# Cybersecurity and Privacy Awareness Training

## Introduction

### Course Objectives

In this course, you will learn how to protect and maintain the Confidentiality, Integrity, and Availability of the FDIC's network, systems, software, and data.

By the end of this course, you will be able to identify:

- Cybersecurity, Privacy, Sensitive Information (SI), and Personally Identifiable Information (PII)
- Cyber-threats and Privacy risks
- Laws, regulations, policies, and directives that govern Cybersecurity and Privacy
- Methods used to protect the FDIC's information during the Information Lifecycle
- How to provide continuous protection of the FDIC's information

### Cybersecurity, Privacy, and You

The FDIC's first line of protection is you. Cybersecurity and Privacy are the responsibility of each FDIC employee and contractor. This course is designed to provide you with information, tools, and techniques to protect information systems and sensitive data from internal and external threats.

# What We Are Protecting

## Key Terms

In order to strengthen the FDIC's Cybersecurity and Privacy posture, it's imperative that we make Cybersecurity and Privacy awareness a part of our culture.

To help you understand your role as the first line of protection for Cybersecurity and Privacy issues, let's learn more about some key terms that will be used in this course:

- Cybersecurity
- Privacy
- Sensitive Information (SI)
- Personally Identifiable Information (PII)

## Cybersecurity

Cybersecurity refers to the protection of networks, systems, devices, and data from unauthorized access and use. It is the practice of protecting systems, networks, programs, and data from digital attacks.

There are three elements to protecting information systems:

1. **Confidentiality:** Protecting information from unauthorized disclosure to people or processes
2. **Integrity:** Assuring the reliability and accuracy of data and information technology (IT) resources
3. **Availability:** Defending information systems and resources from malicious and unauthorized users to ensure accessibility by authorized users

**Below are examples of three elements of protection.**

*Example 1: Three Elements of Protection*

To understand how Confidentiality, Integrity, and Availability work in practice, consider what happens when you log in to an e-commerce site to check your orders and make additional purchases.

- **Confidentiality:** When you log in, you're asked for a password. If it's been a while since your last log in, you may be asked to input a code that has been sent to you via email/text or some other form of two-factor authentication.
- **Integrity:** Data Integrity is provided by making sure your purchases are reflected in your account and allowing you to contact a representative if there's a discrepancy.
- **Availability:** You can log in to your account whenever you want, and you may even be able to contact customer support at any time of the day or night.

*Example 2: Three Elements of Protection*

To understand how Confidentiality, Availability, and Integrity work in practice, consider a bank ATM transaction that offers users access to bank balances and other information.

- **Confidentiality:** It provides Confidentiality by requiring two-factor authentication (both a physical card and a PIN code) before allowing access to data.
- **Integrity:** The ATM and bank software enforce data Integrity by ensuring that any transfers or withdrawals made via the machine are reflected in the accounting for the user's bank account.
- **Availability:** The machine provides Availability because it is in a public place and is accessible even when the bank branch is closed.

## FDIC’s Privacy Program

The FDIC's Privacy Program ensures that privacy is sustained and not eroded by changes in either the financial industry or government practices that impact the FDIC and that privacy protections are integrated into FDIC operations.

The Privacy Program's vision is to provide a strategic, risk-based, and sustainable enterprise-wide privacy program. The Privacy Program's mission is to fulfill, preserve, and anticipate privacy needs of the public that the FDIC serves and to provide leadership to the federal and financial privacy communities.

The Privacy Program works to help achieve the FDIC's mission while appropriately handling information about individuals. Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual. We oversee processing of PII and manage privacy risk.

## How the Privacy Program Supports You

It is important to remember that PII is information about people even if the information does not contain names or other direct identifiers. The Privacy Program is here to help you meet legal requirements, provide transparency to the public, and manage risk to individuals as you use information about people to meet the mission of the Corporation.

When should you contact the Privacy Program?

- Before collecting information linked to people, even from publicly available sources
- Before sharing information about people outside the agency or within the agency for a new purpose
- Before launching a new collection of PII whether a small survey or a large IT system
- When you have questions about appropriate uses of information, including the creation and use of test data

The Privacy Program is here to help! You can find us at Privacy@FDIC.gov.

## Your Responsibilities - Legal Requirements: Privacy Act

You are responsible for complying with the Privacy Act of 1974, including providing the Privacy Program with the information needed to publish System of Records Notices when required. There are penalties, including civil and criminal penalties, for failing to follow the requirements of the Privacy Act.

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. These requirements also apply to certain contracted agency functions.

The FDIC has established safeguards to protect against any anticipated threats that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

The FDIC publishes System of Records Notices at fdic.gov/privacy and in the Federal Register to provide the public with information about collections of information and ways the public can access or amend information about themselves.

## Your Responsibilities – Legal Requirements: E-Government Act

You are responsible for complying with the E-Government Act of 2002, including providing the Privacy Program with the information needed to conduct a Privacy Impact Assessment (PIA) when required.

Privacy Impact Assessments are required by the E-Government Act. The Privacy Program conducts PIAs to ensure sufficient protections for the privacy of personal information.

