CANADIAN FREQCOORD
UNCLASSIFIED SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: The Computer Fraud and Abuse Act, as amended (18 U.S.C. § 1030) authorizes collection of the following information.

PRINCIPAL PURPOSE: To record names, signatures, and other identifiers to validate the trustworthiness of individuals requesting access to the National Telecommunications and Information Administration (NTIA) systems and information. The requestor information will be stored in electronic or paper form.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information will prevent the processing of this request.

TYPE OF REQUEST	**DATE (DDMMYYYY)**
☐ INITIAL ☐ MODIFICATION ☐ RENEWAL ☐ DELETION	

PART I (*To be completed by User*)

1. NAME (LAST, FIRST, MI)	**2. TITLE**
3. AGENCY / COMPANY	**4. OFFICE**
5. MAILING ADDRESS	

6. PHONE	**7. FAX**	**8. EMAIL**

9. PHONE NUMBER(S) FOR AUTHENTICATION:

Primary Phone number _____ Alternate Phone Number _____

STATEMENT OF ACCOUNTABILITY

I understand my obligation to protect my password and user credentials. I have reviewed and will abide by the NTIA FREQCOORD System Rules of Behavior and protect the data and the integrity of this system. I will not exceed my authorized access. I acknowledge that all documents, unless otherwise marked, are to be treated at a minimum as pre-decisional, sensitive information and cannot be released without the expressed written consent of the Associate Administrator, Office of Spectrum Management, National Telecommunications and Information Administration. I have read; I understand; and I will follow the NTIA FREQCOORD Rules of Behavior and the Security Awareness training slides attached to this request form.

USER SIGNATURE	**DATE (DDMMYYYY)**

PART II (*To be completed by Canadian Government Spectrum Office*)

10. IS THE USER A CANADIAN GOVERNMENT EMPLOYEE?

☐ Yes ☐ No

11. CONTENT ACCESS REQUIRED

☐ FREQCOORD (Read Only)

(FREQCOORD SAAR/ROB version 1.0 created on 9/7/2017)

12. JUSTIFICATION FOR ACCESS

VERIFICATION OF NEED TO KNOW

I certify that the requestor requires access to FREQCOORD in the performance of his/her job function.

CANADIAN GOVERNMENT SPECTRUM OFFICE SIGNATURE	DATE (DDMMYYYY)

PART III (*To be completed by the FREQUENCY ASSIGNMENT BRANCH CHIEF)*

13. HAVE THE USER'S CREDENTIALS BEEN VERIFIED?

☐ YES ☐ NO

FREQUENCY ASSIGNEMENT BRANCH CHIEF VERIFICATION

I have verified that the requestor requires access to the FREQCOORD system as indicated in Part III of this form.

SIGNATURE OF BUSINESS OWNER	DATE (DDMMYYYY)

PART IV (*To be completed by FREQCOORD System Administrator)*

14. USERID	15. USER CONTEXT	16. ACCOUNT EXPIRATION

SIGNATURE OF SYSTEM ADMINISTRATOR	DATE (DDMMYYYY)

INSTRUCTIONS

NOTE: All requestors MUST read the "Privacy Act Statement" on the top of the form, the "Statement of Accountability" above the user signature block, and the attached "System Rules of Behavior" before signing this SAAR form.

TYPE OF REQUEST: Place an "X" in the appropriate box.
DATE: Enter the date in DDMMYYYY format.

A. PART I: The requesting user must provide the following information for establishing or modifying a user account:

Block 1 – NAME: The last name, first name, and middle initial of the user.
Block 2 – TITLE: The user's job function title (*i.e.*, Electronics Engineer).
Block 3 – AGENCY/COMPANY: The user's current Agency or Company name.
Block 4 – OFFICE: The member's office/division/branch (*i.e.*, Army Spectrum Management Office).
Block 5 – MAILING ADDRESS: The user's complete mailing address including mail stop, street, city, state, and zip code.
Block 6 – PHONE: The user's direct voice telephone number including area code.
Block 7 – FAX: The user's facsimile phone number including area code.
Block 8 – EMAIL: The user's email address.
Block 9 – PHONE NUMBER FOR AUTHENTICATION: The user's phone number for the system to call for authentication. The user will be required to enter an access control number or PIN.
USER SIGNATURE: User must sign the SAAR form with the understanding that he/she is responsible and accountable for his/her password and PIN, abiding by the system Rules of Behavior, and for protecting the content and integrity of the system. (the form may be signed electronically)
DATE: Date the form signed using DDMMYYYY format.

