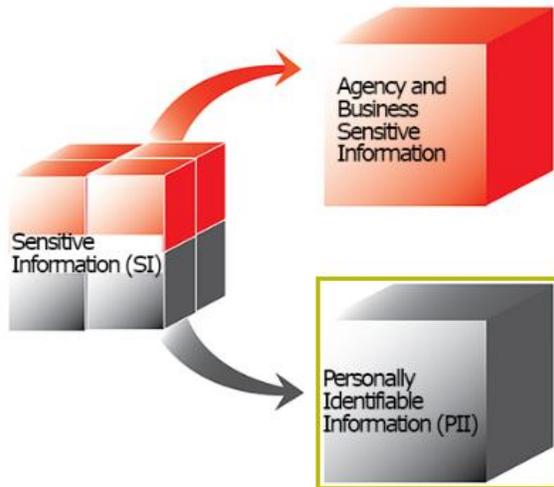


FDIC Corporate University

Play Help Resources Transcript Exit Menu Back Next

Lesson 1: Types of information we are protecting

PROGRESS



Personally Identifiable Information (PII)

Examples of PII include:

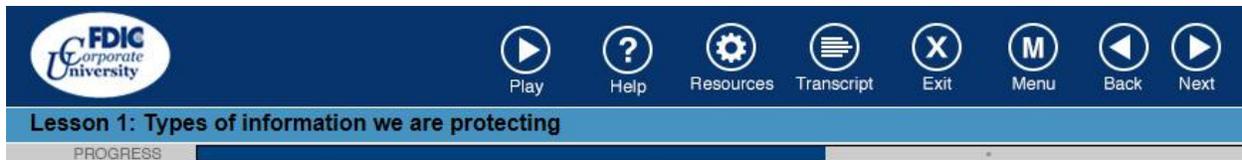
- Full Names
- Home Addresses
- Telephone Numbers (Non-work)
- Email Addresses (Non-work)
- Financial Information

Sensitive PII (SPII) is a subset of PII:

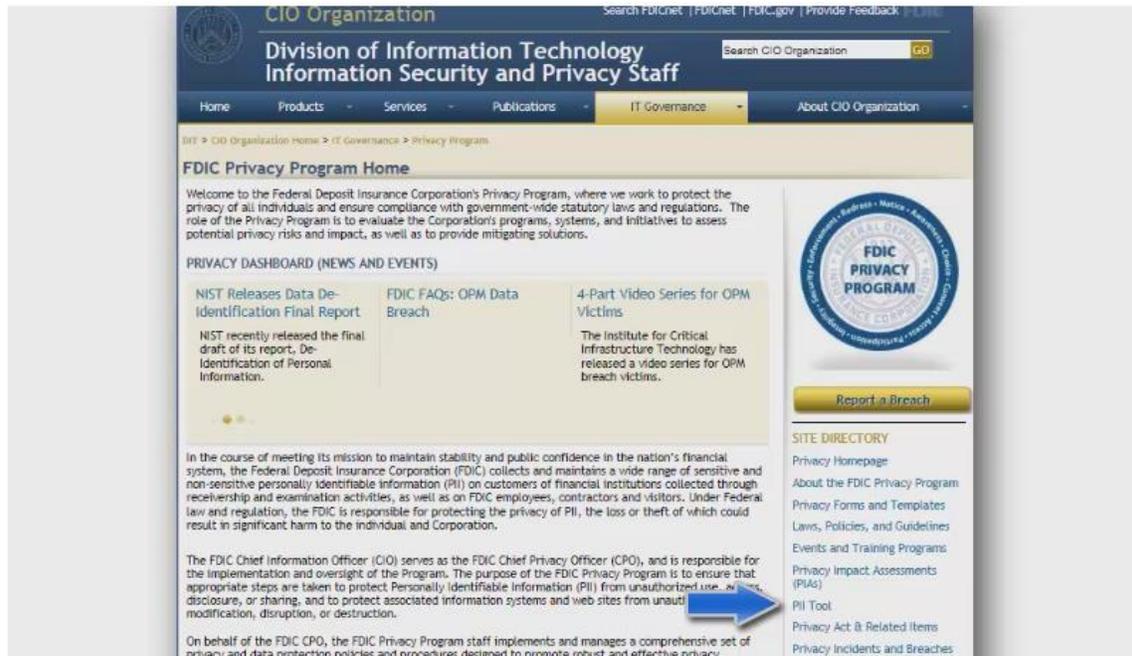
- It may be a single item
- Or a combination of data elements such as full name with a credit card number or a financial institution account

The second type of information that requires additional care is Personally Identifiable Information (PII). Examples of PII include names, home addresses, home telephone numbers, financial information, and other personal data of FDIC employees, contractors, and visitors, as well as bank customer information.

Sensitive PII (SPII) is a subset of PII which if lost compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. SPII may be a single item of information, such as a Social Security Number (SSN), or a combination of data items such as full name with a credit card number or a financial institution account. Since a breach of SPII could be used to commit identity theft or other serious harm, it requires the highest level of protection.



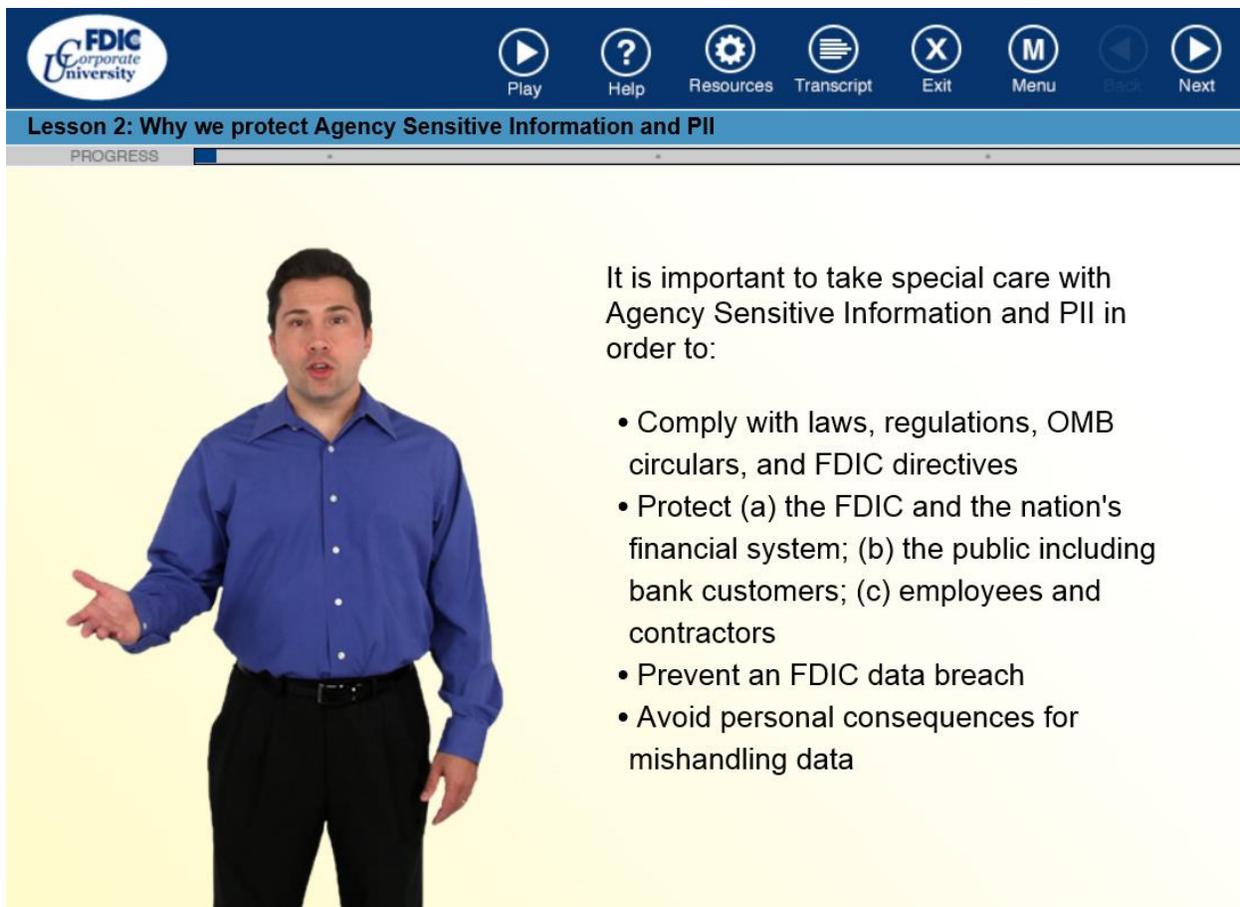
FDIC PII Verification Tool



The FDIC PII verification tool is available to help you determine whether you are handling or maintaining PII and/or Sensitive PII (SPII). Check boxes appear beside PII items. In this example, if you want to determine whether you are handling or maintaining PII and/or SPII of an investigation report for an FDIC employee, you would select "Full Name," "Investigation Report or Database," and "Criminal History or Information." According to the PII tool, this information is considered SPII.

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:

- Comply with laws, regulations, OMB circulars, and FDIC directives
- Protect (a) the FDIC and the nation's financial system; (b) the public including bank customers; (c) employees and contractors
- Prevent an FDIC data breach
- 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 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 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.

- | | |
|---|---|
|  The Privacy Act of 1974 | <p>The Privacy Act requires the FDIC to protect certain records containing PII (both electronic and in paper) and provide individuals with special privacy rights.</p> |
|  E-Government Act of 2002 | <p>The E-Government Act requires FDIC to address information technology (IT) training, IT security, and the protection of personal privacy.</p> |
|  Freedom of Information Act (FOIA) | <p>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.</p> |
|  OMB Circulars | <p>The OMB provides the FDIC with policy and guidance to manage and protect information resources.</p> |

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, as amended
- E-Government Act of 2002
- Freedom of Information Act (FOIA)
- OMB Circulars

Click on each button to learn more.



Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

https://fdicnet.fdic.gov/content/dit/home.html

View Favorites Tools Help

CIO Organization Search FDICnet | FDICnet | FDIC.gov | Provide Feedback FDIC

Division of Information Technology Information Security and Privacy Staff Search CIO Organization GO

Home Products Services Publications IT Governance About CIO Organization

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
- FDIC computer systems and networks

You should familiarize yourself with the information in FDIC Circular 1360.9, Protecting Sensitive Information.

[Click to visit the CIOO Website](#)

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 Chief Information Officer Organization (CIOO)'s 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.



Play Help Resources Transcript Exit Menu Back Next

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



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 or 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.

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. Click each button to learn more.



Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

3. Prevent an FDIC data breach

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](#)

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.



Play Help Resources Transcript Exit Menu Back Next

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Click the "Back" button to return to the previous screen.

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.

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 for these violations 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

Click the "Back" button to return to the previous screen.

