CNCS Cybersecurity User Training

with Privacy, Phishing, and PII

CyberSecurity

Corporation for National & Community Service

Course Objectives

The objective of this training is to provide CNCS users an understanding of:

- how to protect yourself from phishing attacks,
- the importance of safeguarding sensitive and Personally Identifiable Information (PII), and
- your role and responsibilities when using PII in their daily routine.

What the Law Requires

This course focuses on responsibilities and annual training requirements mandated by the following laws:

- Federal Information Security Management Act of 2002 (FISMA)
- Privacy Act of 1974, as amended
- Freedom of Information Act (FOIA)
- Computer Fraud and Abuse Act of 1986
- Office of Management and Budget (OMB) Memoranda
- Federal Records Act of 1950

What is Phishing?

Phishing (e-mail) or SMSishing (text message) attacks seek and exploit an individual's personal information by luring or tricking them into downloading malware, and/or sending their personal information. For example:

From: Internal Revenue Service [irs-service@IRS.GOV] Sent: Tue 2/3/2009 3:55 PM
To:
Cc:
Subject: Official Notification

After the last annual calculations of your fiscal
are eligible to receive a tax refund of $92.50.
Please submit the tax refund request and allow us 3-6 days in order to process it.
A refund can be delayed for a variety of reasons. For example submitting invalid
records or applying after the deadline.

To access the form for your tax refund, please click here :

http://cimaonline.ca/form/Internal/Revenue/Service/index.html

Regards,
Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.

Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.

Protect yourself from Phishing

Use caution at all times when opening emails and clicking on links. To protect yourself:

- Be selective about what you download on your computer.
- Do not accept free-deals unless verified.
- Don't click on links sent via suspicious emails.
- Look for secure sign ('https' or a lock symbol) in the URL when accessing websites.

It is almost always a scam if the email:

- Requests personal information and directs recipients to respond through websites that seem legitimate but are not, with the threat of account being shut down, or
- Is not personalized, has poor grammar and/or has misspellings.

Report any phishing emails immediately to phishing@cns.gov.

What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) is any information about an individual maintained by an agency, including

(1) **any information that can be used to distinguish or trace an individual's identity**, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

(2) **any other information that is linked or linkable to an individual**, such as medical, educational, financial, and employment information, as defined in NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of PII*.

Aggregated Sources for PII

Sometimes information combined from multiple sources enables an attacker to successfully distinguish and establish your identity, even though these pieces of information may not individually trace back to you. Some examples are:

Website or platform related

- IP address
- Cookies
- Login name, screen name, nickname & Password
- Form data such as email address, first & last names, address

Device related

- Unique device identifier
- Location/GPS data
- Contact list or directories
- SD card or other stored data
- Network communications data

Third-party related

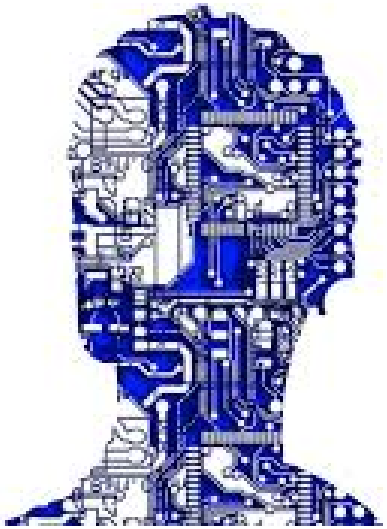
- Health, insurance, treatment, or medical information
- Criminal history

… And so on.

What can attackers do with PII?

Data collected from or about individuals by the third party may be combined with or imported into other databases to create more detailed profiles of individuals without their knowledge or consent.

Using these profiles, hackers, foreign intelligence, organized crime, and others seek to exploit vulnerabilities in devices, networks, or programs to target you so that they can obtain unauthorized access to information.



What is a PII breach?

"The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic."

- OMB Memorandum M-07-16, *Safeguarding and Responding to the Breach of Personally Identifiable Information*.

