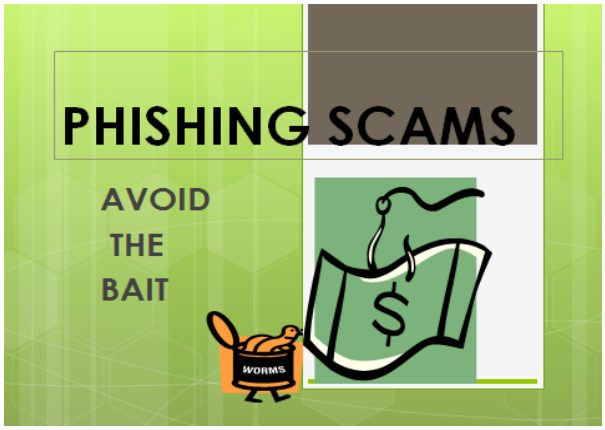
The Front Burner
Cybersecurity

Office of the Chief Information Officer
Office of Cyber Security
Issue No. 20, January 2015



Scam artists are becoming more clever in their attempts to defraud people of their personal information. Cyber awareness is essential in that it minimizes your chance of being defrauded while using the Internet and maximizes its benefits.

What is phishing?

Phishing is a malicious attempt to collect personal and/or financial information for illegal purposes by masquerading as an email from a trustworthy entity.

Cybercriminals have become very creative in their attempts to 'lure people in' and trick them into clicking on a malicious link or to open an attachment. Always be suspicious of unsolicited emails!

Below are a few examples of Phishing scams. The senders are phishing for your information so they can use it to commit fraud. Avoid the Scams . . . don't take the bait! Protect your personal information.

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

How do you protect yourself?

- Watch out for 'phishy' emails. The most common form of phishing is an email pretending to be from a legitimate retailer, bank, organization, or government agency. Never confirm personal information in a suspicious email.
- Do not click on links to web sites within emails that ask for your personal information. To check whether the message is really from the company or agency, call the company or agency directly.
- Keep your personally owned computers clean with up-to-date spam filters, anti-virus and anti-spyware software, and a firewall.
- Act immediately if you think you have been hooked by a phisher. If the phishing attempt happens at work, contact your Help/Service Desk per your site's policy. If the attempt happens in your home environment, you can access more information here: http://www.consumer.ftc.gov/features/feature-0014-identity-theft.

Phishing Definitions

Spear Phishing is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.

Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. The targets of whaling are high-ranking executives and others in powerful positions.

Tabnapping is a computer exploit and phishing attack, which loads a fake web page in one of the open tabs of your browser and captures your login details and passwords when you think you are logging into a legitimate popular website.

2014 DOE OCIO Cybersecurity Achievement Awards

The 2014 Cybersecurity Achievement award recipients will be announced at the DOE Cybersecurity Training Conference in Kansas City, Missouri in April.

Securing Your Wireless Network

Securing your wireless network prevents strangers from using it to gain access to your computer – including the personal and financial information you've stored on it.

Here are a few steps that can keep you secure:

1) **Understand How a Wireless Network Works**

- Going wireless generally requires connecting an Internet "access point" – like a cable or DSL modem – to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any computer within range with a wireless card can pull the signal from the air and access the Internet.
- Unless you take certain precautions, anyone nearby with a wireless-ready computer or mobile device can use your network. That means your neighbors – or any hacker nearby – could "piggyback" on your network, or access information on your computer. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

2) **Use Encryption**

- Encryption scrambles the information you send over the Internet into a code so that it's not accessible to others. Using encryption is the most effective way to secure your network from intruders.
- Two main types of encryption are available: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers.
- Some older routers use only WEP encryption, which may not protect you from some common hacking programs. Consider buying a WPA2 router.

3) **Secure Your Computer and Router -** *Use anti-virus and anti-spyware software, a password, and a firewall.*

- Use the same basic computer security practices that you would for any computer connected to the Internet. Change the name of your router from the default. Change your router's pre-set password.

4) **Limit Access to Your Network** - *Allow only specific computers to access your wireless network.*

- Every computer that is able to communicate with a network is assigned a unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

5) **Don't Assume That Public Wi-Fi Networks Are Secure** - *Be cautious about the information you access or send from a public wireless network.*

- Many cafés, hotels, airports, and other public places offer wireless networks for their customers to use. These "hot spots" are convenient, but they may not be secure.

For more information, go to: https://www.onguardonline.gov/articles/0013-securing-your-wireless-network

2014 National Cybersecurity Awareness Month

October was National Cybersecurity Awareness Month (NCSAM), and the Office of the Chief Information Officer (OCIO) sponsored the DOE Headquarters events.

The DOE NCSAM theme was ***"Securing the Internet of Things"*** which focused multi-faceted usage of the Internet and how it has become the main source of all things, to all users, thus requiring the shared responsibility of all computer users.