Security Violations

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

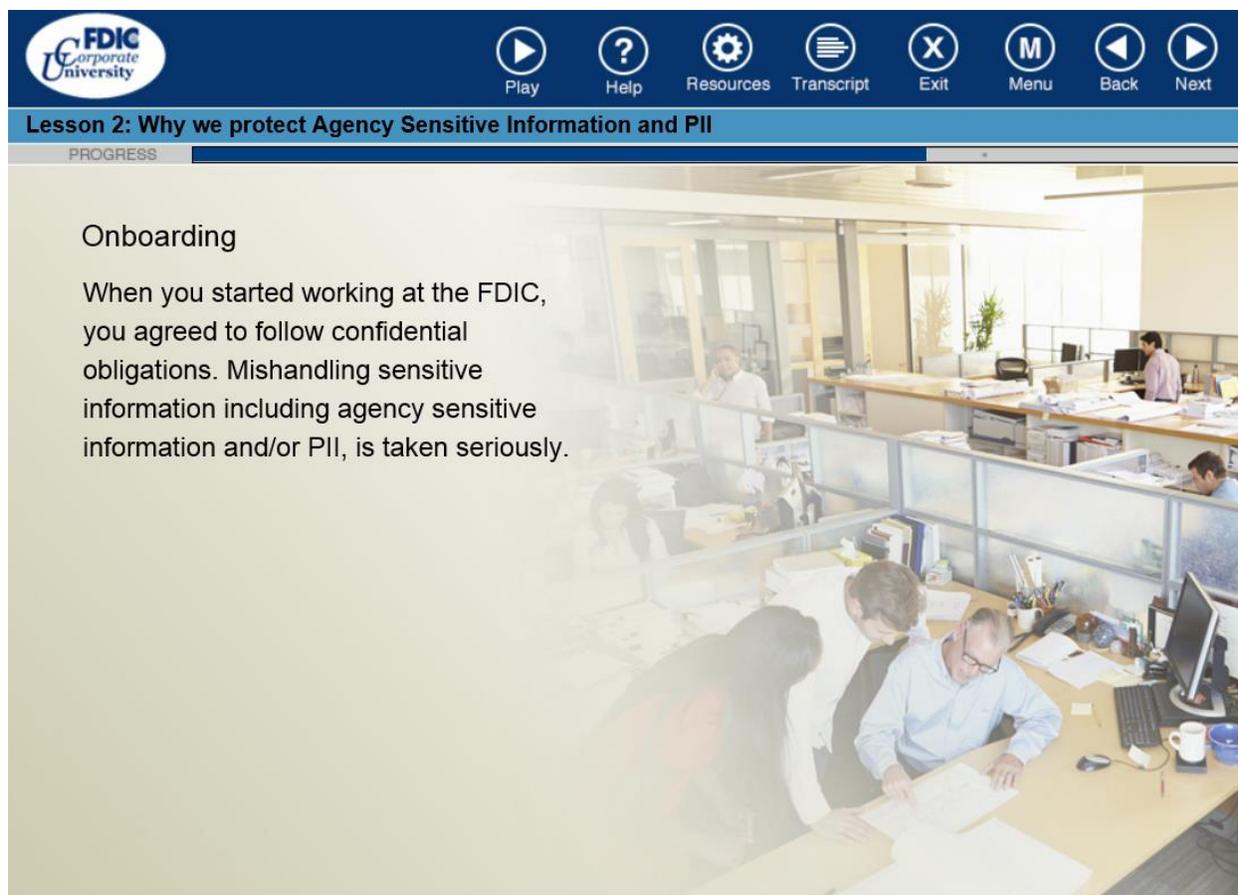
Security regulations and guidelines define penalties for activities that may include the following:

- 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 whether on network or portable media.
- 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.

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

Security regulations and guidelines define penalties for activities that may include the following:

- 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 whether on network or portable media.
- 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.



FDIC
Corporate
University

Play Help Resources Transcript Exit Menu Back Next

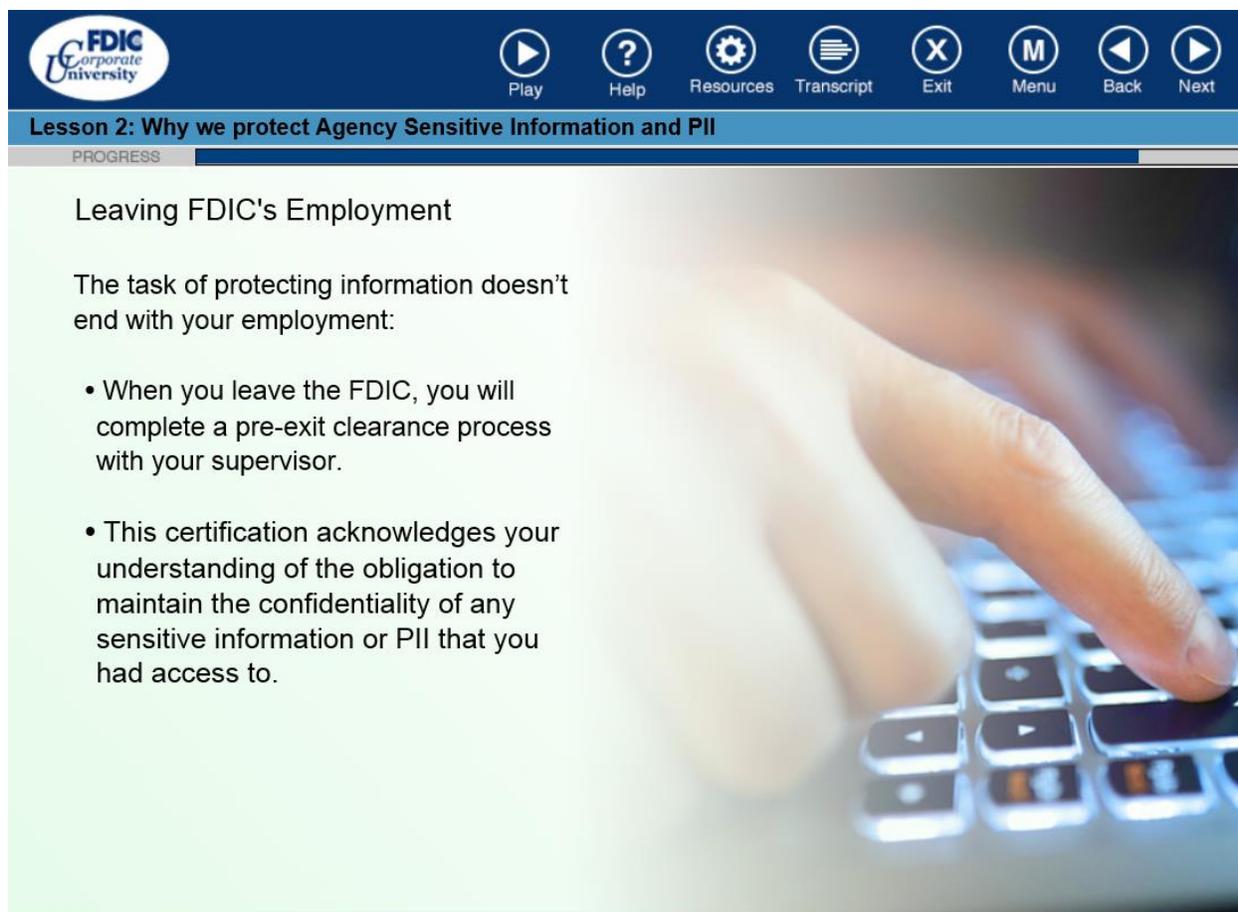
Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS

Onboarding

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

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



FDIC
Corporate University

Play Help Resources Transcript Exit Menu Back Next

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:

- When you leave the FDIC, you will complete a pre-exit clearance process with your supervisor.
- This certification acknowledges your understanding of the obligation to maintain the confidentiality of any sensitive information or PII that you had access to.

The task of protecting information doesn't end with your employment. When you leave the FDIC, you will complete a pre-exit clearance process with your supervisor or oversight manager. This certification acknowledges your understanding of the obligation to return and maintain the confidentiality of any sensitive information, including agency sensitive information and PII, that you had access to during your employment with the FDIC.



Play Help Resources Transcript Exit Menu Back Next

Lesson 2: Why we protect Agency Sensitive Information and PII

PROGRESS



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

Protecting Agency Sensitive 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 can have serious negative consequences for individuals, the FDIC, and you.

LESSON 3:

CHALLENGES PROTECTING

AGENCY SENSITIVE INFORMATION

AND PII.



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

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 lifecycle. Select Next to begin.



FDIC
Corporate
University

Pause Help Resources Transcript Exit Menu Back Next

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 protection of information throughout its life cycle, from its initial collection to its ultimate disposal or destruction.

LESSON 4:
PROTECTING INFORMATION
THROUGHOUT THE LIFECYCLE



Pause Help Resources Transcript Exit Menu Back Next

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

This lesson reviews phases throughout the information lifecycle.

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



Protecting data can be challenging. It is important to know how to protect information throughout the entire lifecycle - 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 lifecycle phases, talk with your supervisor, your division ISM or contact FDIC's Privacy Program at privacy@fdic.gov.

The screenshot shows a presentation slide with a dark blue header. On the left is the FDIC Corporate University logo. On the right are navigation icons: Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below the header is a light blue bar with the text 'Lesson 4: Protecting information throughout the lifecycle' and a progress indicator. The main content area has a light yellow background with a large, faint graphic of a document lifecycle showing 'Collection and Creation', 'Storage', and 'Disposal' stages. The text on the slide reads:

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
- If the collection is paper-based or web-based
- Whether the collection of information requires a new or modified Privacy Act of System Records Notice

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;
- If the collection is paper-based or web-based; and
- Whether the collection of information requires a new or modified Privacy Act System of 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, your division or office's Information Security Manager (ISM) or contact FDIC's Privacy Program by emailing privacy@fdic.gov.

Click "Next" to review ISM listing

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 ISM or contact FDIC's Privacy Program by emailing privacy@fdic.gov.



 Pause
  Help
  Resources
  Transcript
  Exit
  Menu
  Back
  Next

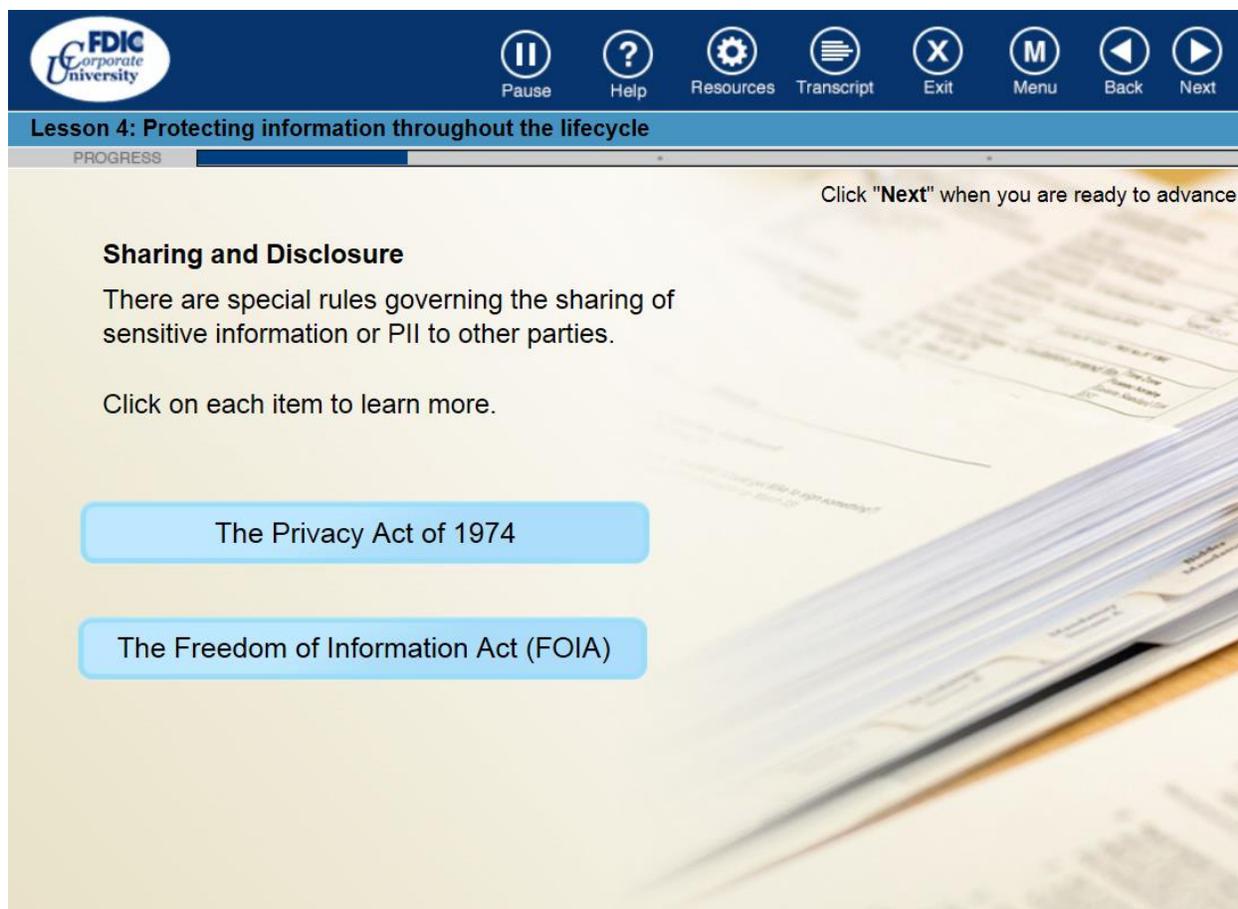
Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Division/Office	Name	Phone	Email
DIR	Jack Talbert	202-898-3547	JTalbert@fdic.gov
CIOO: DIT/DMB, DIT/ETB Executive Offices: CU, FFIEC, EO, OCOM, OCRM, OMWI, OLA, OO	John Mercado	703-516-1101	JoMercado@fdic.gov
CIOO: DIT/ISB, DIT/BAB, ISPS	Reem Nazzal-Hajeer	703-516-5733	RNazzalHajeer@fdic.gov
DOA	Kim Berger	703-562-2107	KBerger@fdic.gov
	Lynn VanHorn	703-516-5731	LVanHorn@fdic.gov
DOF, GAO	Anita Butler	703-562-6142	AButler@fdic.gov
DRR	Edward Collins	703-516-5765	EdCollins@fdic.gov
DCP	Dale Witherspoon	703-254-0352	DaWitherspo@fdic.gov
Legal	MaryBeth Dormuth	703-562-2355	MDormuth@fdic.gov
OCFI	Jack Talbert (Acting)	202-898-3547	JTalbert@fdic.gov
OIG	Philip Roman	703-562-6428	Proman@fdic.gov
RMS	Victoria Hill	703-254-0342	VHill@fdic.gov
	Barbara Strong	703-562-2876	BStrong@fdic.gov

