DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

Department of the Navy (DON) Annual Privacy Training

Introduction

"As the Department of the Navy's senior official for privacy, reducing the loss, theft or compromise of personally identifiable information (PII) is one of my top priorities. This training will provide you with the information necessary to better manage DON PII. I urge you to understand and apply the DON policy and best practices presented here and use the resources available on the DON CIO website. Safeguarding PII is an all-hands effort."

- Rob Foster, Department of the Navy Chief Information Officer

Introduction

In the 1970s, concerns over the quantity of information collected about individuals by the U.S. Government received a lot of public attention. Congress believed it was important to stop unwarranted collection of personal information by the government and to properly protect the personal information that is collected. As a result, the Privacy Act of 1974 was enacted.

Introduction

The Privacy Act has four basic objectives:

- **To restrict disclosure of PII;**
- **To grant individuals access to records maintained on themselves;**
- **To grant individuals the right to correct records that are not accurate, relevant, timely, or complete; and**
- **To establish a code of "fair information practices" to regulate the collection, maintenance, use, and dissemination of PII on individuals.**

Introduction

In other words, as an individual you have rights. You have the right to know what information is collected about you, how it will be used and by whom, to have it corrected if it is wrong, and to have it protected from unauthorized disclosure to others.

As DON military, civilian and contractor personnel you also have responsibilities:

- **To only collect and maintain PII about individuals when authorized to do so;**
- **To only collect the information that is necessary;**
- **To inform individuals of the authority to collect their information, the principal purpose or use(s) for the collection, to whom it will be disclosed, and the effects on the individual for refusing to provide the information. This is accomplished by providing a Privacy Act Statement, to the individual at the time of collection.**

Introduction

You are also responsible for:

- **Ensuring that the information maintained is accurate, relevant, timely and complete;**
- **Ensuring that PII collected and maintained by the DON is kept confidential and is protected against misuse; and**
- **For knowing what to do if you suspect misuse or if there is a potential or actual compromise of PII.**

Introduction

The Department of Defense (DoD) and the Secretary of the Navy have issued guidance to clarify these rights and responsibilities, and to establish privacy programs to ensure that all of the requirements are met. The DON Privacy Program affirms that it is the Department's policy that an individual's privacy is a personal and fundamental right that should be respected and protected. Further, DON personnel, including contractors, have a responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating PII about an individual. Failure to properly safeguard PII may result in criminal or civil penalties.

Did you know? The DON CIO is the Senior Component Official for Privacy (SCOP) and oversees the Department's Privacy Program.

Introduction

Dramatic changes in information technology (IT) have taken place over the past few decades. The digital landscape has evolved and grown well beyond what was considered when the Privacy Act was enacted. Advances in IT capabilities make it possible to generate and maintain significantly greater quantities and increasingly diverse and sensitive types of information. PII may include unique identifiers such as name, date of birth, Social Security Number (SSN), DoD ID number, DoD Benefits number, geographic location information and biometrics.

Introduction

In today's data-driven world, it is necessary for the Navy and Marine Corps to collect, maintain, and use unprecedented volumes of PII. However, there are risks associated with maintaining this information. The evolution of the digital landscape, giving us easier access to a greater volume of information, increases the risk of unauthorized access to, unauthorized disclosure or use of, and loss of PII (also known as a breach). This requires the DON to take new and more aggressive approaches to both preventing and responding to breaches of PII.

Introduction

Several Federal agencies have experienced high profile breaches affecting thousands of employees. One of the most notable breaches occurred in June 2015. The Office of Personnel Management (OPM) discovered that the background investigation records of current, former, and prospective Federal employees and contractors had been stolen. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the SSN's of 21.5 million individuals, was stolen from the background investigation databases.

Introduction

To adequately protect PII, you must first understand what PII is. The term PII refers to any information about an individual, including but not limited to, education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, SSN (either full or truncated), date and place of birth, mother's maiden name, address, phone number, biometric information, or any other personal information that can be linked to an individual. This information needs to be protected, because, if compromised, an individual may be put at risk. The compromise of PII can result in embarrassment, inconvenience, reputational harm, financial harm, lower morale, an increased risk to personal security, and identity theft.

Introduction

Identity theft is a significant problem in the United States. Identity thefts represented 16% (490,220) of the over 3 million complaints received by the Federal Trade Commission (FTC) in 2015 and in 2014, 17.6 million individuals, or 7% of all U.S. residents age 16 or older, were victims of one or more incidents of identity theft.