We were fortunate to have two dynamic guest speakers. Mr. John Pescatore, SANS Director of Emerging Security Trends, spoke on "Securing the Internet of Things - Separating Hype from Reality" addressing the latest Internet evolution, the billions of "things" connecting to users, businesses, and other "things" using mixtures of wired and wireless connectivity. Dr. Karen Paullet spoke on "Opening the Digital Pandora's Box: Mobile Device Security Awareness," Dr. Paullet shared how cell phones have become ubiquitous within our society, and many now consider them a necessity rather than a convenience.

Overall, it was a successful event and the OCIO would like to thank all who took the time to participate. To view these sessions or download/print materials from NCSAM events, go to the Powerpedia Cybersecurity Awareness webpage at: https://powerpedia.energy.gov/wiki/Cyber_Awareness

Cybersecurity Resources

SeniorNet - http://www.seniornet.com – Provides older adults education for and access to computer technologies to enhance their lives and enable them to share their knowledge and wisdom.

Phishing - http://iasecontent.disa.mil/eta/unclass-phishing_brochure.pdf - information on awareness of Phishing Warfare, and specifically, warfare on executives.

Phishing Training - http://iase.disa.mil/eta/Pages/online-catalog.aspx?Paged=TRUE&p_ID=5&PageFirstRow=5&&View={12592695-374A-4840-8DB6-0273FE729BAB} - This training explains what phishing is and provides examples of different types of phishing, to include spear phishing and whaling. Phishing techniques such as deceptive emails and web sites, as well as browser "tabnabbing" are discussed. Guidelines are provided to help users to recognize phishing attempts, so that appropriate actions may be taken to avoid these attacks and their consequences. Phishing is a serious, high-tech scam and users are the best line of defense against phishing. Further, the training illustrates why users should always be on the lookout for phishing attempts, even from people within their own organization.

What Do Supply Chain and Malware Have In Common?

By nature, a chain is a series of links, interdependent on each other. The supply chain is no different. Though the links may be intangibles like suppliers, retailers and customers, each piece serves as an important function. The supply chain is under siege from criminals who want to use these linkages to proliferate malware (malicious software) to steal sensitive information and deceive consumers into using fraudulent websites for their gains.

Hackers hit supply chains in two ways; one is a traditional method of infecting systems with malware bearing file names matching popular downloads. This method allows the malicious use of email messages, fraudulent websites, and online advertisements to deceive people into revealing personal information such as account passwords, social security numbers, and credit card numbers. For example, attackers in the Target breach used this method to steal credentials (valid user name and password) that gave them authorized access to the point of sale system. The other way installs malware (hidden or compromised files) on users' computers from links on websites or in emails or pre-installed on system components. Malware is insidious software that is covertly installed and performs secret operations, usually with bad intent, ranging from unauthorized simple email advertising to complex identity-theft and password-stealing. Malware programs operate invisibly, often without displaying themselves in Task Manager. Malware usually can't be uninstalled through the control panel and requires special tools to delete them.

Recently, Microsoft discovered a botnet embedded in more than 4,000 computers purchased by consumers from U.S. retailers. The malware allows hackers to remotely turn on the machines, access microphones and webcams, and log keystrokes, compromising passwords and banking information. This breach shows how vulnerable supply chains really are. The ease with which cyber thieves are attacking technology users is unsettling.

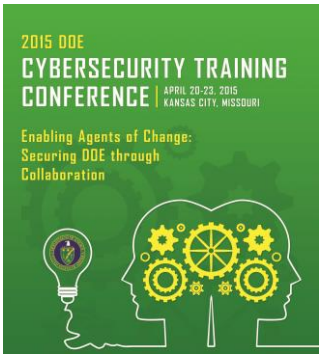
There is potential risk of serious intentional and unintentional faults in the technology we buy. In a market with complex global supply chains, dependence on foreign technology companies increases the likelihood of malicious intrusion and compromise of sensitive information. Knowing what you are buying and from whom is an important step in securing your technology supply chain. Our best advice is to be careful. A reputable business respects your privacy and is concerned about the integrity of the products it sells.

If you have any additional questions or suggestions contact us at enterpriseSCRM@hq.doe.gov.

We're Back!!!
2015 DOE CIO Cybersecurity Training Conference
April 20-23, 2015
Kansas City, Missouri

Planning is underway for the 32nd Department of Energy CIO Cybersecurity Training Conference to be held in Kansas City, MO, April 20-23, 2015. This year's theme, ***Enabling Agents of Change: Securing DOE Through Collaboration*** focuses on collaboratively exploring and implementing new cyber technologies required to securely accomplishing the DOE mission. Further, the theme underscores the importance of understanding current cyber threats and vulnerabilities and sharing innovative approaches and strategies to mitigate such threats.