The FDIC publishes Privacy Impact Assessments at fdic.gov/privacy to document how the FDIC processes personally identifiable information and manages privacy risk for FDIC systems and programs.

## Sensitive Information (SI)

Sensitive Information (SI) is data that must be guarded from unauthorized access and unwarranted disclosure in order to maintain its Confidentiality, Integrity, and Availability. The loss or misuse of Sensitive Information could adversely impact the FDIC's ability to carry out its mission.

In accordance with FDIC Circular 1360.09 Protecting Information, FDIC employees and contractors are required to protect all Sensitive Information collected or generated while working for the FDIC.

**Below are examples of SI.**

*Sensitive Information Examples*

Examples of Sensitive Information include:

- Bank examination and bank closing information
- Proprietary information that could disadvantage the FDIC in procurement actions with vendors and service providers
- Agency proprietary information that could be a disadvantage to the agency in an ongoing negotiation
- Security management information
- Information related to the FDIC's network or information technology that could be misused by malicious entities (for example, IP addresses, server names, firewall rules, encryption and authentication mechanisms, and network architecture pertaining to the FDIC)

## Personally Identifiable Information (PII)

PII is a subset of Sensitive Information that requires additional safeguarding. As previously noted, PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

The FDIC uses PII collected from employees, contractors, and financial institutions. Be sure that when you collect PII, you have the legal authority to do so and if necessary,

have a Privacy Act System of Records Notice (SORN) in place that describes the information.

**Below are examples of PII.**

*Examples of Personally Identifiable Information (PII)*

- Full Names
- Addresses
- Telephone Numbers
- Email Addresses
- Logon IDs
- Financial Information
- Social Security Numbers, including the last four digits
- Biometric Identifiers (e.g., fingerprint, voiceprint)
- Photographic Identifiers (e.g., image, video)

## Summary

Cybersecurity protects the FDIC's information from risks. Cybersecurity measures protect online information and secure the infrastructure on which it resides, along with network and application infrastructures that protect data and Sensitive Information.

Cybersecurity and Privacy protection are interconnected. You are responsible for securing PII when it is in transit AND when stored on a hard drive, laptop, flash drive, or archived.

Organizations strive to keep pace with the changing landscape created by innovative technologies, social practices, and ever-changing threats. The next lesson describes the many cyber-threats faced by the FDIC.

# Cyber-Threats

## What Do Cyber-Threats Include?

Cyber-threats are any circumstances or events with the potential to adversely impact organizational operation (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.

Types of Cyber-threats:

1. **Activity that *targets computers and data*:**
    - Malware
    - Ransomware
    - Password Attack
2. **Activity that *targets users/individuals*:**
    - Social Engineering
    - Phishing
    - Smishing/Vishing

Next, we'll look at examples of each type of Cyber-threat.

## Malware

Malware, which is short for malicious software, is a software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer, network, or server. Malicious email links and attachments are two of the most common sources of malware infections.

Ransomware is amongst the most common type of malware attack, where files and users are locked out until a ransom is paid.

| Type | What It Does |
|---|---|
| Fileless Malware | Makes changes to files that are native to the operating system |
| Spyware | Collects user activity data without their knowledge |
| Adware | Delivers advertisements to generate revenue for its creator or a third party. It is often used in conjunction with spyware. |
| Trojan | A type of malware that is disguised to look like a legitimate program, utility, or game |
| Worm | Spreads through a network by replicating itself |
| Rootkit | Gives hackers remote control of a victim's device |
| Keylogger | Monitors users' keystrokes |
| Mobile Malware | Infects mobile devices |

## Malware: Symptoms and How to Take Action

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

- Does your computer demonstrate reduced responsiveness or sudden loss of power?
- Are you suddenly running low on hard drive space?
- Do you have missing files or notice that your file names have changed?
- Does your computer crash frequently?
- Do others report receiving unusual messages from you?

If you experience any of these symptoms, please call the CIOO Service Desk.

## How to Report It

If you suspect your computer is infected with malware, contact the FDIC's CIOO Service Desk.

Telephone: 1-877-334-2999

Email: ServiceDesk@FDIC.GOV

## Malware: Prevention

Follow the **tips** below to stay protected and minimize threats to your data and accounts.

- Help the FDIC to deploy workstation security patches on your FDIC equipment by accepting and allowing the security patches to run on your devices.
- If you have an FDIC-issued iPhone or iPad, install iOS and other app updates in a timely manner.
- Be wary of links and attachments.
- Watch out for malicious or compromised websites.

## Computer Security Incidents

A computer security incident is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information. These incidents can jeopardize the Confidentiality, Integrity, or Availability of information. This includes interference with information technology operation and violation of laws or regulations, security policies, security procedures, or acceptable use policies.