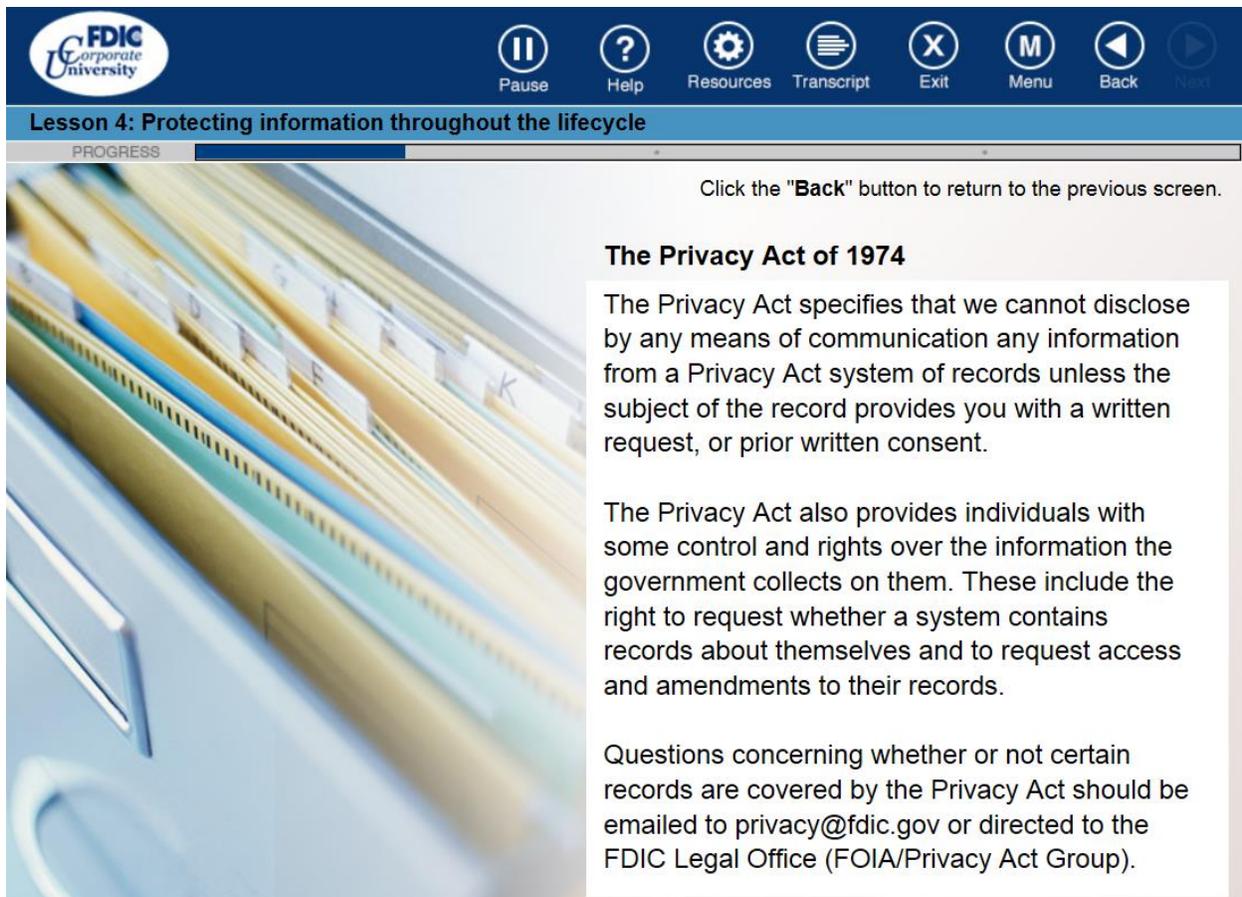
Click to review ISM list

Here is a list of ISMs for each Division and Office.



The screenshot shows a user interface for a learning module. At the top left is the FDIC Corporate University logo. To its right is a navigation bar with icons for Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below this is a blue header bar with the text "Lesson 4: Protecting information throughout the lifecycle". A progress bar is visible below the header. The main content area has a light beige background with a blurred image of a document. The text reads: "Click 'Next' when you are ready to advance." followed by the section title "Sharing and Disclosure". Below the title is the text: "There are special rules governing the sharing of sensitive information or PII to other parties." and "Click on each item to learn more." Two blue buttons are displayed: "The Privacy Act of 1974" and "The Freedom of Information Act (FOIA)".

There are special rules governing the sharing of sensitive information or PII to other parties.
Click on each item to learn more.



Click the "Back" button to return to the previous screen.

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.

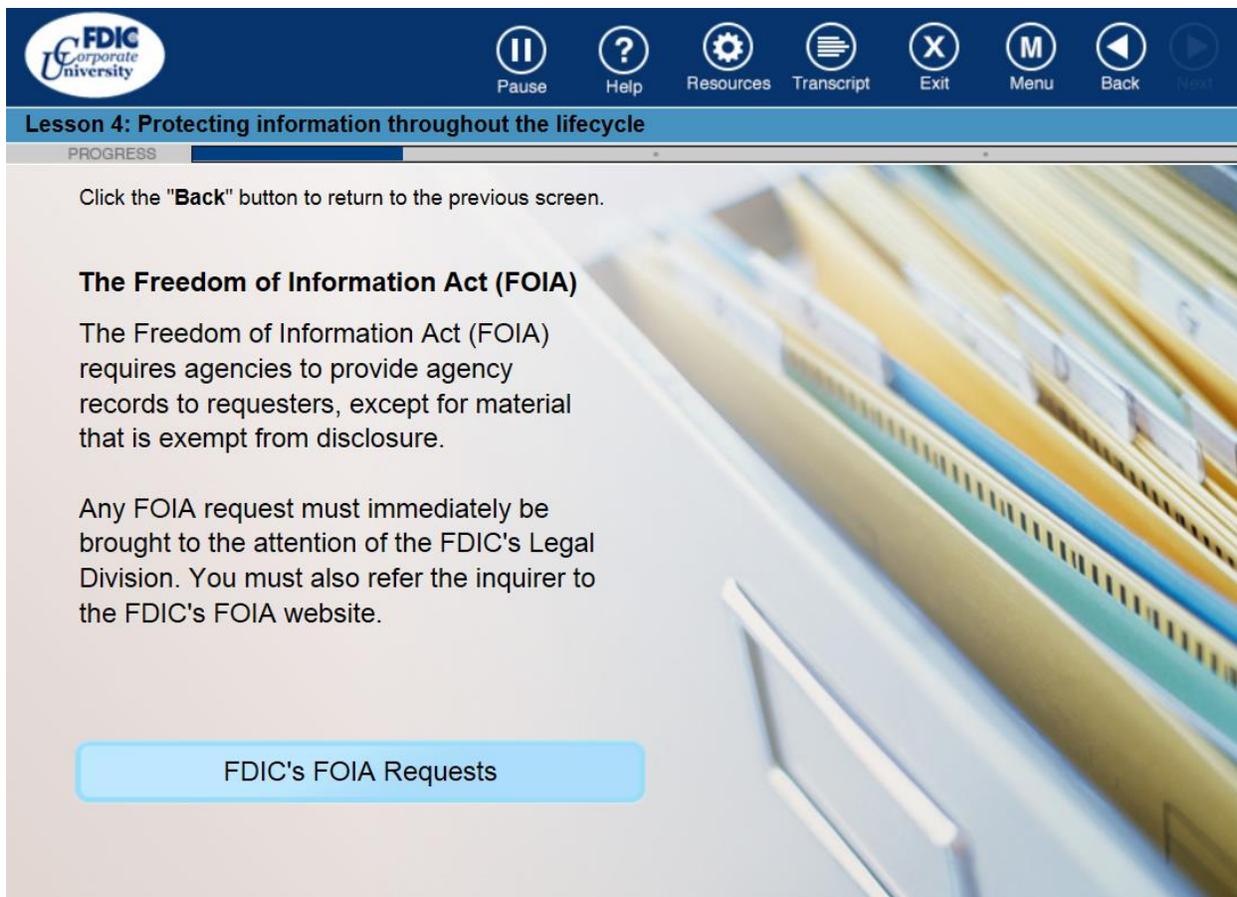
The Privacy Act also provides individuals with some control and rights over the information the government collects on them. These include the right to request whether a system contains records about themselves and to request access and amendments to their records.

Questions concerning whether or not 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 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 or not 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).



Click the **"Back"** button to return to the previous screen.

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](#)

FOIA requires agencies to provide agency records to requesters, except for material that is exempt from disclosure. The Legal Division can advise you regarding information that has been requested through FOIA and whether any of it is exempt.

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.