Introduction

Perhaps more alarming is that the risk of harm to individuals in today's data-driven economy goes well beyond financial identity theft. Today, malicious actors use stolen PII to create driver licenses, passports, health insurance identification cards, permanent resident cards, and other high-quality identity document forgeries that may then be used to:

- **obtain prescription drugs;**
- **receive medical treatment;**
- **travel internationally;**
- **obtain a job;**
- **claim benefits, such as unemployment;**
- **file false tax returns to claim a refund;**
- **obtain authentic government credentials; and**
- **aid in criminal activities.**

Introduction

Additionally, identity theft can result in embarrassment, inconvenience, financial loss, reputational harm, unfairness, and in rare cases risk to personal safety.

Tip: If offered credit monitoring and you do not already have it, take it. Be proactive by monitoring your bank accounts and credit reports yourself.

Introduction

There are many ways that a breach can occur. A breach may occur as a result of human error; intentional, unauthorized disclosure by employees with access to information; or theft by external attackers. Most occurrences result from human error. Knowing what the risks are, and following guidelines and procedures to protect against those risks, is essential to reducing the number of breaches and the harm they may cause.

Introduction

One of the more common risks that we face is called “phishing.” Phishing is a criminal activity in which an adversary attempts to fraudulently acquire sensitive information by impersonating a trustworthy person or organization. Examples of phishing include manipulated emails that appear to be from government agencies, financial institutions, credit card companies, and other recognizable contacts.

The ultimate goal of phishing is to obtain personal information which can then be used to gain access to, or create new accounts.

Email Scenario

Here is a scenario for you to consider. In this scenario you will be asked to respond to various email messages.

From: no_reply@online.abcbank.com
Subject: Account Status

Received: 9:15 am

Dear ABC Bank Customer,

Due to recent suspicious online activity, we have temporarily prevented access to your account. ABC Bank safeguards your account when there is a possibility that someone other than you attempts to sign on. You may be getting this message because you signed in from a different location or device. If this is the case, your access may be restored when you return to your normal sign on method.

For immediate access, you are required to follow the instruction below to confirm your account in order to secure your personal account information.

- ***Please respond to this message with:***
- ***User name***
- ***Password***
- ***Social Security Number***

Regards, Carter Franke
Chief Customer Service Officer - Card Member Services

How would you respond to this message?

A. Reply with requested personal information
B. Reply with only user name and password
C. Report the suspicious email to your system administrator or security officer.
D. Ignore the email and delete it from your inbox

Answer

The correct answer is "C".

This is a phishing attempt. Requests to verify your account, password, or provide PII are red flags which should alert you to these scams. You should never answer any email that attempts to collect PII and other critical information unless the email has been authenticated. Legitimate financial institutions will never ask for this information via email. You could also contact your bank to alert them to the scam.

Summary

Learn to recognize red flags such as:

- unknown sender;
- misspelled words and poor grammar;
- urgent sensational subject lines;
- promises of financial gain, gifts, or prizes;
- requests to verify your password or account.

Tip: Did you know many cyber hacking attacks start with a phishing email attempt?

Email Scenario Part 2

From: cdr.smith32@navy.mil
Subject: Recall Roster

AllPers,

Review your information on the attached recall roster and let me know if it requires updating.

Thanks,

CDR Smith

Click "View attachment" to view recall roster spreadsheet, which includes SSN, name, email, home phone, and home address.

Email Attachment (Recall Roster)

SPREADSHEET - RECALL ROSTER

	A	B	C	D	
1	**SSN**	**Name**	**Email**	**Home Phone**	**Home Address**
2	698-03-XXXX	George Washington	george.washington1@navy.mil	703-789-1127	3200 Mount Vernon Hwy,
3	227-66-XXXX	John Adams	john.adams2@navy.mil	567-220-6365	1250 Hancock Street Quin
4	212-31-XXXX	Thomas Jefferson	thomas.jefferson3@navy.mil	774-930-8899	931 Thomas Jefferson Pkv
5	229-13-XXXX	James Madison	james.madison4@navy.mil	703-622-1987	11350 Constitution Hwy, C
6	034-64-XXXX	James Monroe	james.monroe5@navy.mil	703-695-1892	2050 James Monroe Pkwy
7	691-03-XXXX	John Quincy Adams	john.q.adams6@navy.mil	571-202-1367	141 Franklin Street, Quinc
8	696-03-XXXX	Andrew Jackson	andrew.jackson7@navy.mil	571-657-1134	4580 Rachels Ln, Hermitag
9	695-03-XXXX	Martin Van Buren	martin.v.buren8@navy.mil	703-994-1874	1013 Old Post Rd, Kinderh
10	691-05-XXXX	William Henry Harrison	william.h.harrison9@navy.mil	703-867-8917	1230 N Delaware St, India
11	348-86-XXXX	John Tyler	john.tyler10@navy.mil	571-765-5566	14501 John Tyler Memoria
12					

Sheet1

Does this represent a PII breach?