The requestor must forward the form to Canadian Spectrum Management Office.

B. PART II: The Canadian Government Spectrum Management Office must provide the following information:

Block 10 – IS THE USER A CANADIAN GOVERNMENT EMPLOYEE? Place an "X" in the appropriate box.
Block 11 – CONTENT ACCESS REQUIRED: Place an "X" in the appropriate boxes.
Block 12 – JUSTIFICATION FOR ACCESS: A brief statement to justify establishment of an initial user account. Provide appropriate information if the account is to be modified, renewed or deleted.
SIGNATURE: Only the Canadian Government Spectrum Management Office can sign the form affirming the user's requirement for access to the FREQCOORD.
DATE: Date the form using DDMMYYYY format.

The Canadian Government Spectrum Management Office must forward original forms to the NTIA FREQUENCY ASSIGNMENT BRANCH CHIEF and should maintain a copy.

C. PART III: The Business Owner must provide the following information:

Block 13 – HAS THE USER'S MEMBERSHIP STATUS BEEN VERIFIED? Place an "X" in the appropriate box.
BUSINESS OWNER'S VERIFICATION: The business owner must sign verifying the requestor's need for access to the content on FREQCOORD.
DATE: Date the form in DDMMYYY format.

The business owner must forward original forms to the NTIA Helpdesk with a request for an FREQCOORD user account and maintain a copy.

D. PART IV: The System Administrator must provide the following information:

Block 14 – USERID: Enter the authorized user identity (*e.g.*, jdoe).
Block 15 – USER CONTEXT: Enter the user's role in the system.
Block 16– ACCOUNT EXPIRATION: Enter the account expiration date in DDMMMYYYY format.
SIGNATURE OF SYSTEM ADMINISTRATOR: The system administrator must sign the document certifying that the user account was established in accordance with system policies and that access is restricted to the content indicated in Part III.
DATE: Date the form in DDMMYYYY format.

The system administrator must forward the original forms to the IT Security Officer and maintain a copy.

NTIA FREQCOORD
System Rules of Behavior

The purpose of the FREQCOORD Rules of Behavior is to increase individual awareness and responsibility and to ensure that all users utilize Department of Commerce (DOC) and National Telecommunications and Information Administration (NTIA) Information Technology (IT) resources in an efficient, ethical, and trustworthy manner. The Rules of Behavior that are understood and followed help ensure the security of the FREQCOORD system and the confidentiality, integrity, and availability of NTIA information. These rules apply to users at their primary workplace and at any alternative workplaces (e.g., teleworking from home or from a satellite site). They also apply to users on official travel. All FREQCOORD users must read and acknowledge the Rules of Behavior to receive access to the FREQCOORD. Failure to abide by these rules may constitute grounds for termination of access privileges, administrative actions such as disciplinary actions, and/or criminal prosecution, if warranted.

I understand that I must read and acknowledge the Rules of Behavior to receive access to the DOC and NTIA IT resources. I agree to comply with all DOC and NTIA IT policies and procedures to include the following:

1. I will only use my authorized user identity (ID) and will not divulge my user ID. I will protect passwords, and PINs, from disclosure. I will not share passwords or PINs. I will not record user IDs, passwords, or PINs on paper or in electronic form on unencrypted workstations, laptop computers, or portable electronic devices.
2. I consent to monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for NTIA IT resources. I understand that I have no expectation of privacy while accessing the FREQCOORD or other DOC and NTIA IT resources.
3. I am responsible for protecting and maintaining, to the best of my ability, any information used or stored in my accounts. I will safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
4. I will properly handle and protect the information on this system.
5. I will cooperate with designated personnel during investigations of incidents, compliance reviews, audits, and surveys.
6. I will log off or lock my workstation or laptop whenever I step away from my work area. I will log off from the system when I leave for the day.
7. I shall complete the annual security & privacy awareness training.
8. When I no longer require access to FREQCOORD, I will inform the Canadian Spectrum Management Office Representative and make no further attempt to access these resources.
9. I will report immediately to the NTIA Help Desk, at ntiahelpdesk@ntia.doc.gov or (202) 482-4631, all FREQCOORD-related security incidents to include the loss, theft, or compromise of the FREQCOORD system.