**Examples of security incidents include:**

- Unauthorized disclosure of Sensitive Information via email or other types of data transfers
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data
- Loss or theft of equipment storing institutional data
- Denial of service attack
- Interference with the intended use of IT resources
- Compromised user accounts

## Computer Security Incidents: Violations and Failures

Violations of security rules and regulations may result in a variety of serious consequences including:

- Permanent loss of data
- Identity theft
- Unauthorized disclosure of data

Failure to abide by FDIC's security policies could result in adverse actions including:

- Removal of access
- Reprimand
- Suspension, demotion, or termination
- Referral to law enforcement

## Password Attack

Password attacks refer to various methods that attackers use to maliciously access a password-protected system by compromising a legitimate user account. Some of the most common types of password attacks include dictionary attacks, credential stuffing, and brute force attacks.

- **Dictionary Attacks:** The use of commonly used passwords such as words found in the dictionary
- **Credential Stuffing:** The use of previously compromised passwords on multiple accounts belonging to a user
- **Brute Force:** Using computing power to try all possible combinations of passwords for a system

To help prevent password attacks, you should use strong passwords and multi-factor authentication when it is available. You should also never use the same password for multiple accounts.

## Password Protection

When multi-factor authentication is not available, passwords provide a critical defense against access to your FDIC equipment and accounts. Creating a strong password is one of the best ways to help protect the FDIC.

You should always create long and strong passwords to help prevent unauthorized access to your computer or accounts.

Passwords must contain three of the following:

- English uppercase letters (A through Z)
- English lowercase letters (a through z)
- Arabic numerals (0 through 9)
- Punctuation and other special characters (! @ # $ % ^ & * ( ) _ + | ~ ` - = \ { } [ ] : " ; ' < > ? , . /)

You must change your password every 365 days. You cannot reuse your previous ten (10) passwords when you change your password.

If you forget your password, you may use the Self-Service Password Reset utility at https://www.fdic.gov/PasswordReset.

## PIV Card

A Personal Identity Verification (PIV) card is a smart card with a computer chip that is used to access facilities or information systems and assure appropriate levels of security. A six to eight-digit PIN is required to access your system. Your laptop does not lock when you remove your PIV card. Please remember to lock your computer by selecting Ctrl+Alt+Del or the Windows key + L simultaneously.

Your PIV Card is more than a picture ID. It contains Sensitive Information about you and your system access rights.

If your PIV Card is lost or stolen, you must report the loss immediately.

Here are three ways to protect your PIV Card:

- Never share your PIV PIN.
- Create a PIN that is hard for someone to guess.
- Never leave your PIV card unattended.

## Social Engineering

Social engineering is typically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and Sensitive Information for fraudulent or criminal purposes. Social engineering attacks are more common and more successful than the other cyber-threats.

Social engineering attacks are based on human character traits such as:

- Trust
- Desire to help
- Desire to avoid conflict
- Fear
- Curiosity
- Ignorance or carelessness

Offenders prey on basic human emotions, empathy, and naiveté to obtain your personal information, access sensitive government information, and even steal your identity.

## Social Engineering Types and Impact

In social engineering attacks, attackers try to fool their targets through impersonation. They might pretend to be your boss, your supplier, someone from our IT team, or your delivery company. Regardless of who they're impersonating, their motivation is typically the same—extracting money or data.

### *Spear Phishing*

A communication that targets a specific, named person in order to steal Sensitive Information such as account credentials or financial information. Spear phishing plays on the target's trust, exploits weak security practices, and can cost a business millions of dollars.

### *Deepfake*

A fraudulent piece of content (videos or audio recordings) that has been manipulated or created using artificial intelligence.

**Example:** A criminal gang operating in a tourist location conducts targeted and opportunistic fraud schemes against victims using synthetic images and video to depict someone in a situation of captivity.

### *Vishing*

Vishing is also known as voice phishing. It is the use of fraudulent phone calls to trick people into giving money or revealing personal information. Vishing frequently involves a hacker pretending to represent a trusted institution, company, or government agency.

### *Smishing*

Smishing is a form of phishing in which an attacker uses a compelling text message to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphone.

### *Baiting*

Social engineering attack where a scammer uses a false promise to lure a victim into a trap which may steal personal and financial information or inflict the system with malware.

### *Scareware*

A tactic that manipulates people into believing they need to download or buy software that may not be needed and can sometimes be malicious.

*Pretexting*

Pretexting is a type of social engineering attack where a cybercriminal stages a scenario, or pretext, that baits victims into providing valuable information that they wouldn't otherwise disclose.

## Phishing

Phishing, another form of social engineering, is the practice of sending fraudulent communications, such as emails or text messages, that appear to come from reputable sources. The goal is to trick the reader into revealing personal or confidential information, such as passwords and credit card numbers, or to install malware on your computer or mobile device.

For example, phishing scams quite often alert you to a problem with your account and ask you to click on a link and provide information to correct the situation. These emails look real and often contain the organization's logo and trademark.

Visit the OCISO Phishing Guidance website for more information and examples of phishing.