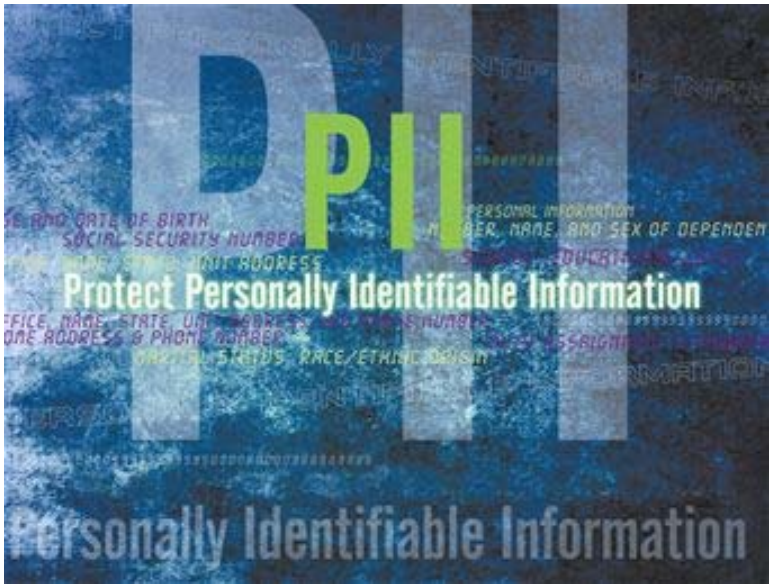
Why do we need to protect PII?

Once attackers have access to your information, they can commit some real-world crimes like:

- Engage in fraud that can cause substantial financial damage
- Issue threats, and/or harassment
- Install malware on your devices to track you further and target your associates
- Plan and/or commit terrorist or other criminal acts
- Obtain national security intelligence and security measures

User Responsibilities to Safeguard PII

- Transfer PII to mobile devices that are encrypted, and only when there is a legitimate business need.
- Do not place Agency's privacy or sensitive data on a personal computer or personal mobile devices.
- Access PII through VPN when teleworking to ensure protection of information from inadvertent viewing over the network.
- Know that sharing PII to others who do not have a legitimate need to know, and who would not have access to this information otherwise, is a violation of law.
- Only keep PII for the length time needed to perform your business functions.



User Responsibilities to Safeguard PII (cont.)

- Use Secure File Transfer when sending PII or other sensitive information electronically.
- Remove paper documents containing sensitive information from printers or fax machines immediately after use and store securely. Utilize locked shredder bins to dispose.
- The longer it takes to report an incident, the greater the risk is of a loss or breach of information. CNCS is required to report within 1 hour from when the breach occurs, so your timely reporting of the incident is essential.

Lock your machine

Lock your computer when you are away from your desk.

When you leave, you may be logged into an application or system that contains sensitive data.

Do not rely on the automatic timeout to lock your system.

If you fail to protect your PC when you leave it unattended, and someone uses your account to perform unauthorized activities, **you** may be held accountable.

Getting Coffee?

Did you remember to

Lock Your Computer?

Lock your machine (cont.)

Locking your computer is simple:

- Press the Ctrl+Alt+Del keys and click "Lock this computer". When you return to your computer, simply press the Ctrl+Alt+Del keys again and type in your password to unlock the computer.
- On a Windows machine, you can hit the “Windows” button and “L” to lock your machine.

Password Protection

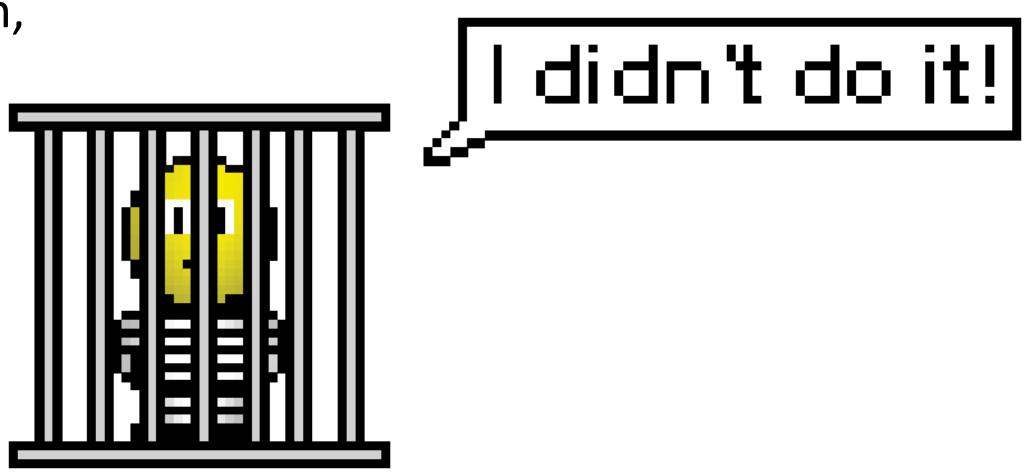
It is NOT okay to share your password…

- ***With anyone***!
- Not even your supervisor, co-workers or the Help Desk.