IT Security Awareness
For FreqCoord Canadian Users

Prepared by NTIA Information Assurance Branch
Based on DOC Security Awareness Training

October 2017

Training Objectives

- To protect FreqCoord system and the NTIA network
- To educate FreqCoord users on basic security precautions and cybersecurity best practices
  - Ransomware
  - Phishing attack
  - Social Engineering
  - Identity Theft
- To educate FreqCoord users on the objectives of the Privacy Act

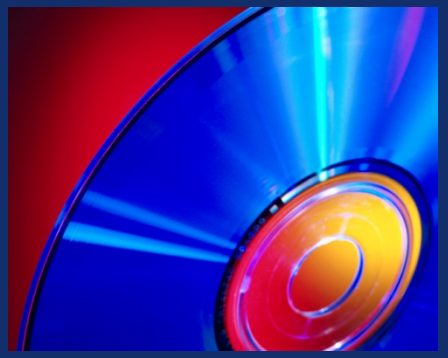
Basic Security Objectives

U.S. Federal Information Security Modernization Act (FISMA) defines three security objectives for information and information systems:

- Confidentiality – protecting information from unauthorized disclosure to individuals or systems
- Integrity – protecting information from unauthorized changes
- Availability – ensuring IT assets are functioning correctly and accessible when needed

What Needs to be Protected?

- IT Assets include:
  - People
  - Hardware
  - Software
  - Data
  - Infrastructure
  - Facilities



Some security Threats: Ransomware

- Ransomware is a new type of attack that denies access to your computer or files until you pay a ransom, usually in BitCoin or other hard to trace cryptocurrency.
- Cryptolocker, WinLock are types of this attack
- Ransomware usually enters a system via downloaded files or network vulnerabilities

Ransomware (continue)

- Once on a user system, it encrypts the user's files and spreads over the LAN/WAN to infect as many systems as possible.
- The user then is denied access to their files and is presented with a screen demanding a ransom be paid in Bitcoins in a certain period of time or the files would be forever lost.

Some Security Threats: Phishing

- Phishing uses fraudulent email to lure unsuspecting users into providing unauthorized access to personal information, communications, and/or computer systems
  - Phishing uses social engineering and email spoofing tricks
- Spear phishing – focused attack
- Whaling – targeted attacks at senior executives within an organization
  - The most common whaling techniques involve emails purportedly sent from one member of the executive management team to another

Voice Phishing

- Cybercriminals use a combination of SMS and voice phishing techniques to obtain debit card details
  - Bank customers received text messages claiming their debit cards have been deactivated and instructing them to call a phone number
  - An Interactive Voice Response (IVR) system asked callers to input their debit card and PIN numbers to reactivate the card
  - An estimated 250 cards per day were stolen via this phishing campaign

Tips to Thwart Phishing Attempts

- Be suspicious of ***any*** official-looking e-mail message that asks for updates on personal or financial information
- Avoid clicking links in e-mails, especially any that are requesting private information
- Never send passwords, bank account numbers, or other private information in an e-mail
- Be wary of any unexpected e-mail attachments or links, even from people you know
- Look for 'https://' and a lock icon in the address bar before entering any private information
- Keep your anti-virus program updated and ensure that it can scan e-mail

- **If you suspect you have been phished, call your help desk**

Some Security Threats: Social Engineering

Social Engineering is:

- Defined as “the act of manipulating a person to accomplish goals that may or may not be in the “target’s” best interest
  - This may include obtaining information, gaining access, or getting the target to take certain action
- A hacker’s clever manipulation of the natural human tendency to trust

