PII Awareness Briefing
Introduction

• Cyber attacks on private, public and government information systems are becoming all too common.

• From hackers to cyber criminals and nation states, today’s attackers are more disciplined, sophisticated and aggressive than ever before.

• As some of the most effective attacks on cyber networks worldwide exploit user behavior, everyone plays a role in defending against the growing cyber security threat.

• Cyber attacks ultimately seek to obtain information to be used maliciously.
Learning Objectives

• Identify what is Personally Identifiable Information (PII), its use and employees’ responsibilities with regard to it.
• Recognize types of security and privacy risks.
• Identify the impact and consequences of improper disclosure of information and inadequate protection of computer resources.
• Identify, report, respond to and prevent cybersecurity incidents and PII breaches.
• Identify best practices for cybersecurity and privacy awareness.
Personally Identifiable Information (PII)

• PII is defined as all personal information associated with an individual and includes everything from their name to their Social Security number.
• PII is used to IDENTIFY, CONTACT, & LOCATE.

First Name or Initial and Last Name
SSN
Driver’s license or State ID card number
Passport number
Credit card number
Security question answers
Passwords
Fingerprints
Financial account number
Medical information
Health insurance information
What is PII?

AGE
GENDER
RACE
SCHOOL
LAST NAME
Protecting PII in Communications

• Sensitive PII sent via email must be encrypted (Attachments):
  - a password-encrypted archive.(zip, 7zip, rar, tar)
  - secure email
• Secure uploads or file transfer utilizing HTTPS.
Identifying PII

*Everyone has a role in information security and protecting PII*

• Do you handle any PII?
• Do you know what kind of PII you handle?
• Do you know who is entitled to have access?
• Do you know the rules on how to transmit PII?
• Do you know how to recognize a social engineering attack when someone is trying extract PII from you?
• Do you know what industry or regulatory compliance guidelines you are required to follow?
• Do you know how to report PII breaches?
Risks

Internet, Search Engines, Data Mining

• Mobile Devices
  • Say no to unnecessary features
  • Know how to remotely wipe

• Social Media
  • Think before you post

• Anonymity
  • Browser Private Mode
  • Separate Accounts
  • VPN
Compliance

- PCI DSS - Payment Card Industry Data Security Standards
- HIPAA - Health Insurance Portability and Accountability Act
- HITECH - Health Information Technology for Economic and Clinical Health
- GLBA - Gramm-Leach-Bliley Act (Banks)
- FERPA - (SCHOOL)
- FISMA - (Federal Government)
- FERC/NERC - (Energy Sectors)
Prevent Data Breaches

- Minimize information collection.
- Store information securely.
- Dispose of PII properly.
- Follow configuration management processes.
- Always ask “Why” before providing information.

If you suspect a PII breach, notify your IT/Security/Helpdesk.
Questions?
Some content utilized from our KnowBe4 LMS subscription with KnowBe4.

KnowBe4 provides computer based security awareness training.