Consequences

If your account is misused or compromised, there can be serious and far-reaching consequences, including but not limited to:

- Disciplinary and/or legal action, including but not limited to:
  - Loss or limitation of use of information resources,
  - Termination of employment, and/or
  - Referral for criminal prosecution



Congratulations!

Congratulations! You have completed the CNCS Cybersecurity User Training. You should now have a better understanding of the following:

- how to protect yourself from phishing attacks,
- the importance of safeguarding sensitive and Personally Identifiable Information (PII), and
- your role and responsibilities when using PII in their daily routine.

To finish this training, you must sign the ROB.

- Print and sign the signature page of the ROB.
- Scan and email it to cybersecurity@cns.gov.

By signing the ROB, you attest that you've received this training, and that you understand it completely.

POC for Questions

For questions and suggestions on this training, please contact cybersecurity@cns.gov.

To report phishing forward the message to phishing@cns.gov.

To report security, PII or other privacy breaches or incidents, please use the online form or contact the OIT Help Desk at 202-606-6600.

CYBERSECURITY | Corporation for NATIONAL & COMMUNITY SERVICE

CNCS Cybersecurity Rules of Behavior Agreement

What is the Purpose of the CS Rules of Behavior?

The intent of the CNCS Cybersecurity (CS) Rules of Behavior (ROB) is to provide guidance for all CNCS employees, contractors, interns/temporary employees, and volunteer personnel working for CNCS concerning information and personal security and to obtain written certification that personnel have read and understand these ROB. Everyone plays a major role in preventing security vulnerabilities that can lead to system compromises that hinder our mission or facilitate unauthorized disclosure of sensitive information. Each individual's actions can affect the security of CNCS information and information technology (IT) systems. Knowledgeable users are the foundation of a successful CS program.

Who is covered by these Rules?

These rules extend to all CNCS federal employees, contractors, interns/temporary employees, and volunteers using CNCS IT systems or accessing CNCS information under formally established agreements. All users must be fully aware of, and abide by, these rules and CNCS CS policies.

What is Sensitive Data?

Sensitive data is data that must be protected against loss, disclosure, or alteration because of the risk and magnitude of harm that could result. Examples include personally identifiable information (PII), procurement, budget, system/application vulnerabilities, and planning information.

What is Personally Identifiable Information (PII)?

The term PII refers to any data that could potentially identify a specific individual, either by itself or when combined or linked to other identifiable information. PII must be protected from disclosure. The following are examples of PII:

- Name and any associated data
- Non-Business Phone Numbers, emails, and addresses
- Social Security Number
- Date and Place of Birth
- Fingerprints
- Photos
- Mother's Maiden Name
- Passport Number
- Driver's License Number
- Taxpayer Identification Number
- Financial Account or Credit Card Numbers

PII includes any other information that is linked or linkable to an individual's identity, such as:

- Medical
- Educational
- Financial
- Employment

Rules of Behavior

System Access:

- ☐ I understand that I will be held accountable for my actions while accessing and using CNCS systems.
- ☐ I will complete the new employee training and all other mandatory CNCS CS training within the specified timeframes. I understand that not completing the training will result in the loss of access to CNCS information and information resources.
- ☐ I agree to become familiar with and abide by all Office of Information Technology (OIT) policies and the Records Management Policy all of which are located on the CNCS Policy Page.
- ☐ I understand that I am given access to only those systems for which I require access in order to perform my official duties.
- ☐ I will not attempt to access systems or information I am not authorized or required to access as part of my official duties.
- ☐ I understand that I have no expectation of privacy when using any Government Furnished Equipment (GFE) and/or accessing any CNCS information systems, all of my communications and searches including instant messaging (i.e. Skype/Lync), may be monitored, logged, and audited. Text messages from CNCS iPhones are currently not captured by CNCS, but may be in the future, as such should not be used to transact agency business.
- ☐ I understand that by accessing and logging in to the CNCS network, I am consenting to the monitoring of my activities.
- ☐ I will connect to CNCS systems only through the following approved methods:
    - Using CNCS-issued Government Furnished Equipment (GFE) or
    - Using non-GFE and a CNCS issued token to access the CNCS VPN.
- ☐ I understand that the Rules of Behavior apply to all CNCS Systems, including the CNCS Guest Wireless Network.