Goals of Social Engineering

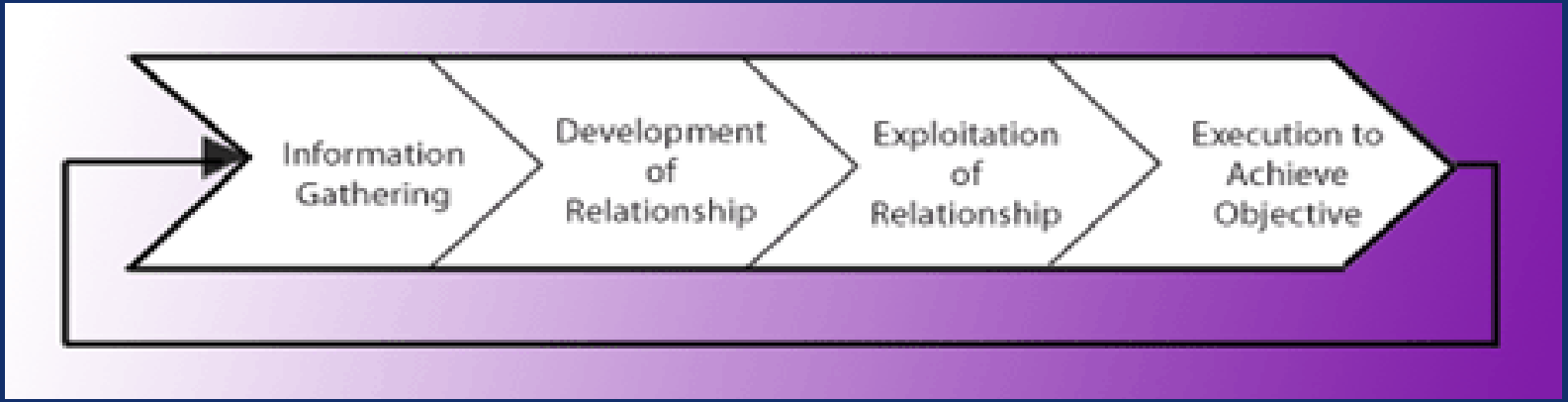
The basic goals of social engineering are to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network

Social Engineering– Requests for Information

- Your phone rings, and the pleasant individual asks if you have a few minutes to answer a couple quick questions
  - What should you do?

- A web site requires you to fill out a form identifying the IT hardware and software systems in use within your organization prior to downloading a hot-off –the press report on a current topic
  - What should you do?

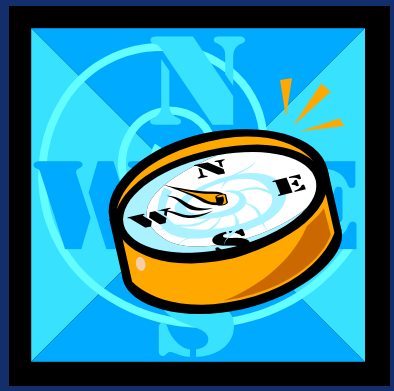
Social Engineering Attack Cycle



- **Info Gathering:** Attackers use a variety of techniques to gather info about their target
- **Development of Relationship**: Attackers exploit the tendency to trust to develop a rapport with their targets
- **Exploitation of Relationship**: Attacker exploits the target into revealing information or performing an action that would not normally occur
- **Execution to Achieve Objective**: Attacker executes the cycle to obtain the end objective, combining methods and information gathered

Social Engineers use Adaptive Attacks

- Playing the authority
- Playing someone in need
- Identity theft
- Maintenance and support
- Malicious software
- Reverse social engineering
- Research



Tips to Prevent Social Engineering

Never give out:

- Usernames; Administrators should know it or can find out themselves
- Passwords; Administrators can ask your to enter it into the computer, but don't tell anyone
- ID numbers
- PIN numbers
- Server names
- System information
- Credit card numbers
- Schedules
- Sensitive data

Tips to Prevent Social Engineering – Be Wary of What is Being Asked

Via the Phone:

- Ask for a full and correct spelling of the caller's name, a call back number, and why they need the information
- Have the caller contact the correct information source directly if you are asked for information managed by someone else
- When in doubt, put the caller on hold or tell them you will call them back. This gives you time to log any strange calls and verify if it is ok to give out information.

