Safeguarding Personally Identifiable Information and Tribal Data

March 20, 2023

ACF OFFICE OF CHILD SUPPORT ENFORCEMENT

Agenda

- Identity Theft
- Phishing Scams – Social Engineering
- Protect Personally Identifiable Information (PII)
- Malicious Code, Viruses, and Ransomware Attacks
- Protecting Data and Networks
- General Office Data Handling Safeguards
- Incident Response

Identity Theft

What Is Identity Theft?

- When someone uses your PII to commit fraud and other crimes
- Three types
  - Financial
  - Medical
  - Online
- Biggest targets
  - Elderly
- U.S. has the highest number of cases
  - Federal Trade Commission (FTC) estimates an average of 9 million cases annually
  - A new case occurs every 22 seconds

Signs of Identity Theft

- Unexplained credit card charges or bank card withdrawals
- Medical bills from doctors you have not visited
- New credit cards you didn’t apply for
- Errors on your credit report
- Collection notices or calls for unknown debt
- Denial on application for credit card, car loans, etc.
- Missing mail
- Errors on your tax return or social security statements

What Can You Do

Place a credit freeze with all 3 credit bureaus

- Equifax (888) 766-0008
- TransUnion (800) 680-7289
- Experian (888) 397-3742

Phishing Scams – Social Engineering

What Is Phishing?

- Fraudulent emails that appear to be from reputable companies
  - Use tricks to get you to reveal information to gain access to systems and networks or click on bad links to download malware
  - Email that appears to be from your IT department
  - Claims your account has been compromised
- One of the biggest threats to cybersecurity
- Accounts for 22% of all data breaches
- Increased by 61% in 2022

Protect Personally Identifiable Information

Tips

- Review your credit reports three times a year
- Review bank statements and credit card statements monthly
- Don’t open suspicious email or email from unknown sources
- Don’t click on links in emails or respond with PII
- Inspect ATMs, gas pumps, and other card scanners for skimming devices before inserting your debit or credit card

Malicious Code, Viruses, and Ransomware Attacks

What Is Ransomware?

- Infects computers and encrypts computer files until you pay a ransom
- After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible computers
- Ransomware identifies the drives on an infected system and begins to encrypt the files within each drive
- Ransomware generally adds an extension to the encrypted files such as .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, or cryptolocker

How Does Ransomware Occur?

- Delivered through phishing emails or via “drive-by downloads”
- A “drive-by download” is a program automatically downloaded from the internet without your consent or even your knowledge
- Malicious code may run after the download without any action from you
- After the malicious code runs, the computer becomes infected with ransomware

Tips to Prevent Ransomware

- Update and patch your system and /network
- Use caution with links and when entering website addresses
- Open email attachments with caution
- Encrypt PII and sensitive information
- Verify email senders
- Inform yourself
  - Question
  - Research
  - Investigate
  - Verify
- Install antivirus software, firewalls, and email filters

Protecting Data and Networks

Data Security – Three Crucial Components

- **Confidentiality** – Prevent unauthorized disclosure of information
- **Integrity** – Assure that data cannot be modified in an unauthorized manner
- **Availability** – Make information readily available for authorized users

Protecting PII

- Employees are the key to safeguarding and protecting PII both in electronic and paper formats
- The success of protecting information depends on everyone's cooperation

Biggest Threats to Your Data and Network

- Phishing
- Social Engineering
- Malware Attacks
- Ransomware
- Weak Passwords

How to Protect Data and Networks

- Back up your systems and network
  - Perform frequent backups of your system and other important files
  - If your systems become infected, you can restore your system to its previous state using your backups
- Store your backups separately
  - Store your backups on a separate device that cannot be accessed from a network, such as on an external hard drive
  - Once the backup is complete, make sure to disconnect the external hard drive or separate device from the network or computer
- Train your organization
  - Conduct regular and mandatory cybersecurity awareness training sessions to ensure all personnel are informed about current cybersecurity threats.

Antivirus Scans Highly Recommended

- Identify malware and viruses
- Identify any vulnerabilities within your organization
- Quick scans may not detect some malware or viruses
- Full scans can require much more time but detect all known viruses
- Total global damage to businesses for cybercrimes in 2021 around $5 billion dollars
- Home Depot PII breach in 2015 exposed 56 million customers and credit card information

General Office Data Handling Safeguards

General Office Data Handling Tips

- Password guidance
- Transmitting PII through email and fax
- Storing sensitive data
- Mailing office documents
- Destroying PII
- Working remotely

Passwords Guidance

- Easy or generic passwords pose a weak link to cybersecurity
- Nearly 20% of passwords are compromised each year due to weak passwords
- A secure password should be at least 12 to 14 characters
- Create a password with capital letters, lowercase letters, numbers, and special characters
- Use a passphrase to remember passwords
- Commit passwords to memory and don’t leave them near your computer or desk

Emailing PII

- Use encryption when emailing PII to another party
- Use FIPS 140-3 compliant encryption software
- Include the PII in an encrypted attachment, never in the main body of the email
- Do not send the passcode to decrypt the attached file in a separate email
- Use voice mail, text message, or phone call

Faxing PII

- Notify the recipient of the fax before sending
- Verify the fax number
- Include a disclaimer notice on the fax cover sheet
- Remain at the fax until the documents are transmitted
- Advise the recipient to wait at the fax machine to receive the document

Storing PII

- Never store PII on you personal computer or laptop
- Never store PII on portable media unless it is encrypted with FIPS 140-3 compliant encryption
- Never store PII on your office laptop unless you have full disc encryption
- Store PII in a secure encrypted folder on the office network drive

Mailing PII

- Place content in a double-sealed envelope
- Mark interior envelope “Confidential, to be opened by designated official only”
- Send PII with a courier with tracking software
- Monitor package while in transit
- Notify the recipient that document(s) are coming
- Have the recipient notify you if they do not receive the document or package in a timely manner

Destroying PII

- Place documents in a secure shred container
- Shred documents using a cross-cut shredder
- Destroy electronic media using a media destruction machine
- Erase electronic records to leave no trace of the PII
- Physical and electronic records containing PII should be destroyed when you are done with them

Working Remotely

- Only use a secure wireless network
- Do not use a public Wi-Fi network such as those at coffee shops, airports, or hotels
- Hackers frequent these spots and can Wi-Fi sniff or other mechanisms to steal data from your device
- Use a Virtual Private Network (VPN) to encrypt your connection
- A VPN protects data on your device

Impact of Lost or Stolen PII

- Your agency reputation takes a hit through breached trust and lost customer confidence
- Data loss can be expensive due to Investigations, litigation, compensation, and other monetary losses
- Lost productivity and availability of data due to the downtime needed to investigate or remediate the data breach
- Fraud and direct monetary loss

Incident Response

Incident Response and Reporting

- Know the types of security incidents to report
- Know your role and responsibility in the reporting process
- Report known or suspected incidents to management immediately
- Protect the integrity and reputation of your agency by quickly reporting, managing, and resolving incidents

Security Incidents to Report

- System password is compromised
- Office break-in
- Unauthorized access to data
- Re-disclosure of data verbally, on paper, or in electronic format to unauthorized person
- Laptop/case files stolen (especially from cars)
- Victim of ransomware or malware attacks
- Infected files

Questions and Contact Information

Danny Markley

Danny.Markley@acf.hhs.gov

202-260-1888