If you are suspicious of an email or text message:

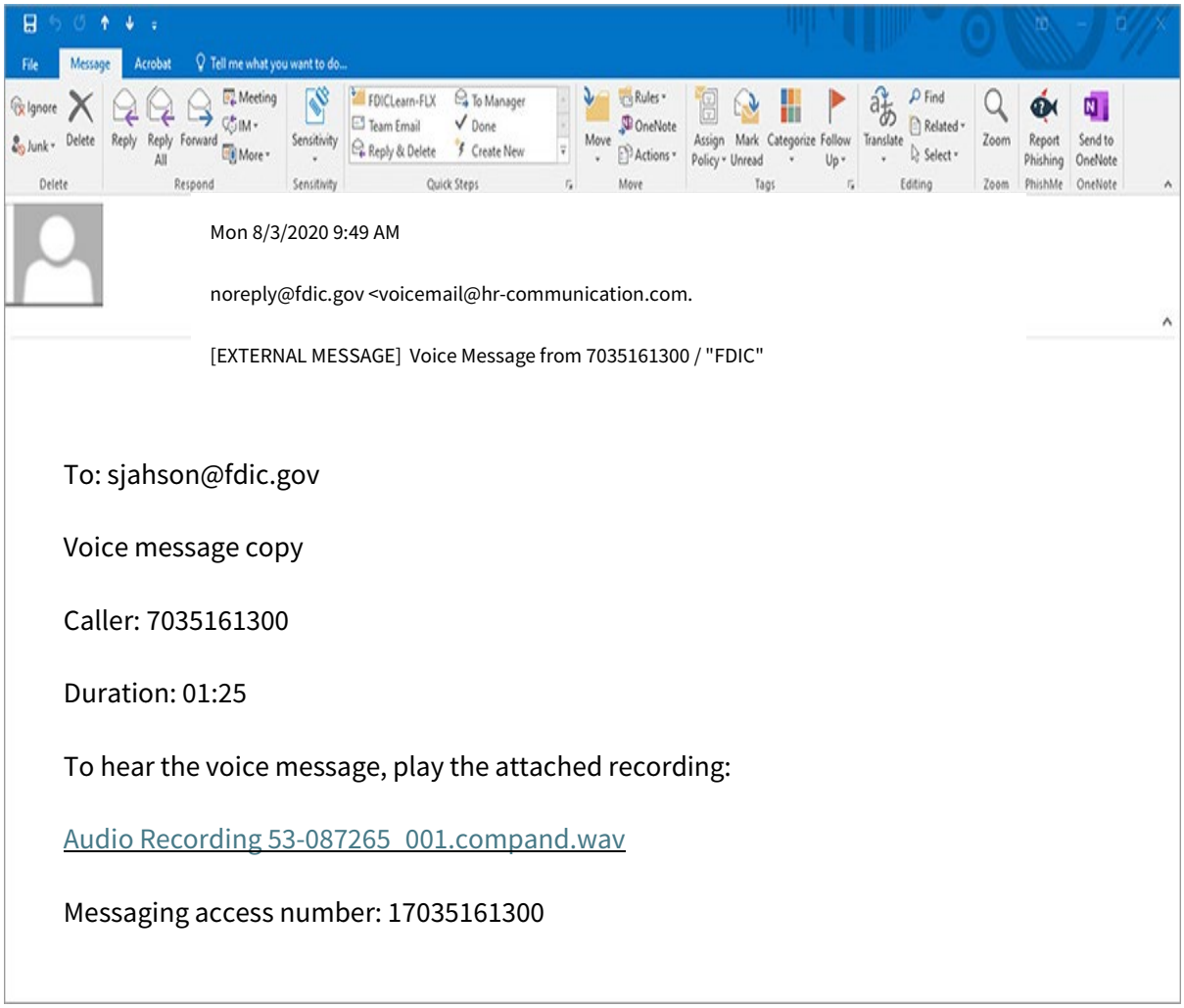
- Do not reply.
- Do not click on the links provided in the email.
- Do not download OR open any attachments in the email.
- Do not provide FDIC business information, sensitive or personal information, or financial data.

## Steps in a Phishing Attack

1. Attacker sends an email to the victim.
2. Victim clicks on the email and goes to the phishing website.
3. The victim enters their credentials.
4. The attacker collects the victim's credentials.
5. The attacker uses the victim's credentials to access confidential information.