The screenshot shows a user interface for an e-learning module. At the top, there is a dark blue navigation bar with the FDIC Corporate University logo on the left and several icons for navigation: Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below the navigation bar is a light blue header for 'Lesson 4: Protecting information throughout the lifecycle'. A progress bar is visible below the header. The main content area has a light yellow background with a large, faint graphic of a computer keyboard. The 'Maintenance' key is highlighted in a darker shade. To the right of the 'Maintenance' key, there is a text box with the following content:

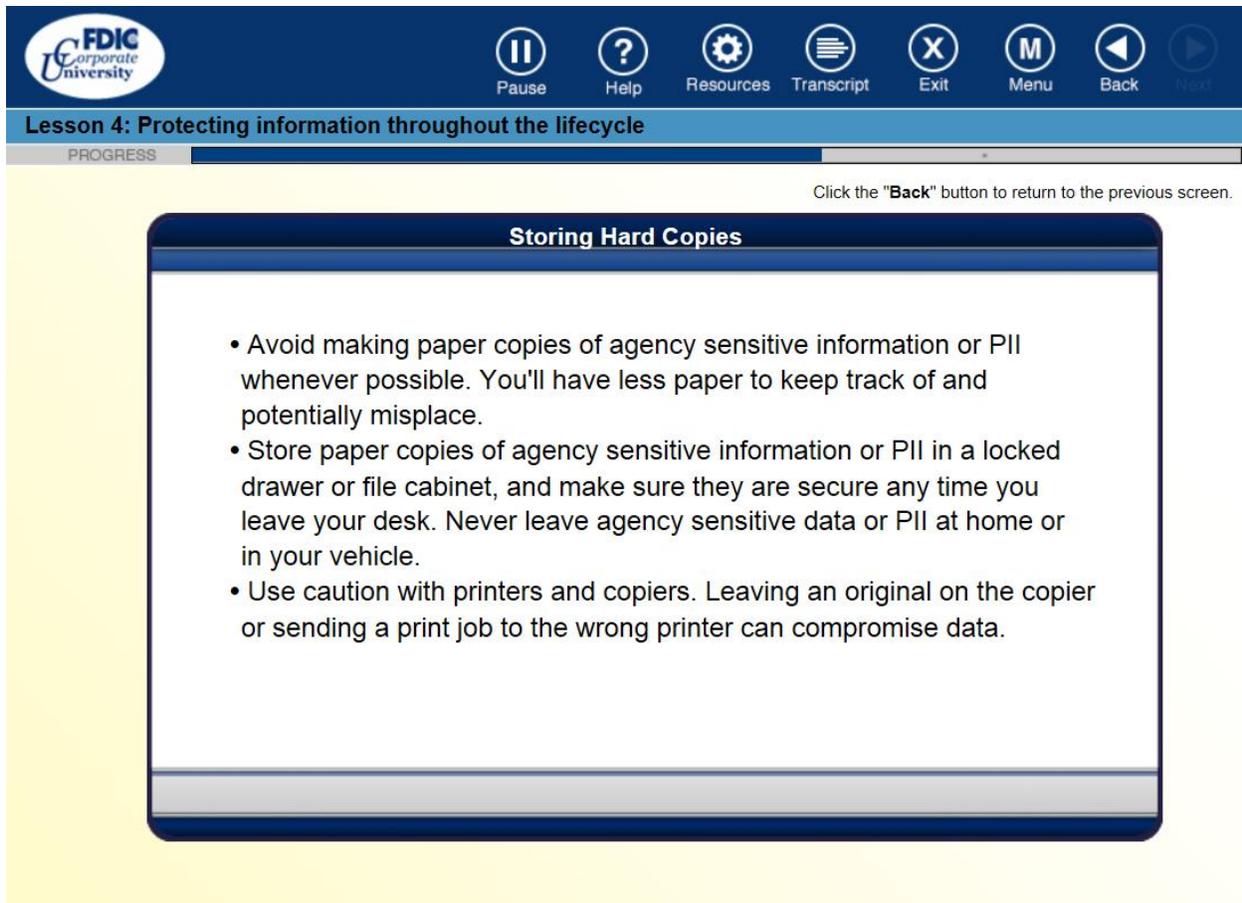
Maintenance
You have a responsibility to maintain current, accurate and relevant information, whether in electronic or paper form. For more information contact your division Records Liaison or visit the RIM website.

Below the text box is a blue button with the text 'Click to visit the RIM website'.

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.

The screenshot shows a training module interface. At the top, there is a dark blue header with the FDIC Corporate University logo on the left and a row of navigation icons: Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below the header is a light blue bar with the text "Lesson 4: Protecting information throughout the lifecycle". Underneath that is a progress bar labeled "PROGRESS" with a blue fill indicating the current position. The main content area has a light yellow background with a large, faint, 3D-style graphic of a folder labeled "Storage". Inside this graphic, there are two smaller boxes labeled "Paper copies" and "Electronic copies". To the right of the "Storage" graphic, the word "Storage" is written in a bold, black font. Below this heading, there is a paragraph of text: "You must properly secure information to help prevent accidental loss or dissemination. Click each button to learn more about storing both paper and electronic copies of information."

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



The screenshot shows a presentation interface. At the top left is the FDIC Corporate University logo. To its right is a navigation bar with icons for Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below this is a blue header for 'Lesson 4: Protecting information throughout the lifecycle' and a progress bar. The main content area is a slide titled 'Storing Hard Copies' with a list of three bullet points. Below the slide, a text instruction reads: 'Click the "Back" button to return to the previous screen.'

FDIC Corporate University

Pause Help Resources Transcript Exit Menu Back Next

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Click the "Back" button to return to the previous screen.

Storing Hard 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.
- Use caution with printers and copiers. Leaving an original on the copier or sending a print job to the wrong printer can compromise data.

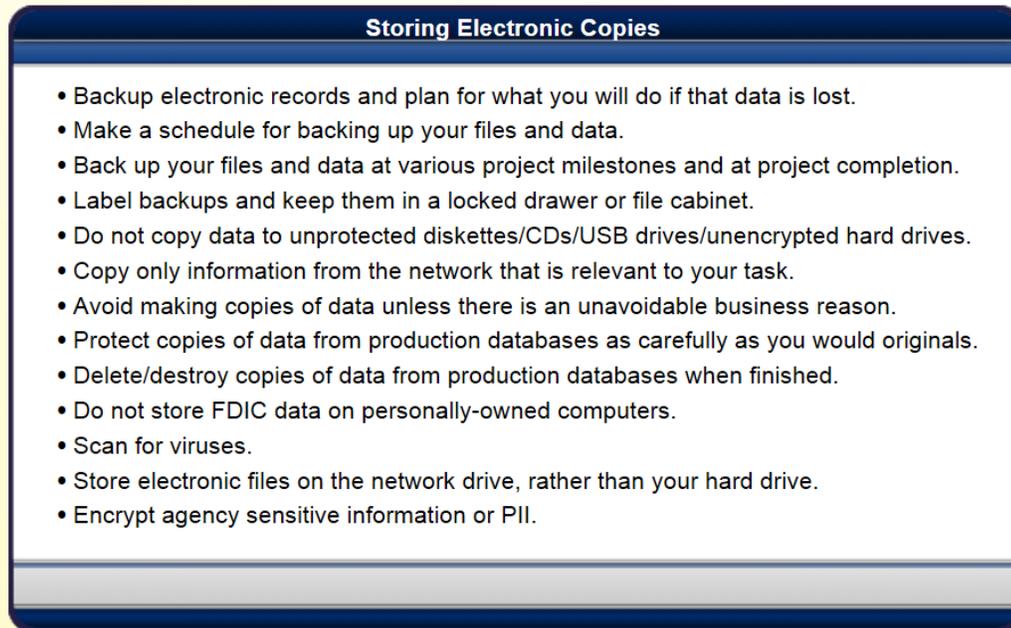
Storing Hard Copies

- 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.
- Use caution with printers and copiers. Leaving an original on the copier or sending a print job to the wrong printer can compromise data.



The screenshot shows a presentation interface. At the top left is the FDIC Corporate University logo. To its right is a navigation bar with icons for Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below the navigation bar is a blue header with the text 'Lesson 4: Protecting information throughout the lifecycle'. Underneath the header is a progress bar labeled 'PROGRESS'.

Click the "Back" button to return to the previous screen.



The screenshot shows a presentation slide with a blue header and a white body. The header contains the title 'Storing Electronic Copies'. The body contains a bulleted list of 14 items related to data backup and storage.

Storing Electronic Copies

- Backup electronic records and plan for what you will do if that data is lost.
- Make a schedule for backing up your files and data.
- Back up your files and data at various project milestones and at project completion.
- Label backups and keep them in a locked drawer or file cabinet.
- Do not copy data to unprotected diskettes, CDs, USB drives, or unencrypted hard drives.
- Copy only information from the network that is relevant to your task.
- Avoid making copies of data from a production database unless there is an unavoidable business reason.
- Protect copies of data from production databases as carefully as you would the originals.
- Delete or destroy copies of data from production databases as soon as you are finished with them.
- Do not store FDIC data on personally-owned computers.
- Scan for viruses.
- Store electronic files on the network drive, rather than your hard drive.
- 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. This includes your desktop computer's hard drive and portable storage media, such as USB flash drives, CDs, and DVDs. The FDIC restricts the ability to write data to removable media.

Click on the links below to review guidance on encryption and removable media protection.

[FDIC's Encryption Guidance](#)

[FAQs Removable Media Protection](#)

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.

As a general rule you should never store unencrypted sensitive information in an easily accessible place. This includes your desktop computer's hard drive and portable and removable storage media, such as USB flash drives, CDs, and DVDs. Click on the links below to review guidance on encryption and removable media protection.

Lesson 4: Protecting information throughout the lifecycle

PROGRESS

Disposal

You should reduce the amount of agency sensitive information or PII kept on hand. Information should be properly disposed of or destroyed when it is no longer needed. For further information visit DOA's RIM website.

Click to visit the RIM website

Reduce the amount of agency sensitive information or PII in your possession. Information should be properly disposed of or destroyed when it is no longer needed, or the mandatory timeframe for retention of records has passed.

For further information visit DOA's RIM website.

LESSON 5:

**RECOGNIZE HOW TO PROTECT
SENSITIVE INFORMATION AND PII.**



FDIC Corporate University

Pause Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

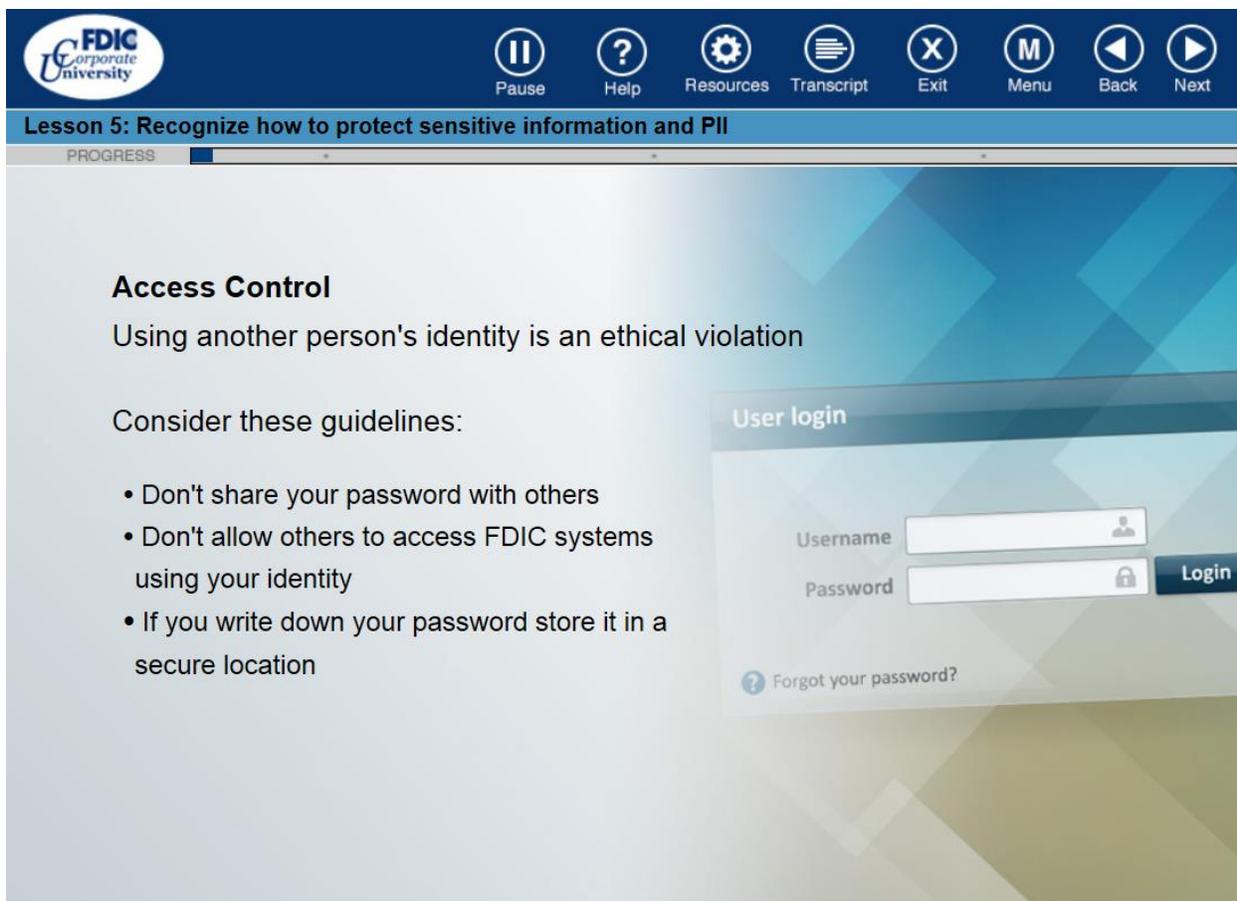
PROGRESS

INFORMATION SECURITY & PRIVACY

FDIC

YOU ARE THE KEY TO SECURITY.

