Security Awareness, Training, & Education Contest

Entry Form

Please review rules before completing entry form including the due date. No late entries will be accepted. E-mail entries to fissea-contest@nist.gov.

Name of submitter: Deborah Coleman

Organization: The Department of Education, Office of the Chief Information Officer, Information Assurance Services

Address: 550 12th Street, S.W., PCP-100-30, Washington, DC 20202

Phone: (202) 245-7304

Email Address: Deborah.Coleman@ed.gov

Type of Entry: Awareness: Newsletter

Title of Entry: Department of Education Info Security News – A View to a Spill

Description of Entry:

The theme of this newsletter is based upon the FY2013 cyber security and privacy awareness campaign which focuses on encouraging all Department personnel to protect themselves and the Department from harm by becoming an ED-Defender. Our ED-Defender "secret agent" character is a parody of the 007 character in James Bond movies. The ED-Defender shield, "secret agent" character and movie parody concepts are woven into all campaign materials, including newsletters, posters, briefings and videos. The newsletter submitted features awareness of spear phishing attacks, best practices for protecting personally identifiable information (PII) and preventing spear phishing attacks, what to do if you are the victim of identity theft and how to report an incident. The newsletter provides information that the reader can use to protect themselves and the Department.

Info Security News

March 2013

In today's busy world we are more interconnected

than ever before and are in constant communication with others. Email, messaging and even social networking have become the norm. Yet, for all its advantages, these methods of connecting and communicating can increase your vulnerability to cyber-attacks. One common attack, spear phishing, uses fake emails which masquerade as legitimate correspondence to convince recipients in a targeted organization to provide confidential information which may result in a data breach. For example, the email message might appear as if it came from your supervisor, human resources, the IT department, or from another government agency, or an association. Spear phishing can place you, the Department of Education (ED) and others at risk.

Let's look at the following realistic, yet fictitious scenario to learn more about how spear phishing attacks can happen.

It started out just like any other day. After arriving at the office, you log on to the network and check your email. As you go through your email, you come across one from the Department's Office of the Inspector General (OIG) with the subject line of "Final Request – Attention Required." The body of the email states that you had failed to respond to their first request for information and that a response back was required before the end of the week. That's odd, you don't remember getting the first email. You decide to click the embedded link and provide the basic information on your project to their SharePoint site. After all, you don't want to risk creating a finding in an audit report. That afternoon you notice that your computer is running really slow and you can't seem to get anything done. After opening a ticket with the Help Desk, the Department's IT team determines that your computer is running malware and that it may have spread further into the network. Oh, no....

A View to a Spill

Spear phishing attacks

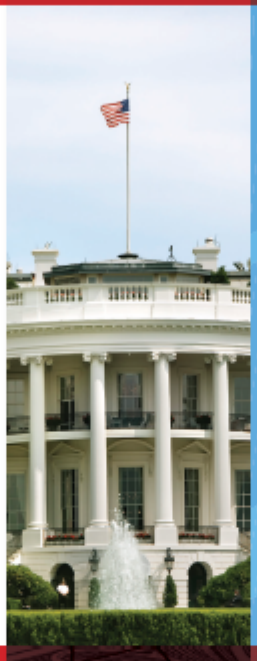
continue to rise at an alarming rate and can cause great damage - even if only one user takes the hook. Let's look at some real world examples of how spear phishing attacks were able to successfully compromise government information systems and networks.

The White House Military Office
September 2012

The Washington Free Beacon broke the news of the incident, after an unidentified national security official told the publication that the breach was the result of a "spear phishing attack against an unclassified network" at the White House. "In this instance the attack was identified, the system was isolated and there is no indication whatsoever that any exfiltration of data took place," the official told the nearly year-old, nonprofit online newspaper. No classified computer systems were impacted or targeted, according to the official.

http://freebeacon.com/white-house-hack-attack/

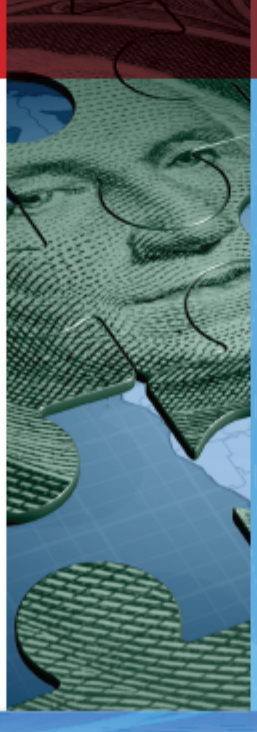
http://news.cnet.com/8301-1009_3-57523621-83/white-house-confirms-spearphishing-intrusion/



South Carolina Department of Revenue
October 2012

A targeted phishing email delivered to an employee at the South Carolina Department of Revenue opened the door for attackers to extract Social Security numbers and other personal data belonging to millions of residents, according to a report prepared by forensic firm. The attack began when a number of workers received a malware-infested phishing email. At least one employee fell for the ruse, which executed malware, stealing their username and password. The full forensic report which provides more information is available from the following link.

http://governor.sc.gov/Documents/MANDIANT%20Public%20IR%20Report%20-%20Department%20of%20Revenue%20-%2011%2020%202012.pdf



Don't Get Hooked!

Protect yourself and federal information systems and avoid becoming a target for phishers by following these security tips:

- Never give out your password to anyone! If someone from IT systems requires access to your computer, they will use their administrator user name and password.
- Do not access the web by selecting links in emails or pop-up messages.
- Never give out information about the Department, or personal or financial information through email, regardless of who sends it.
- If you receive an unsolicited request for information, with or without links, the safest practice is to assume it's a phishing attempt.
- If you have doubts about the authenticity of an email message, contact the sender by phone or some other means before opening an attachment or clicking a link
- Contact your ISSO and let him/her know that you've received a suspected phishing/spam message and contact EDCIRC to report the message: EDCIRC@ed.gov. An EDCIRC Team member will walk you through sending a copy of the message.