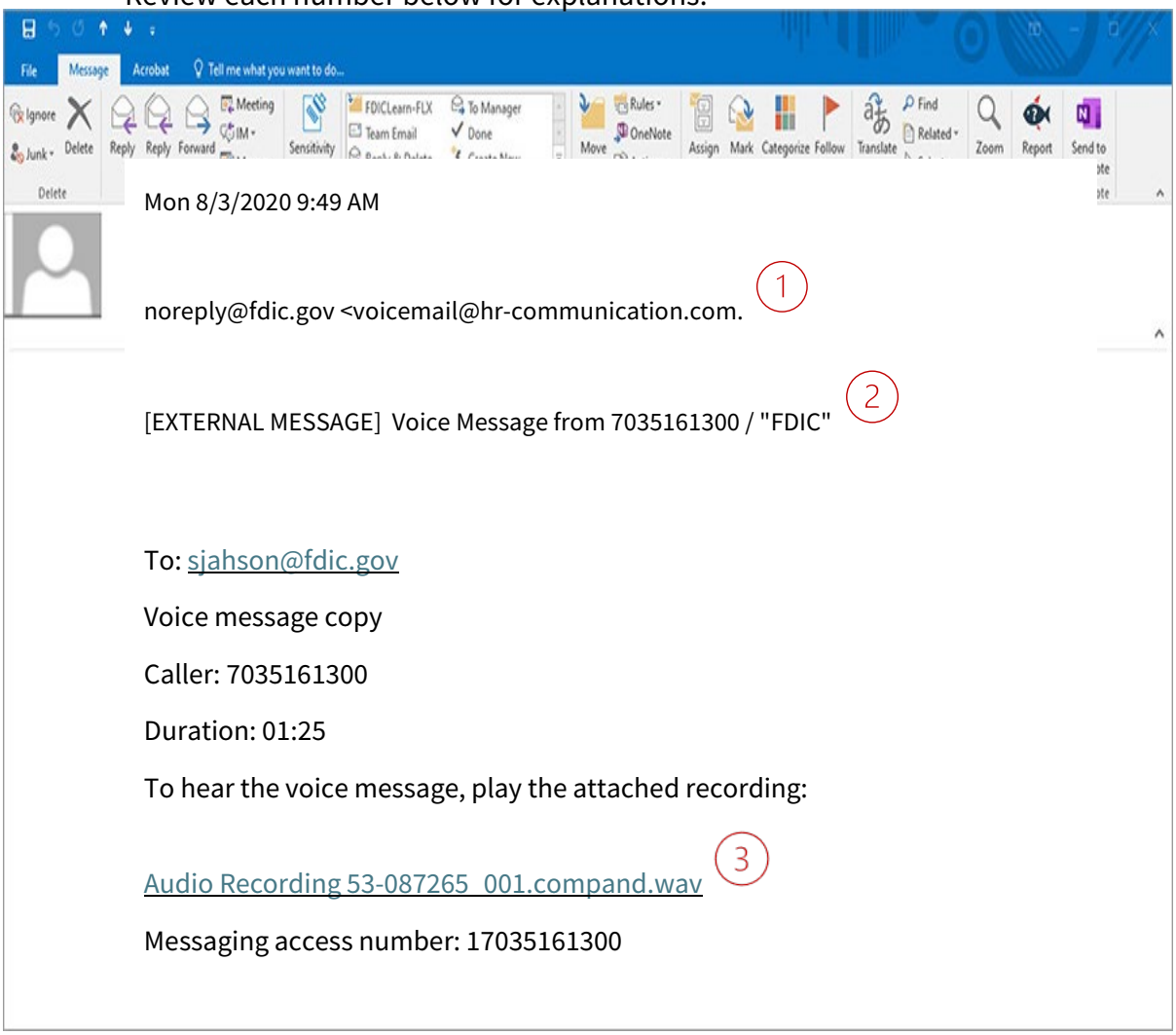
## Can You Identify Phishing?

Review the email below and identify the phishing indicators. Compare your findings with the answers on the next page.



## Did You Identify These Phishing Indicators?

Review each number below for explanations:



*1. The Domain*

The email address indicated does not end with .gov. It ends with .com.

This is an indicator that an email may need to be reported for phishing.

*2. The Subject Line*

The Subject line for internal FDIC email displays an [EXTERNAL MESSAGE] warning.

Emails from external sources should be vetted to ensure the sender is not attempting to gain unauthorized access to your computer.

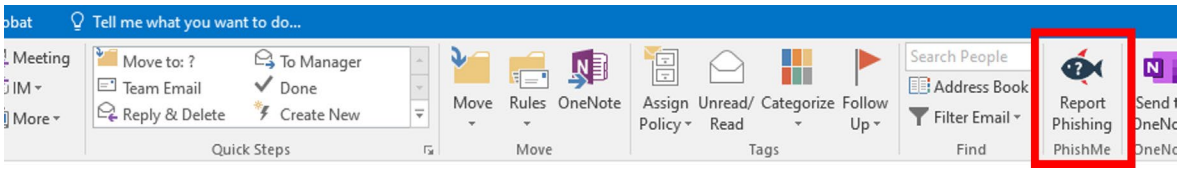
*3. The Link*

Do not open links from unknown senders. When reading emails, hover over links to display their URLs.

Links from unknown senders can contain things that can damage your computer and the FDIC's security like malware.

## Reporting Phishing

If you receive a suspicious email in your FDIC mailbox that you think may be a phishing attack, click on the "Report Phishing" button in the Outlook toolbar. The email will be forwarded to the Security Response Team (SRT) and then moved to your "Junk Email" folder in your Outlook mailbox.



## Social Engineering Prevention

To prevent social engineering attacks:

- Be suspicious of unsolicited phone calls or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about the FDIC, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in emails, and do not respond to email solicitations for this information. This includes following email links or attachments.
- Validate that a website is legitimate and secure before entering or uploading any sensitive data.
- Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with **https**—an indication that sites are secure. Avoid URLs that begin with **http**.

## Avoiding Social Engineering

One method to validate that a website is legitimate is to look for "https" at the beginning of the URL. Most web browsers will display a padlock icon that indicates that a website is using a SSL certificate that has been issued by a trusted authority. You can often click on the padlock icon to get additional information about the website.