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



FDIC Corporate University

Pause Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Access Control

Using another person's identity is an ethical violation

Consider these guidelines:

- Don't share your password with others
- Don't allow others to access FDIC systems using your identity
- If you write down your password store it in a secure location

User login

Username

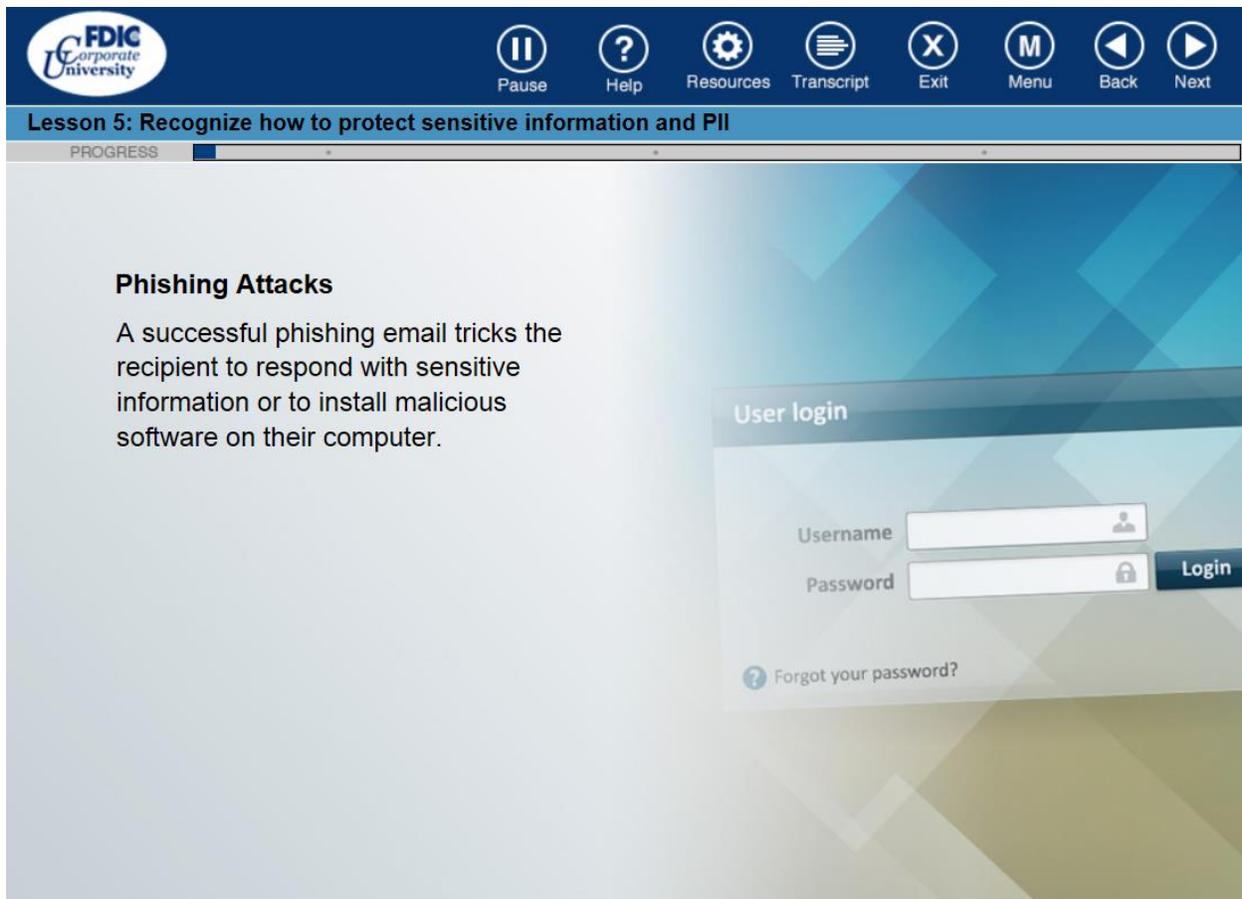
Password Login

[? Forgot your password?](#)

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

To help safeguard your data, consider these guidelines:

- Don't share your password with others.
- Don't allow others to access FDIC systems using your identity.
- If you write down your password store it in a secure location.



The screenshot shows a presentation slide with a dark blue header. On the left is the FDIC Corporate University logo. On the right are navigation icons: Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below the header is a blue bar with the text 'Lesson 5: Recognize how to protect sensitive information and PII'. A progress bar is visible below this. The main content area has a light blue background with a geometric pattern. On the left, the text reads: **Phishing Attacks**
A successful phishing email tricks the recipient to respond with sensitive information or to install malicious software on their computer. On the right, there is a semi-transparent image of a 'User login' form with fields for 'Username' and 'Password', a 'Login' button, and a 'Forgot your password?' link.

Phishing continues to be one of the most persistent security threats to organizations throughout the world. A successful phishing email tricks the recipient to respond with sensitive information or to install malicious software on their computer. In many instances a phishing email results in malicious software installed on the recipient's computer without the user's knowledge. This malicious software could allow the attacker to access sensitive information from the network, and may result in a data breach.

The screenshot shows a lesson interface for "Lesson 5: Recognize how to protect sensitive information and PII". The interface includes a navigation bar with icons for Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below the navigation bar is a progress bar. The main content is a simulated email client window. The email is from "administrator@fdic.gov" with a secondary address "<administrator@rastrear-perdidos.mx>". A green arrow points to the second address with the text "Is the sender's address unfamiliar?". The email subject is "Unauthorized Access" and it has an attachment named "jobaid.exe". The email body contains a warning about restricted website access and a link to "Web Security Logs".

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

- Is the sender's address unfamiliar?
- 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 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 organization you do not know?

FDIC
Corporate
University

Pause Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Phishing Scenarios Exercise

You will see a series of emails.

Some are real and some are considered phishing emails. It's up to you to recognize them.

You will have only 20 seconds to review each email and make your decision.

Select **"Next"** to begin.

Login

Now you will see a series of emails. Some are real and some are considered phishing emails. It's up to you to recognize them. You will have only 20 seconds to review each email and make your decision. Select "Next" to begin.



The screenshot shows a presentation interface for FDIC Corporate University. At the top, there is a navigation bar with icons for Pause, Help, Resources, Transcript, Exit, Menu, Back, and Next. Below this is a title bar for 'Lesson 5: Recognize how to protect sensitive information and PII' and a progress indicator. The main content area features a blue and white geometric background. On the left, the text reads: **Protect against Phishing**
Attackers are always devising new and clever ways to get past defenses to reach your inbox.

On the right, there is a mockup of a 'User login' form. The form includes a 'Username' field with a person icon, a 'Password' field with a lock icon, and a 'Login' button. Below the password field is a link that says 'Forgot your password?'.

FDIC is a large target for phishing attacks. Although the Corporation has implemented technology to block a majority of incoming phishing emails, attackers are always devising new and clever ways to get past defenses to reach your inbox. We need your help identifying these emails to strengthen FDIC's defenses.

Scenario:

- You are a member of DOF working with Jim
- As a FIS, Jim receives email 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
- Describe any phishing indicators

You will now enter a simulated scenario about phishing emails. In this scenario, you are member of DOF working with Jim who joined the FDIC about 6 months ago. As a Financial Institution Specialist, or FIS, Jim receives email from internal and external sources. Jim wants to exercise caution opening emails, and turns to you for help.

Your goals throughout this scenario are to: Distinguish between a real email and a phishing email, and Describe any phishing indicators. Click Next to begin.

Play Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

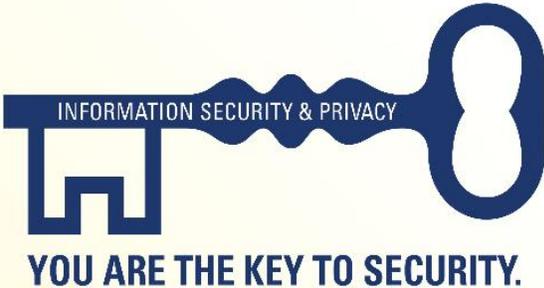
Recognize Phishing Attempts

Successfully recognizing phishing emails is critical to maintaining secure communication.

This topic affects nearly every FDIC employee and contractor.

Common clues to look for include:

- An unfamiliar sender address
- A generic greeting
- Urgent wording
- Poor grammar



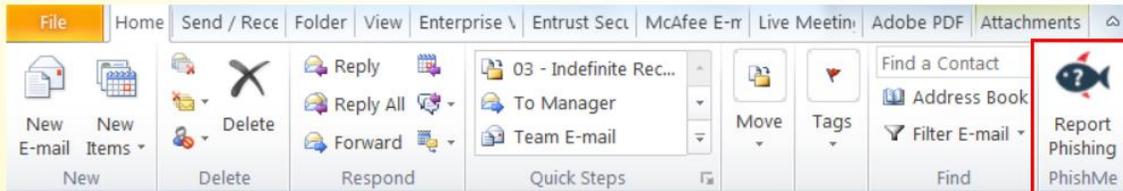
Being able to successfully recognize phishing emails is critical to maintaining secure communication. Since this topic is so important and affects nearly every FDIC employee and contractor, let's review key points about phishing.

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, a generic greeting, urgent wording, and poor grammar.

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Report Phishing



Contact the DIT Help Desk for assistance if you do not see the “Report Phishing” button in Outlook.

FDIC has implemented a “Report Phishing” button in the Outlook e-mail system that you should use to report any suspicious email message you receive. Simply highlight the email in your Inbox and click the “Report Phishing” button on the menu at the top of the screen to automatically forward it to FDIC’s security operations and incident response staff and to move it to your Junk email folder in Outlook. You may also click the “Report Phishing” button even if you have already opened the email. Remember to periodically delete these messages from your Junk Email folder.

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

Email Cautions

- Do not email agency sensitive information or PII to your personal email account.
- Encrypt internal and external emails that contain agency sensitive information or PII.
- 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.