Thanks to all who submitted abstracts for conference presentation consideration. The Steering Committee is excited about reviewing the submitted abstracts and planning the conference tracks. Track presentations are planned for 45-minutes and training workshops range from 2-hours to all-day sessions.



We look forward to seeing you at the conference as we share in *Securing DOE Through Collaboration*.

Additional information on the conference registration, agenda, and logistics will be posted on Powerpedia at: https://powerpedia.energy.gov/wiki/Cybersecurity_Conference.

Questions regarding the 2015 DOE Cybersecurity Conference may be emailed to the **DOE Cybersecurity Training Mailbox at cybsectrn@hq.doe.gov.**

Did You Know?

- Social Engineering is a way for people to gain your trust so they can manipulate you to give them information or unauthorized access to DOE resources.
- If you receive a chain letter in an email you should delete the email.
- If you receive an email from the IT Department and the email instructs you to confirm your user name and password to expedite desktop updates across the agency you should follow your site's policy and forward the email to your Security POC and/or Help Desk and then delete it.

Think carefully before you open or download anything that links to your personal information!

Training Opportunities

Cybersecurity Contractor Training Site (CTS)

The Contractor Training Site (CTS) https://contractortraining.energy.gov provides an excellent opportunity for DOE contractors to take free, online Cybersecurity and other training courses. *(NOTE: The same courses are available on OLC for Federal users).* Descriptions of the Cybersecurity training courses on the CTS are available on the Cybersecurity Awareness & Training (CSAT) Warehouse at http://energy.gov/cio/training/cybersecurity-awareness-training-warehouse.

First time users can register for a CTS account at https://contractortraining.energy.gov using your official DOE email address.

For all technical questions or issues with CTS, please contact the CTS Help Desk at (202) 558-2203 or toll free at (888) 804-4510, from 8:30 am to 6:00 pm EST, Monday through Friday, excluding holidays.

Federal Virtual Training Environment (FedVTE)

The Federal Virtual Training Environment (FedVTE) will be undergoing extensive changes in January and February:

- January 30, 2015 – the current FedVTE website will be shut down
- February 2015 – a new FedVTE site will be available
- User accounts WILL NOT be transferred to the new site, new accounts will need to be set up
- User course completion data WILL NOT be transferred to the new system
- Complete all courses in progress prior to January 29, 2015. Credit WILL NOT be given for any courses still in progress on January 30th.
- Course completion certificates from the current FedVTE must be saved or printed as they WILL NOT be accessible on the new system
- Any POCs needing course completion reports run please email Cybsectrn@hq.doe.gov with your organizational information by January 26, 2015
- No new users will be registered for the current FedVTE after January 26, 2015.

As more information is received from FedVTE it will be emailed to all current users and Training POCs. The information will also be posted on Powerpedia, *search FedVTE.*

Cybersecurity Online Learning (COL)

The 2015 COL Schedule, Recorded Workshop Listing and Registration Instructions are available at *https://colcgpub1.connectsolutions.com/content/connect/c1/7/en/events/catalog.html#currentSearchTag=1218823*

UPCOMING CYBERSECURITY EVENTS

2015 Annual Cybersecurity Awareness Training (Cyber Awareness Challenge 2.0)

The 2015 Annual Cybersecurity Awareness Training (*Cyber Awareness Challenge 2.0*) developed by the Defense Information Systems Agency (DISA) will be available on the Online Learning Center (OLC) and Contractor Training Site (CTS) in **January 2015**. The training provides current cybersecurity awareness information through an interactive forum entitled, Cyber Awareness Challenge 2.0. The Cyber Awareness Challenge is a serious game that simulates realistic cybersecurity scenarios and the resulting threat decisions that federal employees are subject to daily as they perform their work. Competition of this course by employees in your organization will satisfy the FISMA-mandated annual cybersecurity awareness training requirement.

For more details on the course, please check with your individual staff and program offices, HQ organizations or your Training Officer.

2015 TAKIN' IT TO THE STREETS

Cyber Awareness

We are taking Cybersecurity to the streets again. ***Takin' It To The Streets*** is back by popular demand!!! This is an opportunity for DOE Federal and Contractor employees to increase their awareness and assist with the warfare against cyber attackers. DOE Headquarters offices will collaborate to increase cybersecurity awareness and educate our employees.

This summertime event will take place on the Forrestal plaza outside the 10th Street front door entrance. There will be music, water, candy, and tables with information on computing and safe online practices.

Should your organization want to participate in the Cybersecurity Awareness **"Takin' It To The Streets"** Summer event and secure a table, please send an email with your name, organization and contact information to cybsectrn@hq.doe.gov.

For questions regarding these articles or any Cybersecurity issue, search ***cybersecurity*** *on Powerpedia or send an email to cybsectrn@hq.doe.gov*

Be a cyber hero!
Always STOP.THINK.CONNECT.