Tips to Prevent Social Engineering – Be Wary of What is Being Asked

Via the internet

- Watch for any attachments that someone wants you to run in an e-mail
- Avoid any requests to enter account information for verification by following a link in the e-mail (this is known as *phishing*)
- Administrators will never tell you passwords over e-mail
- When in doubt, you can also contact the e-mail sender in a phone call or new e-mail and ask if their e-mail with the subject of <copy the subject> was valid

More Tips to Prevent Social Engineering

In person

- Never be pressured to comply when someone says "Do you know who I am?"
- Ask for a contact to verify the person's need for information
- Have someone asking for configuration/access questions to contact the source directly
- Someone from should only need you to enter your username/password on the computer; not write it down or verbally say it
- Always be aware of people around you when entering your username/password

Mobile Devices and Social Engineering

- Email hoaxes and scams are appearing on mobile devices
  - Free iPad giveaway promos infected systems with malware
  - Twitter span spouting free McDonald's gift cards redirected users to adult dating sites
  - Pintrest users "repinned" a Starbucks logo to get supposed gift cards but instead got malware

Social Engineering – The Bottom Line

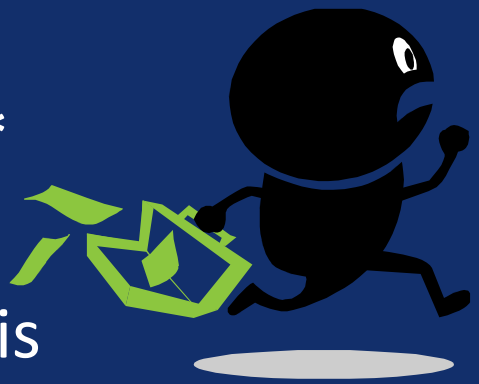
Malicious individuals have always known that the best way around any security system is to manipulate a human target into giving them what they want – what we call social engineering. It remains the single greatest security threat to enterprises.

Some Security Threats: Identity Theft

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else

The Losses are Enormous

- Approximately 15 million United States residents have their identities used fraudulently each year with financial losses totaling upwards of $50 billion.*



- A substantial portion of identity theft is committed by those the victim knows personally or has invited into their home to perform services

Identity Theft – Credit and Debit Cards

- Credit card skimming is common and can occur at
  - ATMS (Use an ATM inside a retail outlet)
  - Gas Pumps (Pay cash or use card inside)
  - Restaurants (Don't use a debit card)

- The "Square" designed for online payments using a smart phone, can be modified for use as a skimmer

- Don't use debit cards for online purchases

Tips to Prevent Identity Theft

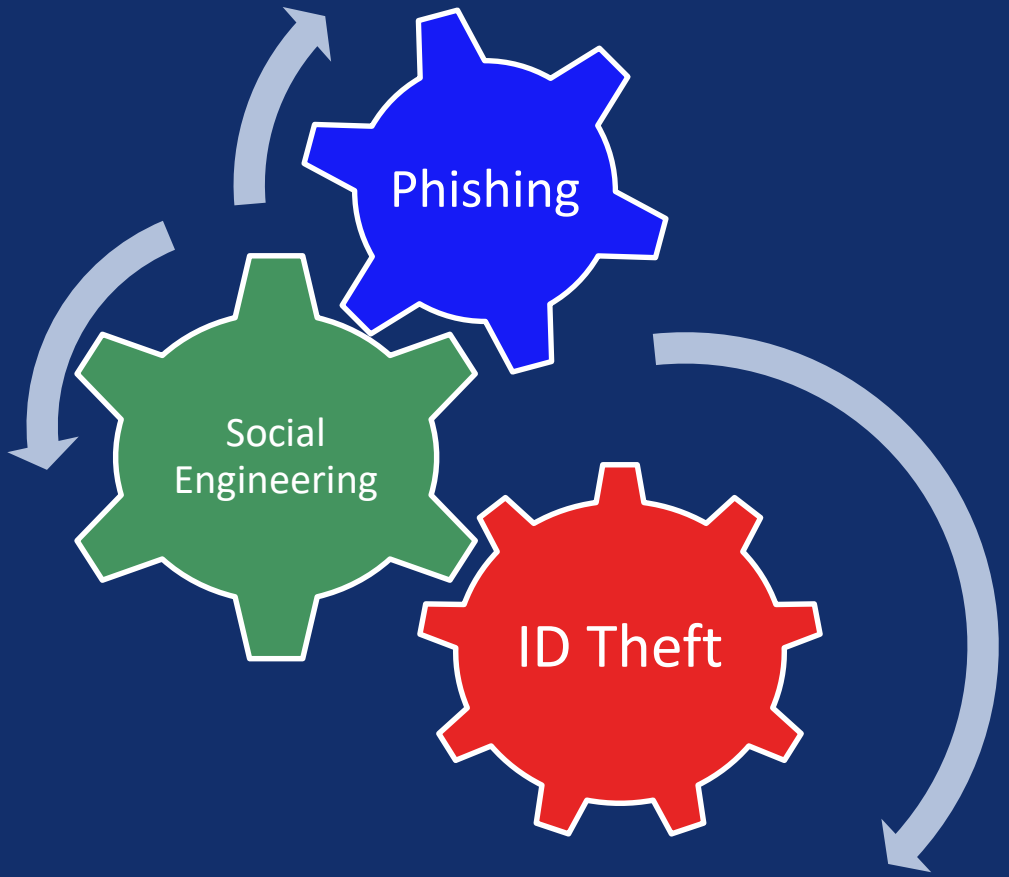
- Shred everything
- Destroy digital data
- Don’t leave important documents in your car
- On travel, never leave personal documents unsecured in hotel rooms
- Protect your Social Security number
- Beware of cleaning services, both at work and at home
- Monitor your credit report