User login

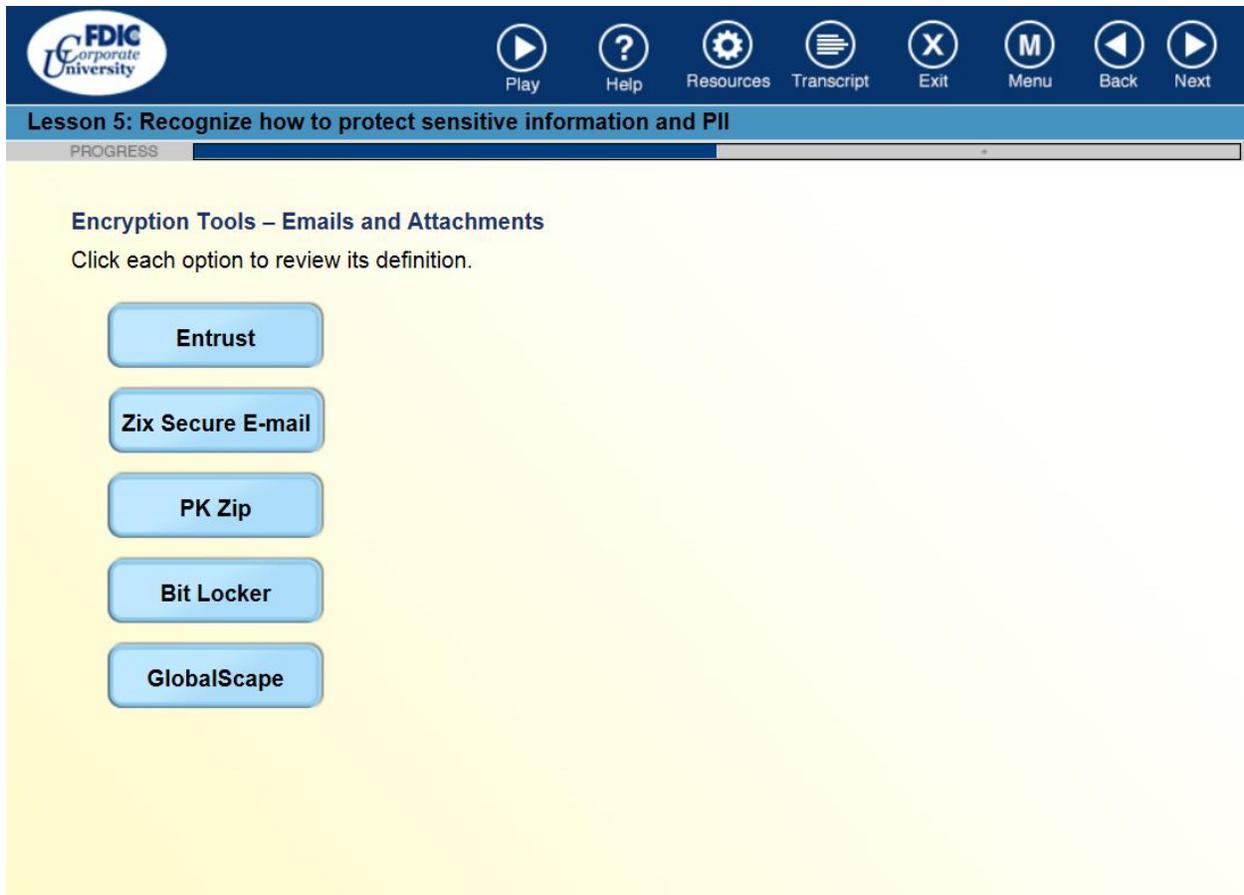
Username

Password

Login

Forgot your password?

Never email agency sensitive information or PII to your personal email account; always encrypt internal and external emails that contain agency sensitive information or PII; and use care when opening weblinks and email attachments, particularly "executable files." As a reminder, FDIC employees and contractors are no longer permitted to copy data to removable media. Click the Resources button for FAQs about Removable Media Protection.



FDIC
Corporate
University

Play Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Encryption Tools – Emails and Attachments

Click each option to review its definition.

Entrust

Zix Secure E-mail

PK Zip

Bit Locker

GlobalScape

Encryption Tools – Emails and Attachments. Click each option to review its definition.

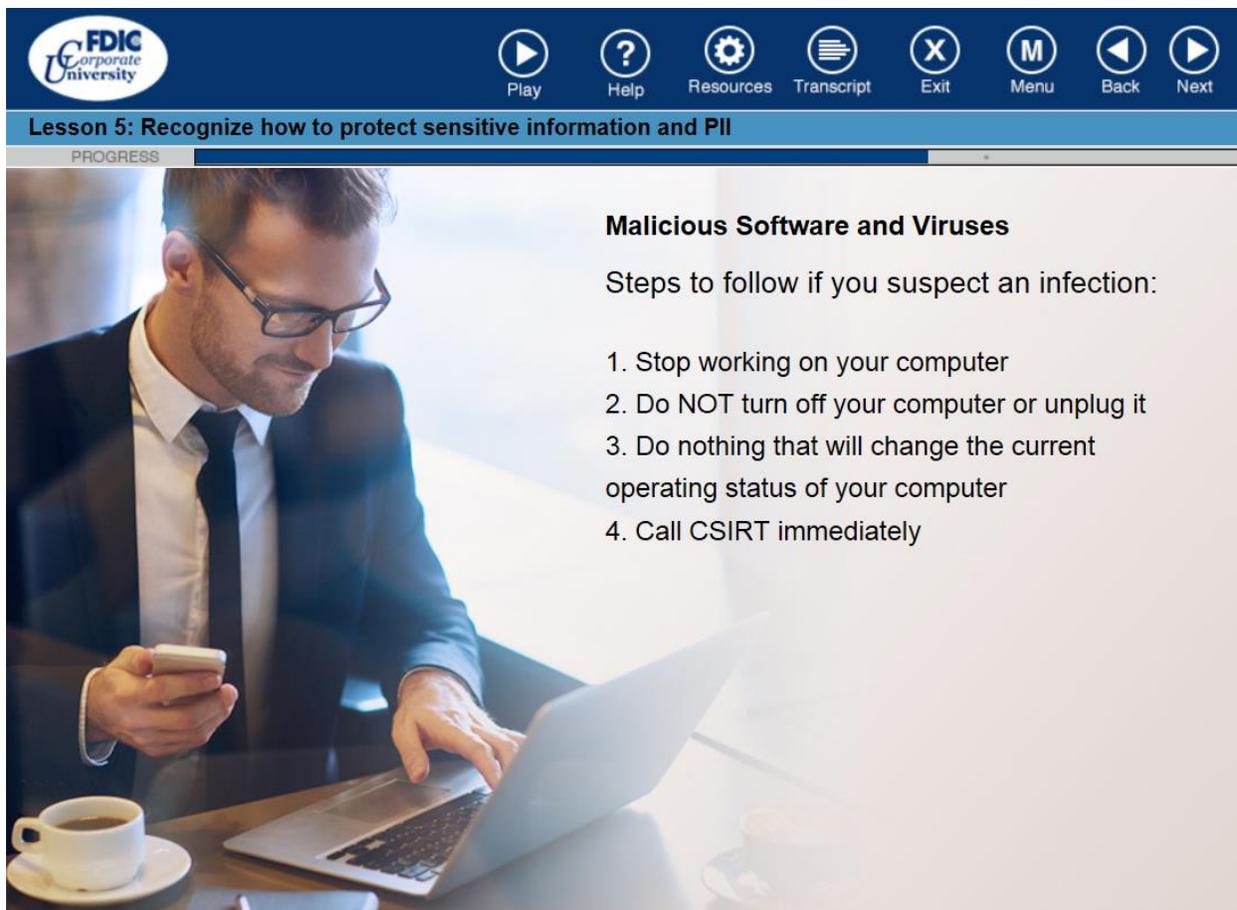
Lesson 5: Recognize how to protect sensitive information and PII

Malicious Software and Viruses

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

[Are you Malware Aware?](#)

There are several symptoms to look for to determine if your computer is infected with malicious software or a virus. For example, 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? If you experience any of these symptoms, check your computer immediately. Click the button to learn more about Malware.



FDIC
Corporate
University

Play Help Resources Transcript Exit Menu Back Next

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

If you suspect that an infection has occurred, follow these steps to remedy the situation:

- Stop working on your computer.
- Do NOT turn off your computer or unplug it.
- Do nothing that will change the current operating status of your computer.
- Call CSIRT immediately.



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: The installation of wireless networks at FDIC facilities is NOT authorized without the expressed written permission of the Deputy Director or CISO for Information Security.

Software Limitations

Software installations: You are not permitted to install software on network computers unless it has been approved by DIT and appears in "Run Advertised Programs." 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.

Firewall Instructions

Internet firewalls: Internet firewalls allow you to connect to the internet from within the FDIC network, while providing a layer of security. When working from home, it is a good idea to have an Internet Firewall in place. Typically home Internet routers will have a firewall built in. You should also install Internet firewall software on your home computer, even if you have a router in place, and keep the program up to date.

Since an FDIC-issued computer can be used to access the network, special steps must be taken to ensure that no one can access information inappropriately or introduce harmful software into the FDIC network, where it might infect many computers or destroy valuable data.

Perhaps the most important security guideline to remember is to never allow someone else to access the network using your User ID and password. Other precautions you should consider include:

- Use of Internet firewalls
- Limit on software installations
- Restrict use of wireless networks

Click on each to learn more.

Lesson 5: Recognize how to protect sensitive information and PII

Information Security Away from the Office

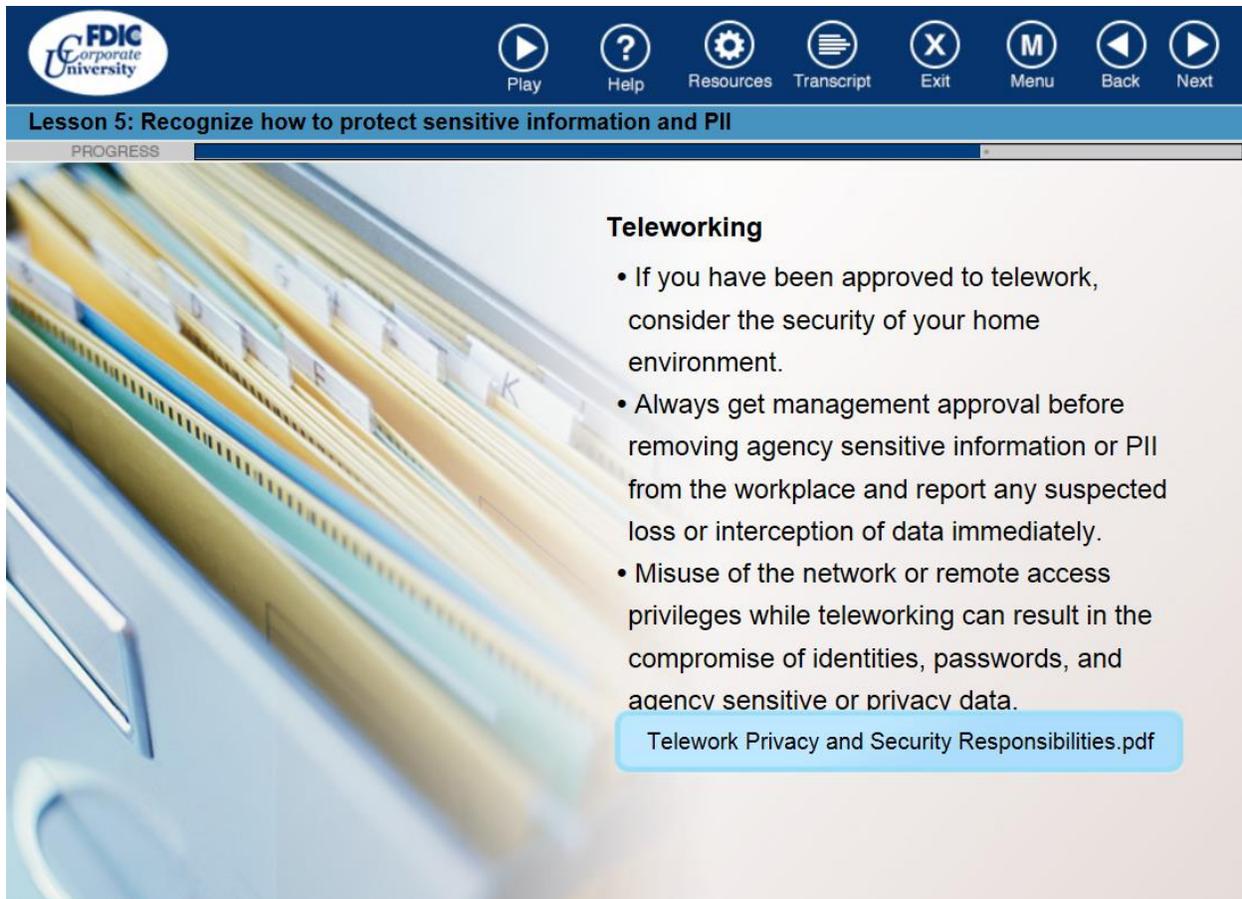
Whether you are on travel status or teleworking, it is important to take precautions to protect agency sensitive information. FDIC employees and contractors are no longer permitted to copy data to removable media.