A. Yes

B. No

Answer

The correct answer is "Yes!"

CDR Smith sent an unencrypted email containing PII to you and other employees, many of whom did not have a "need to know." A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or has the ability to access personally identifiable information or (2) a person accesses personally identifiable information for an other than authorized purpose.

Regardless of whether the information was encrypted or not, individuals who do not need to use PII in the performance of their official duties should never have access to someone else's PII.

What should CDR Smith have done to prevent this PII breach?

A. CDR Smith should have labeled the email attachment with the privacy warning "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties."

B. CDR Smith should not have sent an unencrypted email containing everyone's PII to individuals who did not have a need to know.

C. CDR Smith should not have sent an unencrypted email containing PII via email.

Answer

The correct answer is "B." CDR Smith should always send PII in a digitally signed and encrypted email and should never send PII to recipients that do not need to know the information for the performance of their official duties.

Remember: Sending an email containing PII is acceptable if the proper controls are in place.

- **Before sending an email ask the question "Do the recipients have a need to know?"**
- **Official emails containing PII must be digitally signed and encrypted.**
- **All electronic or paper copies of documents containing PII must be marked with the following: "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties."**

What action should you take first?

A. Delete the message.

B. Reply to CDR Smith.

C. Upon discovery and within one hour, contact your privacy official or supervisor to report the breach.

D. Contact the U.S. Computer Emergency Response Team (CERT)

Answer

The correct answer is "C." Within one hour of the discovery of a loss or suspected loss of PII, notify your supervisor or privacy official, who will initiate the PII breach reporting process.

You should not delete the message, as DON personnel who discover known or suspected losses of PII must report the breaches to their supervisors or privacy officials.

You should not delete the message until you have properly reported the breach and been directed to do so. You should also not contact the U.S. CERT Office directly. The U.S. CERT Office will be contacted, if necessary, during the PII breach reporting process.

Email Scenario Part 3

From: pat.z.anderson@navy.mil
Subject: Overseas Travel Form

Received: 7:22 am

Good afternoon,

I was informed by your manager that you will be taking an overseas trip soon. For security purposes, please fill out the attached form and return it to me as soon as possible.

Thank you,

Pat Anderson

Department of Human Resources

Click "View attachment" to view form.

Tip: Always check to see if the attachments you are sending contain PII. Remember to check all tabs and hidden fields when sending spreadsheets

Email Attachment (Travel Form)

DON OFFICIAL FORM

NOTIFICATION of UNOFFICIAL PERSONAL FOREIGN TRAVEL

Government or Military

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. §§ 5701-5757, Travel, Transportation, and Subsistence; 10 U.S.C. § 135, Under Secretary of Defense (Comptroller); 10 U.S.C. § 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. § 3013, Secretary of the Army; 10 U.S.C. § 5013, Secretary of the Navy; 10 U.S.C. § 8013, Secretary of the Air Force; DoD Financial Management Regulation 7000.14-R, Vol. 9, Travel Policies and Procedures; and E.O. 9397 (SSN) PRINCIPAL PURPOSE: This form is used by military personnel, Department of Defense civilian and contractor personnel, collectively referred to as civilians, when applicable. This form provides visibility and initiates travel processes required to properly prepare personnel for travel outside of the continental United States. ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To Federal and private entities providing travel services for purposes of arranging transportation and lodging for those individuals authorized to travel at government expense on official business. To the Internal Revenue Service to provide information concerning the pay of travel allowances which are subject to federal income tax. The DoD 'Blanket Routine Uses' set forth at the beginning of the DoD compilation of systems of records notices apply to this system. DISCLOSURE: Disclosure of requested information is voluntary, however, failure to provide such information may result in a delay of your processing and travel documentation.

TRAVELER INFORMATION

NAME (Last, First, MI)	EDIPI	COMPETENCY	WORK PHONE #	PASSPORT #

Do you have SCI access? ☐ YES ☐ NO

HOME ADDRESS (Street, City, St, Zip)	HOME PHONE #	CELL PHONE #

SUPERVISOR NAME (Last, First, MI)	SUPERVISOR PHONE #

EMERGENCY CONTACT INFORMATION

Person with knowledge of your travel and whereabouts, who you will contact in an emergency.