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request. Instead, check previous statements or conduct a web search for the company's contact information.

## Your Responsibilities – Breach Response

You are responsible for reporting suspected or confirmed breaches of personally identifiable information as soon as possible. If you observe a breach of PII, whether suspected or confirmed, report the situation immediately to the Security Response Team (SRT) (703-516-5760 or SRT@fdic.gov).

A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

- A person other than an authorized user accesses or potentially accesses personally identifiable information or
- An authorized user accesses or potentially accesses personally identifiable information for another than authorized purpose.

A breach is a type of information security incident. It may include the inadvertent disclosure of PII on a public website, an oral disclosure of PII to an individual who is not authorized to receive that information, or an authorized user accessing PII for a purpose that has not been authorized.

## Summary

Cyber-threats have no bounds. They can impact your personal and professional life.

You must remain vigilant to protect the FDIC from cyber-threats. Remember the following best practices:

- Use strong passwords.
- Be suspicious of unsolicited phone calls, text messages, and email messages.
- Do not reveal personal information or information about the FDIC unless you are certain of a person's authority to have the information.
- Do not click on unfamiliar links or attachments.
- Immediately report actual or suspected security incidents and breaches to the Security Response Team (SRT) at 703-516-5760 or SRT@fdic.gov.

In the next lesson, you will further explore how Cybersecurity and Privacy measures impact the Information Lifecycle.

## Protecting Information Throughout the Lifecycle

### Information Lifecycle

The information lifecycle consists of the following stages: **collection and creation, use, maintenance, storage, sharing and disclosing, and disposal, to include destruction and deletion.**

You are responsible for protecting data from collection and creation to disposition as part of the information lifecycle. Protecting the FDIC's information is required during each stage of the information lifecycle.  Let's look at what your responsibilities are at each stage of the information lifecycle.

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

When gathering the FDIC's information for collection and creation, ask yourself the following:

- Are you allowed to collect the PII by law?
- Do you have a legitimate business need to collect the PII?
- Are you obtaining the information in a safe manner so that it cannot be overheard or seen by others?
- Did you only request the minimum amount of PII to get the job done?
- Are you collecting information that is necessary for your job?

The data should be labeled as soon as it is created or acquired to ensure that sensitive data is handled correctly throughout this whole process.

## Document Labeling

Document Labeling enhances the FDIC's ability to ensure documents are shared and protected appropriately. The requirements for document labeling are contained in FDIC Directive 1350.04 – Document Labeling. The data should be labeled as soon as it is created or acquired to ensure that sensitive data is handled correctly throughout the whole process.

The proper way to label FDIC documents is shown below in the FDIC Document Labeling Framework and associated labels. **In the designation and dissemination columns are detailed definition.** There is also a Document Labeling Decision Tree available.

*FDIC Document Labeling Framework*

| Designation | Dissemination | Visual Label |
|---|---|---|
| **Controlled** Information is Sensitive Information that requires protection from unauthorized access and disclosure under law, federal regulation, Government-wide policy, or FDIC policy. | FDIC Internal Only refers to FDIC employees and FDIC contractor personnel with a FDIC.gov or FDICOIG.gov email address authorized to access or receive FDIC information for legitimate business purposes.<br><br>or<br><br>FDIC Business Partners refers to individuals, organizations, or entities external to the FDIC, authorized to access or receive FDIC information for legitimate business purposes. | CONTROLLED/FDIC INTERNAL ONLY<br><br>CONTROLLED/FDIC BUSINESS |
| **Nonpublic** Information is non-Sensitive Information that has not been approved for release to the general public. | FDIC Internal Only, or FDIC Business Partners | NONPUBLIC/FDIC INTERNAL ONLY<br><br>NONPUBLIC/FDIC BUSINESS |
| **Public** Information is available to the general public and intended for distribution outside of the FDIC. | Not Applicable | As specified by FDIC public release processes |
| **Non-work** Information is personal or other non-business information. | Not Applicable | NONE |

## Use

The use of information and equipment refers to the appropriate handling of the FDIC's information in accordance with authorized legal or business requirements. You are responsible for knowing who is authorized to access Sensitive Information before you disclose it.

Always remember when you walk away from your FDIC laptop to lock your screen by selecting Ctrl-Alt-Del and then pressing Enter or pressing the Windows key + L.

Before using the FDIC's information to accomplish a job function, make sure you ask yourself the following:

- Are you using the information for a purpose that is consistent with why it was collected?
- Are you only using the minimum amount of PII to get the job done?
- Are you accessing PII through secure and authorized equipment and connections?

If you are uncertain about the uses of the information you work with every day, talk with your supervisor. You can also contact FDIC's Privacy Program by emailing Privacy@fdic.gov.

## Acceptable Use Policy for FDIC Information

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 or create a Cybersecurity risk, please remember these **key policies**:

- Seek approval from management to take FDIC-issued equipment outside of the United States.
- 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 unattended.
- Never use your FDIC-furnished device for any illegal or inappropriate activity.
- Never send text messages that contain FDIC Sensitive Information.
- 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 Chief Information Officer (CIO).
- Never install or use unauthorized software or services.
- Never transmit FDIC work-related data to a personal email account.
- Never allow any unauthorized individual to access FDIC-furnished equipment.

