The Front Burner
cyber security

THE OFFICE OF THE CHIEF INFORMATION OFFICER
OFFICE OF CYBER SECURITY

Don’t take the bait

A wide variety of cyber security threats await us as we go about our day-to-day activities on-line. Hackers and attackers have stepped up their use of social engineering, like phishing attacks, to solicit personal information, financial information, and information about the Department of Energy. The purpose of this article is to explain what social engineering is, familiarize you with a social engineering technique known as phishing, and provide some tips to assist in spotting fraudulent messages and avoid these attacks.

What is Social Engineering? Social engineering is a means by which a person can gain information such as company, personal and financial information by use of tricking an individual into freely giving sensitive information to them.

What is Phishing? Phishing is a social engineering technique used to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. PayPal, eBay and online banks are common targets. So is the Department of Energy. Phishing is typically carried out by email or instant messaging, and often directs users to enter sensitive or personal details at a website, although phone contact has been used.

What is Spear Phishing? Spear phishing describes any highly targeted phishing attack. Spear phishers send e-mail that appears genuine to all the employees or members within a certain company, government agency, organization or group.

Phishing scams have been successful at the Department of Energy because employees are spending more time online and are letting their guard down or are not aware of social engineering scams.

If you want more information about on-line scams, please go to http://onguardonline.gov where you can view a wealth of informative materials which include tutorials and videos.

How to avoid being a victim of email phishing attacks?

Be suspicious of unsolicited email messages from individuals asking about your personal information, the Department of Energy, or employees of the Department. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Do not provide personal information or information about your organization at the Department of Energy, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

Don't send personal information over the Internet before checking a web site's security.

Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org/phishing_archive.html).

What do you do if you think you are a victim?

If you believe you might have revealed sensitive information about the Department of Energy, report it to the appropriate security officials within your organization, including network administrators. They can be alert for any suspicious or unusual activity.

If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

Recognizing Email Phishing Attacks

Here are some helpful tips to assist you in spotting fraudulent messages and avoid phishing scams.

- Frequently phishing emails make some form of **urgent appeal to provoke you to take action immediately**. For example, stating that your account may be closed if you fail to confirm, verify or authenticate information immediately.
- There are **embedded links** that look legitimate because they contain all or part of a real company's name. These links take you to fraudulent sites (or pop-up windows) that ask you to enter, confirm or update sensitive personal information. Sometimes the emails instruct the recipient to enter the information into the body of the email.
- There may be **obvious spelling or grammatical errors**.
- The writing may be awkward or inappropriate.
- The visual or design quality may be poor.
- Fraudulent emails typically **will not provide alternative methods for communicating** the requested information (i.e., telephone, mail, and physical locations).
- Fraudulent emails **often provide a general greeting and don't identify you by name**.
- **Fraudulent emails may often contain attachments** asking you to install software. These applications are called Malware and are used by the fraudsters to record your keystrokes; take unauthorized control of your system; steal the data maintained on your system; or use your system to attack other systems.

Generally, legitimate businesses do not:

- Send urgent or time-sensitive emails that **ask you to provide, update or confirm sensitive data** like your Online User ID or Password, Personal Identification Number (PIN), Social Security Number, ATM/Debit Card or account number, credit card **communication** number or expiration date, or mother's maiden name.
- Send email with **attachments asking you to install software**.
- Send emails without providing **alternative methods of communication.**

Remember, sophisticated phishing schemes use sophisticated emails. Use caution when you receive unexpected attachments.

Cyber Clip