What You Need to Know

So what exactly is PII? PII is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Some PII is not sensitive, such as the PII on a business card. Other PII is considered sensitive and requires stricter handling guidelines due to the increased risk to an individual if the information is compromised. ED defines Sensitive Personally Identifiable Information (SPII) as information that if released improperly could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual whose name or identity is linked to the information. Certain types of information is always considered sensitive such as:

- Social Security Numbers (including using just the last 4 digits)
- Date of birth
- Mother's maiden name
- Biometric identifiers (e.g., fingerprint, iris scan, voice print)
- Personal financial information, credit card and purchase card account numbers
- Citizenship and immigration status
- Criminal history
- Computer access passwords and security questions

As an ED employee or contractor, you are responsible for protecting information commensurate with its sensitivity. **SPII always needs protection** no matter what format it is in (e.g., paper or electronic), or where it is located (e.g., file cabinet, database, shared drive, social media application, or transmitted via email).

WinZip to the Rescue

Email SPII securely

Before you send SPII via email, pause and think. Does the recipient really need the information and are you sending more than they actually need? Remember to address your message carefully, so that you don't accidentally send your email to the wrong person.

- Are you sending the information to an external party? If you answered "yes" to this question, you must encrypt!
- SPII sent within ED's network may be sent using a password-protected WINZIP archive. Follow the step-by-step instructions on ConnectED to learn how to use WINZIP.
- For internal emails sent with password-protected attachments, do not email the password in the text of the same email – either use a more secure form of communication, or send two separate emails.

Stop Criminals in Their Tracks

Protect SPII by following these best practices:

- Keep a clean desk – secure Sensitive PII when not in use.
- Don't leave PII or SPII on printers, copiers, or fax machines.
- Be mindful of your surroundings. Do not use speaker phones or talk openly in public about SPII.
- Encrypt mobile devices used to access or store SPII (e.g., a laptop, USB drive, CD-ROM/ DVD, or smart phone).
- Use only ED-issued thumb drives.

Shred documents containing SPII when you are ready to dispose of them. Do not simply place them in the trash or recycle bins.

For more information, please contact ED's Privacy Safeguards Division by calling the Helpline at 202-401-1269 or emailing privacysafeguards@ed.gov

Let's Talk Trash

Just upgraded your personal smart phone, tablet, or computer to the latest technology? Before tossing your old equipment or putting it up for sale on eBay or Craig's List, take the time to protect your privacy by removing any personal information that may be remaining on those devices.

- For an old laptop or PC, you can run a program, such as www.killdisk.com to wipe the hard drive, or physically destroy the drive (but you won't be able to sell the system as complete).
- For old mobile phones, grab the owner's manual and follow the steps for resetting the phone to factory settings. If you don't have the manual, contact your phone vendor or wireless service provider.
- If your equipment had been approved for use on the Department's network and has Department access software installed, remember to inform your Program Office IT Coordinator BEFORE discarding the device.

Shocking! Positively Shocking!

What to do if you are an Identity Theft Victim

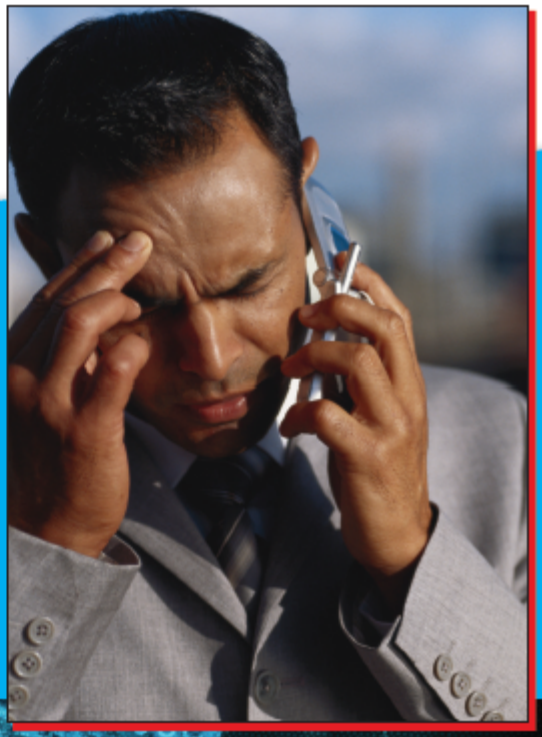
You just answered the phone and a debt collector is demanding payment for an expensive Omega wristwatch. You are taken completely off guard as you don't have a clue what the caller is talking about – you're not James Bond and certainly can't afford that watch. You may be a victim of identity theft. According to the Department of Justice, identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. If you think you've become a victim of identity theft or fraud, act immediately to minimize the damage to your personal funds and financial accounts, as well as your reputation.

The Federal Trade Commission (FTC) recommends that you take the following four steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports and review them. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently. Call and speak with someone in the security or fraud department of each company.
3. File a complaint with the FTC using their online complaint form or call their Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
4. File a report with your local police or the police in the community where the identity theft took place.

Additional information on identity theft is available from the FTC's website:

http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html



Incident Reporting

If you suspect a loss of SPII, or if you are aware of a privacy or security incident, you must notify your POC's ISSO as soon as possible. If you are unable to reach your ISSO, please send an email to EDCIRC@ed.gov and privacysafeguards@ed.gov. Once the incident is reported, the Department's incident response team will determine if additional steps should be taken.