[View Global Message About Removable Media](#)

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

- 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.

Click the link to review the Policy on Use of Removable Media.



FDIC
Corporate
University

Play Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

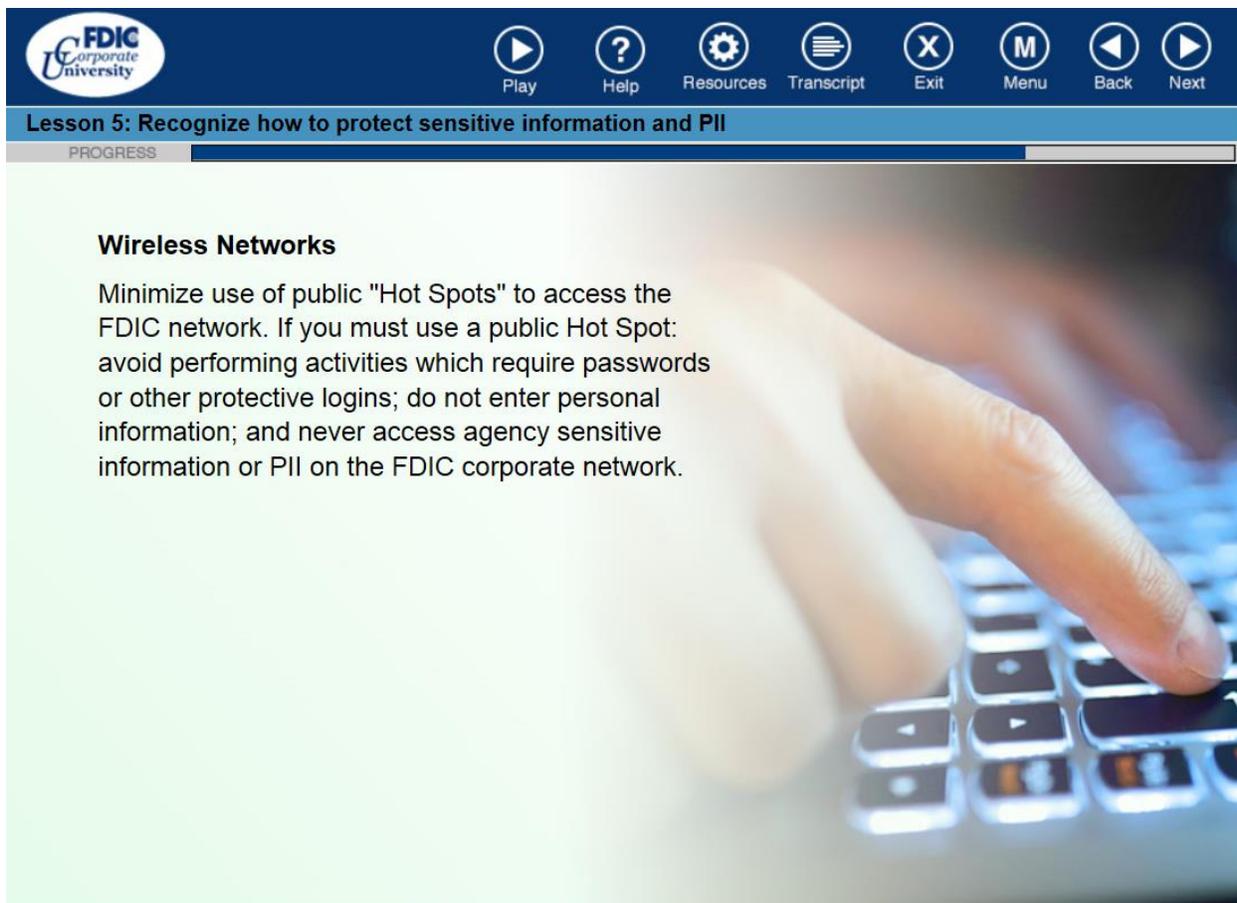
Teleworking

- 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 and 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.

[Telework Privacy and Security Responsibilities.pdf](#)

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 and 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 link to review Telework Privacy and Security Responsibilities.



FDIC Corporate University

Play Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Wireless Networks

Minimize use of public "Hot Spots" to access the FDIC network. If you must use a public Hot Spot: avoid performing activities which require passwords or other protective logins; do not enter personal information; and never access agency sensitive information or PII on the FDIC corporate network.

Because wireless communication is inherently vulnerable, you should minimize use of public "Hot Spots" to access the FDIC network. If you must use a public Hot Spot: avoid performing activities which require passwords or other protective logins; do not enter personal information; and never access agency sensitive information or PII on the FDIC corporate network.



FDIC
Corporate
University

Play Help Resources Transcript Exit Menu Back Next

Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Wireless Network Safety

Users must use only a corporate issued wireless modem connection to a cellular service provider of nationwide or worldwide Internet access.

[Home-Use Wireless Network Setup Guide](#)

When wireless access is required to display or retrieve sensitive information from the FDIC network, users must use only a corporate issued wireless modem connection to a cellular service provider of nationwide or worldwide Internet access. Air cards are only issued to employees whose jobs require the ability to connect to the network in this way on a regular basis.

Home-use wireless connectivity should be configured in a secure manner as reflected in the Home-Use Wireless Network Setup Guide.



Lesson 5: Recognize how to protect sensitive information and PII

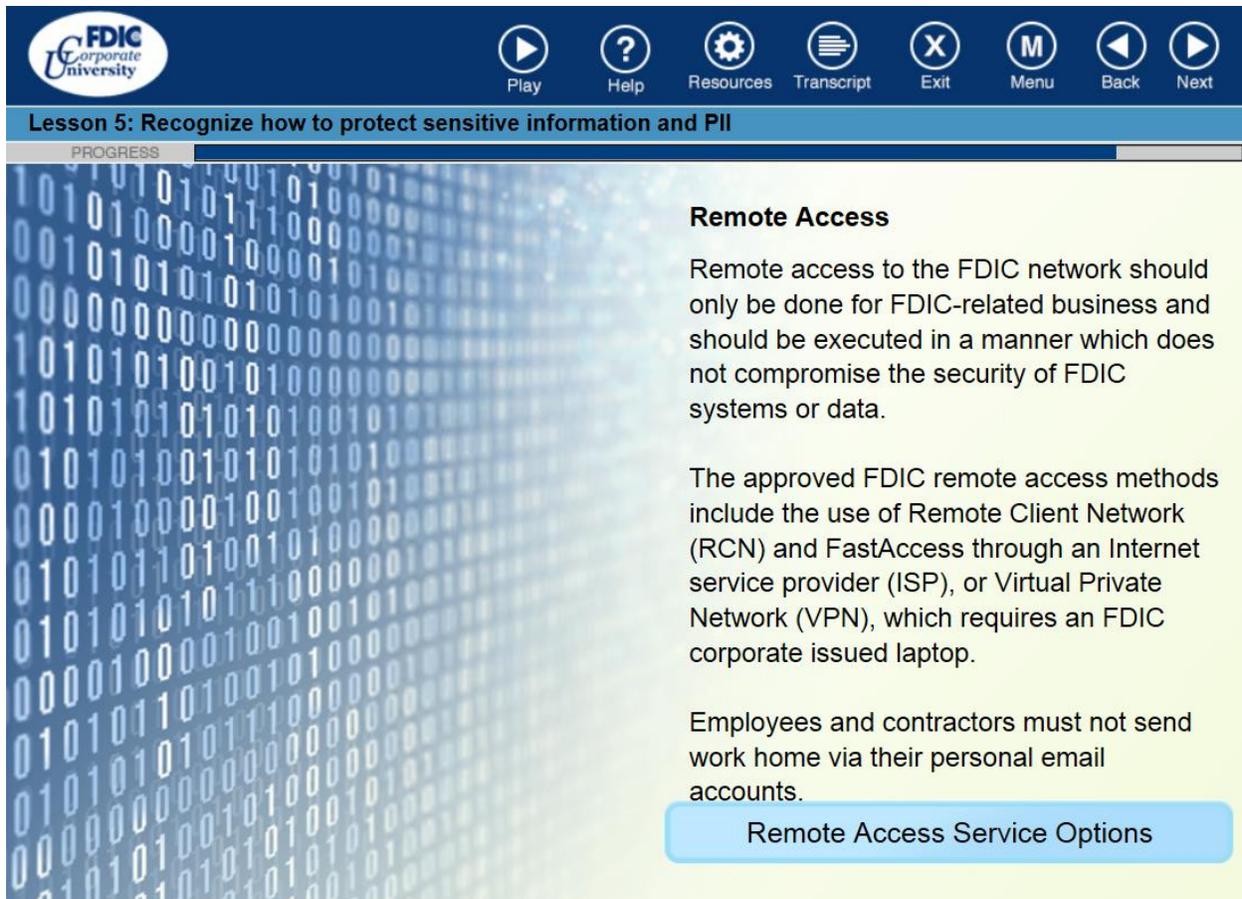
PROGRESS 

Wireless Devices

FDIC provides wireless communication services and equipment to authorized FDIC employees and contractors nationwide. As with all FDIC equipment, these services and equipment should be used for business purposes only and in accordance with guidance. Users must safeguard corporate data and understand their responsibilities for caring for these devices.



FDIC provides wireless communication services and equipment to authorized FDIC employees and contractors nationwide. As with all FDIC equipment, these services and equipment should be used for business purposes only and in accordance with guidance. Users must safeguard corporate data and understand their responsibilities for caring for these devices.



Lesson 5: Recognize how to protect sensitive information and PII

PROGRESS

Remote Access

Remote access to the FDIC network should only be done for FDIC-related business and should be executed in a manner which does not compromise the security of FDIC systems or data.

The approved FDIC remote access methods include the use of Remote Client Network (RCN) and FastAccess through an Internet service provider (ISP), or Virtual Private Network (VPN), which requires an FDIC corporate issued laptop.

Employees and contractors must not send work home via their personal email accounts.

[Remote Access Service Options](#)

Remote access is available to authorized FDIC employees, contractors, and external entities with an authorized need to access the FDIC network from offsite locations. Remote access to the FDIC network should only be done for FDIC-related business and should be executed in a manner which does not compromise the security of FDIC systems or data.

All business-related data on privately-owned computers is subject to internal regulation by the FDIC. Remote users must comply with all FDIC policies and directives. The approved FDIC remote access methods include the use of Remote Client Network (RCN) and FastAccess through an Internet service provider (ISP), or Virtual Private Network (VPN), which requires an FDIC corporate issued laptop. Employees and contractors must not send work home via their personal email accounts.

Click the button to review a list of remote access service options.



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 on a system transferred from one person to another can compromise data and cause serious security and privacy situations.