Acceptable Use:

- ☐ I understand that government equipment and services are to be used for official business only, except for limited personal use as described below. Government equipment includes, but is not limited to, workstations, laptops, mobile phones, mobile hot spots, printers, copiers, and external hard drives. Limited personal use of government IT equipment and services is permitted as long as that use:
    - Is not illegal, inappropriate or offensive to fellow staff or the public.
    - Is conducted on the employee's own time with little or no impact on employee productivity.
    - Does not incur any additional expense to the government (i.e. Calling 411 on GFE phones is not appropriate except in emergency situations.)
- ☐ Government resources such as email, instant messaging, SharePoint, texting, photos, or any other communication methods should not be used for inappropriate or illegal activities, including but not limited to:
    - Sexually explicit or sexually oriented content, or anything that is in violation of sexual harassment or hostile workplace laws;
    - Ethnic, racial, sexist, or other offensive comments;
    - Fraud or gambling; and
    - Illegal weapons, terrorist activities, or the planning or commission of any crime.
- ☐ I understand that accessing such prohibited activities through intermediary accounts (e.g., personal email or home Internet service providers) does not affect the prohibition. If I am using a government computer or accessing a government network, I may not engage in prohibited activities at ***any time***.
- ☐ I will refrain from engaging in inappropriate IT activity that could increase the exposure of the CNCS network and all of its users to viruses and malware from malicious sites.
- ☐ I will refrain from using network resources (e.g., audio/video streaming, storing data on CNCS systems, etc.) for non-work reasons.

Passwords and Other Access Control Measures:

- ☐ **I will not share my access with or disclose my account passwords to anyone.**
- ☐ **I will not use account credentials that belong to someone else, even if the account owner gives me permission to use the credentials.**
- ☐ I understand that I am responsible for all activity that occurs under my account.
- ☐ I will choose strong passwords (minimum number of characters required by the system or application, a number, a special character, a capital letter, and no dictionary words) and take the necessary precautions to protect my account.
- ☐ I understand, consistent with good security practices, I will change my passwords when required to do so.
- ☐ I will protect passwords and access numbers from disclosure.

- ☐ I will not store passwords in an unsecure manner or on unencrypted devices.

Information Protection (electronic & hardcopy):

- ☐ When accessing CNCS Information Systems in any manner (VPN, personal computer, any CNCS wireless service, etc.), I will abide by this ROB Agreement.
- ☐ I will protect all PII from unauthorized disclosure, modification, or destruction.
- ☐ I understand that all Sensitive information and PII transferred inside and outside CNCS must be encrypted.
- ☐ I will use the CNCS secure email solution when emailing sensitive information and PII.
- ☐ I understand that I may only share PII or sensitive information with external people securely:
    - When it is an official business requirement and sent through secure email; or
    - In CNCS' authorized Records Management System such as SharePoint/OneDrive, by controlling read, write, edit and print access.
- ☐ I understand that I must not send sensitive information or PII outside of the CNCS network (e.g., to personal email, instant messaging, or external users' email or SharePoint/OneDrive).
- ☐ I understand that I must NOT store CNCS sensitive information or PII on unencrypted mobile devices (e.g. personal smartphones, tablets, etc.) or unencrypted removable storage media (e.g., USB drives, portable hard drives, memory cards).
- ☐ I understand that information stored on local drives is not backed up; as required that information should be saved to appropriate locations that are backed up.
- ☐ I will use my official CNCS email account and other CNCS-approved communications options (e.g. Lync, Skype) to transact agency business.
- ☐ I will lock my workstation or laptop computer whenever I step away from my work area.
- ☐ I will store electronic files containing sensitive information or PII data in properly secured folders that only allow access to those with a need to know. I will not store or distribute sensitive information or PII data on unapproved systems (e.g., Google Drive, Dropbox, Box, etc.).
- ☐ I will ensure that all hardcopy PII is stored in a secured location in order to protect it from unauthorized disclosure, modification, or destruction.
- ☐ I will minimize the collection and use of PII in performance of my official duties. I will immediately dispose of PII when no longer needed to perform my official duties.
- ☐ I will not disclose any personal information contained in any system of records, except as authorized by applicable laws or regulations.