NAME (Last, First MI)	RELATION TO YOU	WORK PHONE #	HOME PHONE #	CELL PHONE #

TRAVEL INFORMATION

COUNTRIES TO BE VISITED	MAJOR CITIES	DATE FROM	DATE TO

What action should you take first?

A. Report the email to your supervisor or privacy official.

B. Consult with your command forms manager/admin office or visit the Naval Forms Online website to verify this is an approved form.

C. Complete the form and send it back.

D. Delete this email.

Answer

The correct answer is "B." This is a legitimate request for information from a person with a need-to-know, therefore you do not need to alert your supervisor or privacy official, and a response is appropriate.

However, it is always a good idea to verify any form you are asked to complete. You should ensure you have the most recent version of any official form before providing your PII. Visit the Naval Forms Online website for a list of approved Naval forms. Remember to encrypt and digitally sign all emails containing PII.

Please select all proper controls for sending PII:

A. The recipient has an official “need-to-know”
B. The email message is digitally signed
C. The email message is encrypted
D. The body of the email, including any email attachments containing PII, are marked properly (i.e., "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.")
E. The email subject line contains "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE" (a best practice)

Answer

The correct answer is "ALL." All the controls mentioned must be in place before sending PII via email.

Work Space Scenario

Recent PII breach reports highlight the need to conduct searches of shared drives throughout the Department to protect employees' PII and reduce the risk of identity theft. PII is found most often in documents related to awards, employment information, performance evaluations, legal documents, medical records, and financial data.

Scanning software detected files that contained PII in an unprotected folder.

To prevent a future breach of this kind, what controls should be put in place? Check all that apply:

A. Files that actually contain PII should be password protected.

B. Access to any folders that contain PII should be restricted to only those with an official need-to-know.

C. Determine which documents need to be retained, and when and how to dispose of those documents when they are no longer required.

D. Any documents containing PII should be deleted immediately.

Answer

The correct answers are A, B, and C." The controls mentioned must be in place before storing PII on a shared drive. If you ever discover files containing PII, and you are not in a position with an official need-to-know, you should report this to your privacy official immediately.

Ensure shared drive access permissions are established and routinely checked. Shared drives are useful tools to store and share information, but they must be properly managed to ensure personnel understand that indiscriminate posting of PII is not authorized. When there is a need to post PII to a shared drive, access to those files must be strictly controlled and routinely monitored for compliance. Problems often occur when network maintenance causes the removal of access controls.

Objects Around the Office Where PII May be Mishandled

Recycling Bin:

- Whenever disposing of PII, always use a burn bag or an approved shredder. Never use a trash can, recycling bin, or dumpster.

Objects Around the Office Where PII May be Mishandled

Fax Machine:

Faxing is one of the least secure means of transmitting information. It often results in the disclosure of PII to personnel who do not have an official need to know.

The use of fax machines to send information containing Social Security Number and other PII to DON personnel is prohibited except under the following circumstances:

- **When another more secure means of transmitting PII is not practical.**
- **When a process outside of DON control requires faxing to activities such as the Defense Finance and Accounting Service (DFAS), TRICARE, Defense Manpower Data Center (DMDC), etc.**
- **In cases where operational necessity requires it.**
- **When faxing PII related to internal government operations only, i.e., office phone number, rank, job title, etc., also called "Rolodex PII."**

Objects Around the Office Where PII May be Mishandled

Desk:

- Leaving a document containing PII in an open area is a breach.
- When hand-carrying documents containing PII it is a best practice to use a Privacy Act Data Cover Sheet (DD Form 2923).

Objects Around the Office Where PII May be Mishandled

Office Bulletin Board (with a recall roster containing SSN posted):

When creating and sharing a roster of any kind (social, recall etc.):

- Wherever the roster is posted or stored, only those with a need to know should have access.
- Is the information appropriately marked "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.“?
- Limit the collection of PII to the minimum number of elements required to get the job done.
- SSNs, full or truncated, should never be included.
- Provide a Privacy Act Statement any time PII is solicited from an individual, whether in writing or electronically. Contact your Privacy Official for more information.

Objects Around the Office Where PII May be Mishandled

Office Co-Worker:

The following conversation is overheard:

"Hi there! Did you hear that Susan from the Cybersecurity Team is being reprimanded by her supervisor for being constantly late to work?

Response: "No, how did you find that out?"

Person: "I work in the front office, and have access to the boss's email."

This type of breach is referred to as improper disclosure. Both accidental and improper disclosure of PII can result in legal action or other discipline. You should report this conversation to your supervisor or privacy official.