**Violations of the Acceptable Use Policy may be subject to disciplinary action.**

## 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's or Office's Records Liaison.

Your responsibility to aid the FDIC in maintaining current workstation security patches on your FDIC equipment includes you accepting and allowing the security patches to run on your devices.

If you have an FDIC-issued iPhone or iPad, install iOS and other app updates in a timely manner.

Call the FDIC's CIOO Services Desk for patching and update information.

TELEPHONE: 1-877-334-2999

EMAIL: ServiceDesk@FDIC.GOV

## Storage

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

Data should be stored securely in accordance with FDIC policies and standards. Only store data in appropriate locations within the FDIC network. These storage locations may include SharePoint sites, Teams sites, and shared drives, and access to those locations must be limited to only those who are authorized to access the information.

In the next two screens, we will discuss how to manage paper copies and electronic copies.

## Storing Paper Copies

When storing paper copies, follow these guidelines:

- Avoid making paper copies of Sensitive Information or PII whenever possible.
- Store paper copies of 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 sensitive data or PII in your vehicle.
- Printed Sensitive Information at home should never be left out unattended. Documents should be in a locked drawer or file cabinet.
- Sensitive Information that is being transported in a vehicle should always be out of sight and the vehicle should be 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 Electronic Copies

When storing electronic copies, follow these guidelines:

- 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 are relevant to your task.
- Do not download any data from any FDIC-furnished equipment to removable media (for example, USB storage device, CD, or 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 protect the original data.

## Sharing and Disclosure

Before disclosing or transferring sensitive information, ask yourself:

- Are you sending it securely?
- Are you emailing sensitive information to a valid email address?
- Did you verify that the sharing is allowed? Have you verified that everyone receiving the sensitive information has a need to know?
- Did you share only the minimum amount of sensitive information and follow disclosure procedures?

There are special rules governing the sharing of the FDIC's information to other parties.

## Protecting Sensitive Information When Shipping

Sensitive Information must be shipped in accordance with FDIC Circular 1800.08 – Mail Management Program.

Whenever Sensitive Information is shipped, it must be both secure and traceable.

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

## Encryption

Encryption is the translation of data into a secret code. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

With internal and external cyber-threats on the rise, encryption plays a major role in protecting data at rest and in use or in motion. Sensitive data should always be encrypted when doing business internally or externally.

Messages sent to other FDIC personnel on the FDIC network are natively encrypted at rest and in transit. When sending data electronically, see the options below that are available to you:

- **Secure Email (Zix)** – Used to communicate outside the FDIC; limit of 10 attachments with a total 15 MB uncompressed size
- **Secure Attachments (PKZip)** – Used to securely send attachments **within the FDIC**
- **GlobalScape** – Used to securely send ***large*** (75 GB) attachments **outside of the FDIC**

We'll now look at each of these tools and how they should be used.

## Encryption Tools: Zix Secure Email, PKZip, and GlobalScape

**Zix Secure Email:** Zix secure email 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**).

**Secure Attachments PKZip:** The standard FDIC laptop has been pre-installed with PKZip software that allows for the creation of encrypted .zip files. Encrypted .zip files may ONLY be sent **internally** as attachments in email.

**GlobalScape:** GlobalScape is used to securely transmit large files to recipients outside of the FDIC.

- Only used for official business.
- Access is requested through ARCS.
- Recipients will receive a link to access the files.

## Disposal

Dispose of the FDIC's information securely in accordance with record management requirements and organizational disposal policies.

- Follow the disposal timeframes contained in the applicable records retention schedule.
- Verify whether records are covered by a legal hold prior to disposing of the records.
- Put hardcopy documents in an FDIC-provided shred bin.
- Never dispose of FDIC records or equipment by putting them in the trash.

Having a clearly defined and documented information lifecycle management process is key to ensuring employees maintain data and equipment in a way that ensures accuracy and consistency.

## Security on the Go

### What Are Mobile Devices?

Mobile devices are portable computing devices with the following characteristics:

- They are small and easily portable.
- They operate without physical connections (e.g., wirelessly).
- They possess local data storage.
- They are powered on for extended periods of time.

FDIC-issued mobile devices include smart phones and tablets (for example, iPads and iPhones).

The universe of mobile devices is constantly expanding to include fitness trackers, smart watches, medical devices, and other portable technologies.

The portability and wireless connectivity of mobile devices makes them uniquely vulnerable to a range of threats.

In our working environment, we have to be vigilant about protecting FDIC Sensitive Information, information systems, and mobile devices when on travel, working at home, or at remote locations. It is your responsibility to protect FDIC technology and resources that are assigned to you when you are outside of the office, including mobile phones, laptops, and tablets.