Tips to Prevent Identity Theft

- Don’t carry your Social Security card or any documents with your SSN or Individual Taxpayer Identification Number (ITIN) on it
- Don’t give a business your SSN or ITIN just because they ask. Give it only when required
- Protect your financial information
- Check your credit report every 12 months
- Secure personal information in your home
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts
- Don’t give personal information over the phone, through the mail or on the Internet unless you have initiated the contact or you are sure you know who you are dealing with

Tying it Together

- Social Engineering and Phishing are methods of gaining access and gathering data
- ID Theft results from the use of the gathered data



Objectives of the Privacy Act (PA)

- The PA, 5 U.S.Code §552a. has been in effect since September 27, 1975.
- The purpose of the PA is to regulate the collection, maintenance, use, and dissemination of personal information held by the Executive Branch of Government.
- The PA protects personal information maintained in a PA system of records that is retrieved by a name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
- The PA is a statute that regulates the U.S. Federal Government's collection, maintenance, use and dissemination of *personal information* about U.S. citizens (and aliens lawfully admitted for permanent residence).

Privacy Act Violations

Examples:

- Knowingly releasing an individual's background investigation records improperly to any person or agency not entitled to receive them.
- Obtaining or disclosing confidential financial disclosure data under false pretenses or facilitating others acting under false pretenses.
- Discussing in a public area, information such as an individual's application for employment or performance rating.
- Sharing a payment invoice containing an individual's financial information with a person not authorized to see it.
- Maintaining a group of records about an individual that are designed to be retrieved by a personal identifier, prior to the publication in the Federal Register of a Privacy Act Systems of Record Notice (SORN) to cover the records system.

What are Your Responsibilities

- **As an employee, you play a very important role in assuring the staff members who handles Personally Identifiable Information (PII) comply with the provisions of the Privacy Act. Accordingly,**
  - **DO NOT collect personal data without authorization.**
  - **DO NOT distribute or release personal information to other employees unless they have an official need-to-know.**
  - **Use Secure File Transfer (SFT) when PII has to be transmitted electronically**

Privacy Best Practices

- **When you receive an email and it contains personal information about another individual, do not forward that document to others without first assessing whether each recipient has an official need to know.**

- **Use training to educate your personnel on Privacy.**

  - **Ensure all newly assigned personnel receive orientation training on the Privacy Act so they fully understand their role in ensuring that personal information is protected from unauthorized disclosure.**

  - **Ensure all personnel receive refresher training once a year or more often should they be involved in a breach (loss) of personal information.**

  - **Ensure all personnel who deal with personal information contained in a Privacy Act system of records are properly trained on the systems notice and the safeguards addressed therein and the restrictions regarding access to the information.**

Summary

- Doubt whatever is on the Internet
- Don’t give out personal information indiscriminately
- When in doubt about a visitor or a caller, ask the person to wait while you verify (a) identity, (b) need to know, and (c) if you are the rightful/authorized source of the information

An educated employee is our best defense!