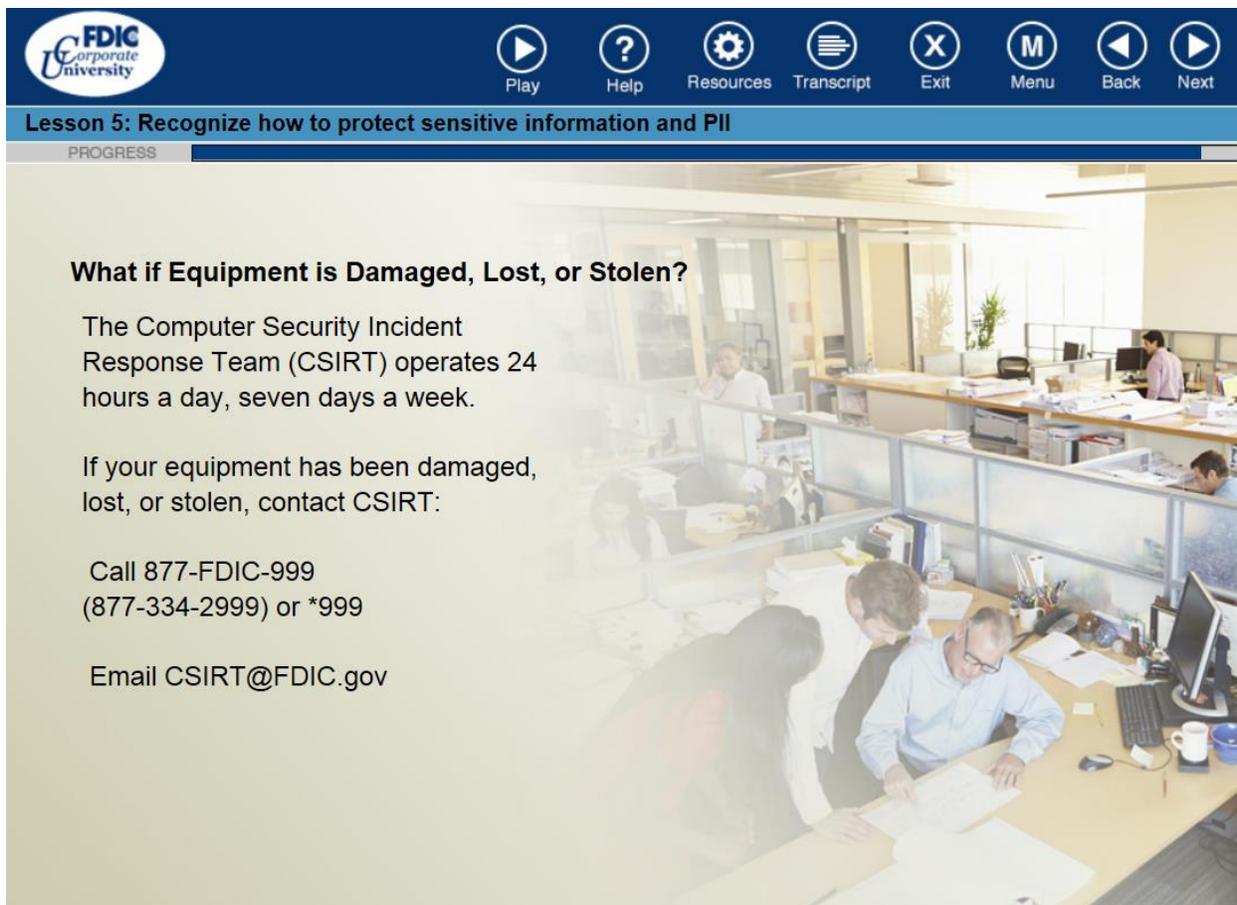
[FDIC Security and Privacy Protection tips](#)

While we have 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 on a system transferred from one person to another can compromise data and cause serious security and privacy situations.

Click the button for more FDIC Security and Privacy Protection tips.



What if Equipment is Damaged, Lost, or Stolen?

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

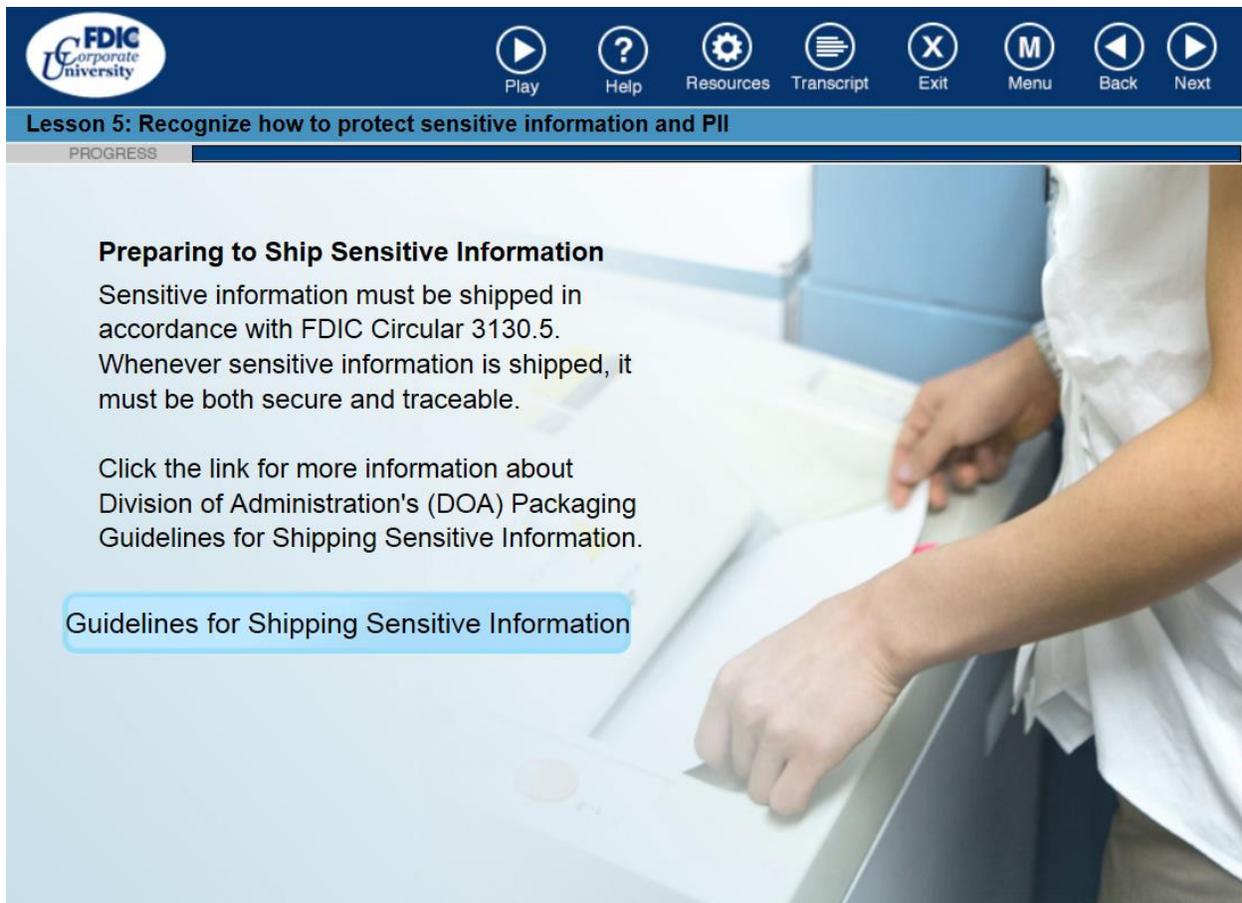
If your equipment has been damaged, lost, or stolen, contact CSIRT:

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

Email CSIRT@FDIC.gov

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 potential computer threats. If your equipment has been damaged, lost or stolen, contact CSIRT.



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](#)

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.

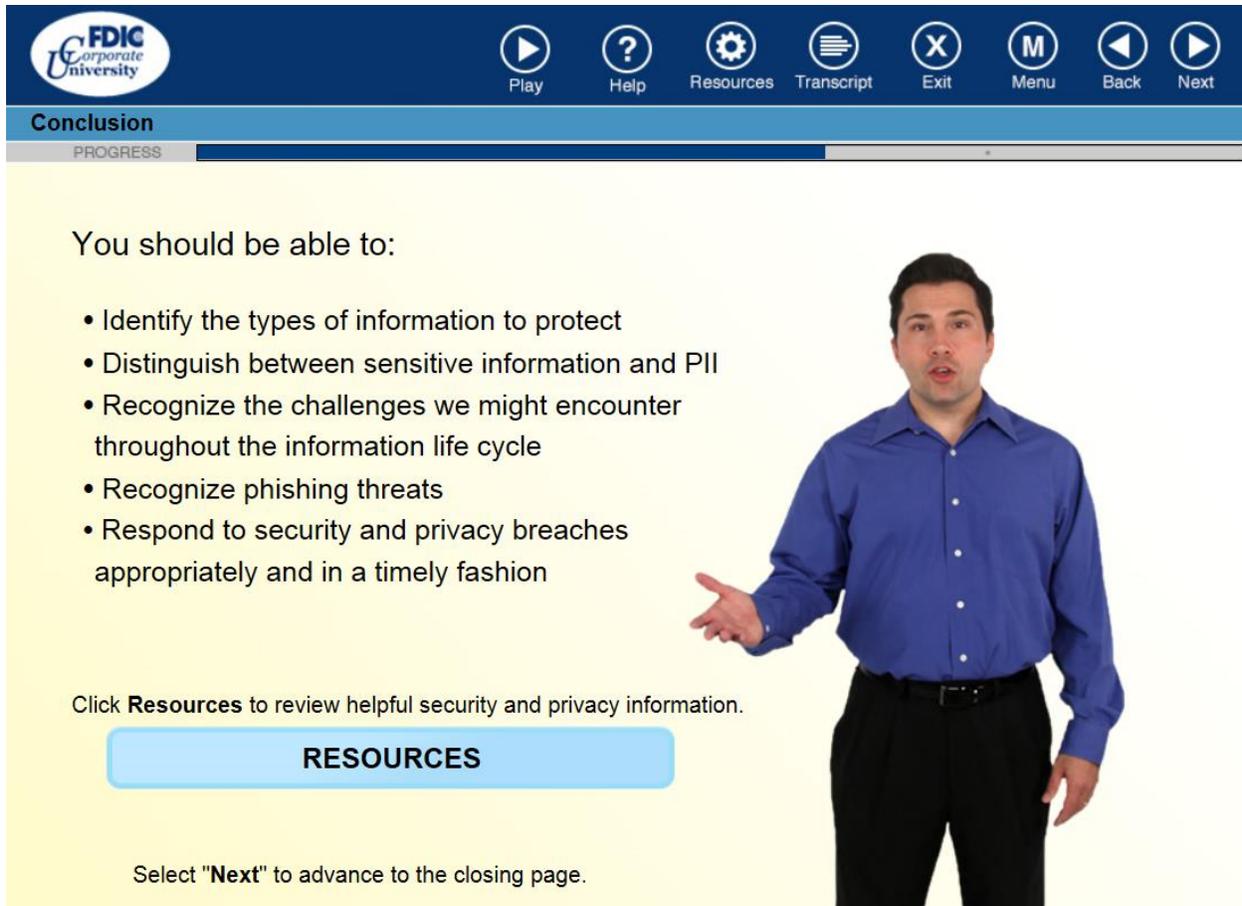
Click the button for more information about Division of Administration's (DOA) Packaging Guidelines for Shipping Sensitive Information.

CONCLUSION



Violating security and privacy-related laws and regulations can lead to serious penalties for all those involved.

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, violating security and privacy-related laws and regulations can lead to serious penalties for all those involved.



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

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

RESOURCES

Select "**Next**" 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 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 and mitigating strategies
- Respond to security and privacy breaches appropriately and in a timely fashion

Click Resources to review helpful security and privacy information. Select the next button to advance to the closing page.

Conclusion

PROGRESS

Congratulations!
You have completed this course.

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

DONE

INFORMATION SECURITY & PRIVACY
FDIC
YOU ARE THE KEY TO SECURITY.

Congratulations! You have completed this course. Click **DONE** to exit. Your transcript in FDIC Learn will reflect your completion of this course. Thank you for your participation and attention to this important information.