### Mobile Device Threats

- Mobile devices are small and can be easily lost or stolen.
- Thieves and fraudsters are able to utilize wireless connectivity technologies to access data on a mobile device.
- There are risks associated with downloading mobile applications such as Privacy concerns associated with applications that can track user activities.
- Only install FDIC-approved mobile apps for business use from the Company Portal (Comp Portal) on iOS devices.

- Data that is transmitted wirelessly is at risk for being intercepted by unauthorized individuals.

## Mobile Device Threats and Vulnerabilities

Threat: **Compromise**

Vulnerability: **Wireless Connectivity**

- Wireless communications can be compromised if they are transmitted on unsecure wireless networks.
- Wireless technologies can enable attackers to connect directly to mobile devices to access data without authorization.

Threat: **Loss/Thef**

Vulnerability: **Physical Size**

- The relatively small size of mobile devices makes them easy to steal and easy to lose.
- Immediately report any lost or stolen mobile device to the CIOO Service Desk (877-334-2999 or ServiceDesk@fdic.gov).

Threat: **Unauthorized Access**

Vulnerability: **Computing Environment**

- To reduce the risk of unauthorized access and malware to your mobile device, only install FDIC-approved mobile apps for business use from the "Comp Portal" on iOS devices.
- Connecting to wireless networks while traveling internationally may give unauthorized parties access to your mobile device.

Threat: **Compromise**

Vulnerability: **Human Factors**

- Phishing attacks are often successful on smart phones because the small screens make it more difficult to review emails.

- Smart phones are also subject to Vishing attacks (voice-based phishing) and Smishing attacks (text-based phishing).

## Securing Your Mobile Device and Communications

Always ensure that your mobile devices are physically secure. Do not leave them unattended. Always store mobile devices in a secure location when not in use.

- Ensure that the software on your mobile devices is up-to-date.
- Exercise caution when connecting to public Wi-Fi networks (secured or unsecured). Although the use of public hotspots and Wi-Fi is acceptable, the FDIC encourages users to connect to the FDIC network through FDIC-issued equipment and services (for example, connecting through an FDIC-furnished Mi-Fi or an FDIC-issued smartphone's hotspot).
- Limit the storage of FDIC sensitive data on mobile devices to as little as necessary.
- You may connect personally owned peripherals (e.g., headsets, keyboards, etc.) to FDIC-furnished mobile devices provided they are "plug and play" technologies. However, do not connect to peripherals that you do not own or control.
- Turn off Bluetooth when it is not needed.

## Protecting Your Mobile Device and Communications

- **Do not** send FDIC Sensitive Information via text message. There are risks associated with texting sensitive FDIC information to other individuals.
- **Do not** attempt to make unauthorized modifications (e.g., jailbreaking or rooting) to FDIC-furnished devices.
- **Do not** take FDIC-issued equipment outside the United States **without** authorization. Submit a CIOO Services Portal International Service Request to request approval.
- **Do not** take photos of FDIC Sensitive Information such as notes on a whiteboard.

- **Do not** click on links received in text messages to avoid Smishing attacks.

## Telework

Being allowed to telework provides workplace flexibility that assists the FDIC in maintaining continuity of operations while also supporting the FDIC's goal of improving employees' ability to balance their work and life commitments. FDIC personnel working remotely must continue to comply with all security, privacy, and records management requirements contained in the FDIC and directives.

Use the following security practices when working remotely:

- Only use your FDIC-issued laptop or mobile device to conduct FDIC business. You should not use your personal computer or mobile phone for work purposes.
- Never use personal email accounts to send or receive work-related information.
- Always maintain control over your FDIC-furnished laptop and mobile device. Be sure to store these items in a secure location when you are not using them.

See Directive 2121.1, FDIC Telework Program for additional information about telework.

## International Travel

While on travel status, it is important to take precautions to protect FDIC Sensitive Information, PII, and FDIC computer resources. Connecting to wireless networks while traveling internationally may give unauthorized parties access to your mobile device.

Here are important tips for protecting information systems while working outside the office:

- Employees are prohibited from taking FDIC-issued equipment outside of the United States without pre-approval from management.
- Always maintain possession of your laptop and other mobile devices.
- Protect all FDIC records and data against unauthorized disclosure, access, and destruction.

As stated in the FDIC Directive 1300.04 – Information Technology Acceptable taking FDIC-furnished IT equipment outside of the United States is prohibited unless authorized by the appropriate Division/Office Director (or delegate). If needed, users can obtain authorization by submitting a CIOO Services Portal International Service Request.

Report a loss or theft of your laptop or other government-furnished devices immediately to the CIOO Service Desk.

## Conclusion

### Course Summary

In this course, you learned how to protect and maintain the Confidentiality, Integrity, and Availability of the FDIC's network, systems, software, and data. By completing this training, you have gained the knowledge to be able to identify:

- Cybersecurity, Privacy, Sensitive Information (SI), and Personally Identifiable Information (PII)
- Cyber-threats and Privacy risks
- Laws, regulations, policies, and directives that govern Cybersecurity and Privacy
- Methods used to protect the FDIC's Information throughout the Information Lifecycle
- How to provide continuous protection of the FDIC's Information

### Course Completion

Congratulations! You have completed this course.