Government Furnished Equipment (GFE)/Telework:

- ☐ I understand that all rules of behavior apply when working off-site.
- ☐ I will not modify the configuration of any GFE computer or tablet without permission from OIT.

- ☐ I will keep the GPS location services turned on all applicable GFE devices.
- ☐ I will take precautions to protect government property, secure government information and information resources in my possession from unauthorized disclosure, theft, destruction, or misuse.
- ☐ Outside of my work location, I will take all reasonable steps towards safeguarding GFE's (e.g., not leaving a device in plain sight in an unattended vehicle, etc.)
- ☐ I will dispose of media (both hardcopy and electronic) using approved means of destruction.
- ☐ When teleworking, I will follow security practices that are equivalent to those required of me at my primary workplace.
- ☐ I will not store sensitive data in non-GFE at alternative work sites.
- ☐ I will report the theft or loss of any IT related asset by using the on-line Missing IT Asset form within **24 hours** of occurrence. If I do not have access to the portal, I will email the incident details to OITHD@CNS.GOV or contact the OIT Help Desk at 202-606-6600.

Incident Reporting:

- ☐ I will promptly report any suspected or actual violations of CNCS security or privacy policies or incidents by using the on-line Security/Privacy Incident Form. For individuals without access to the portal, email details about the incident to OITHD@CNS.GOV, or contact the OIT Help Desk at 202-606-6600.

Records Retention:

- ☐ I understand my obligation to retain records as defined by the CNCS Records Management policy. A record is defined as any material, physical or electronic, made or received by you in connection with the transaction of public business. Records reflect the transaction of agency business by documenting agency functions, policies, decisions, procedures, and/or transactions. Transacting agency business generally does not include logistical, scheduling, or administrative communications.
- ☐ I will only use my official CNCS email account and other CNCS approved communications options (e.g. Lync, Skype) to transact agency business. I will not routinely use any unofficial electronic messaging account (i.e., your personal email account or any text message account) to transact agency business, and never to send sensitive or PII. Text messages from CNCS iPhones are currently not captured by CNCS, but may be in the future, as such should not be used to transact agency business.
- ☐ In cases where I cannot use my official CNCS email account to transact agency business (i.e. in cases of emergency, inaccessibility, non-functionality, etc.), and I use my personal email account, I understand that the Federal Records Act requires that I must either: copy my official CNCS email account on the message, or forward a complete copy of the record to my official email account within 20 days of creating or transmitting the record.

Supervisors/COR:

- ☐ I will ensure that all individuals complete mandatory privacy and security training.
- ☐ I will ensure that all individuals are made aware of the specific security requirements for protecting information (e.g., privacy, procurement, budget, paper copies, etc.) and information systems as part of their job performance.
- ☐ I will ensure that all on-boarding and off-boarding activities are performed.

What are the penalties for non-compliance?

Users who do not comply with the Rules of Behavior are subject to penalties that may be imposed under federal law. These penalties include:

- ☐ Written Reprimands
- ☐ Suspension of System Privileges
- ☐ Temporary Suspension from Duty
- ☐ Removal from Current Position
- ☐ Termination of Employment
- ☐ Criminal Prosecution
- ☐ Reimbursement to the Government for unauthorized charges

Rules of Behavior for Cybersecurity and Privacy Certification

My signature certifies that I have completed the Corporation for National and Community Service Cybersecurity User training. I have read and understood the Cybersecurity Rules of Behavior Agreement. I understand that violation of these rules could result in administrative punishment and/or criminal prosecution.

Name (Print legibly): _____

Dept./Org/ Company: _____

CNCS Username, if known (Print legibly): _____

Signature: _____ **Date:** _____