The Front Burner
Cybersecurity

Office of the Chief Information Officer
Office of Cyber Security
Issue No. 14, September 30, 2013

National Cybersecurity Awareness Month (NCSAM) ~ October 2013

Every October, the Department of Energy joins the Department of Homeland Security (DHS) and others across the country in support of National Cybersecurity Awareness Month (NCSAM) and the "Stop. Think. Connect." campaign. This year marks the tenth year of the cybersecurity awareness campaign.

No citizen, community, or country is immune to cyber risk, but there are steps you can take in your personal and work life to minimize your chances of an incident:

- Set strong passwords, change them regularly, and don't share them with anyone.
- Keep your operating system, browser, and other critical software optimized by installing updates … on your personal computer, your tablet and your smartphone.
- Maintain an open dialogue with your friends, family, and colleagues about Internet safety.
- Use privacy settings and limit the amount of personal information you post online.
- Be cautious about offers online – if it sounds too good to be true, it probably is.
- Login directly and conduct inquiries on the company's website, not through an email link. If you are still uncomfortable, call the company's customer care line. Remember, reputable companies don't ask you for personal information or your user name and password in unsolicited email.

You have the opportunity to join in cybersecurity awareness efforts across the country. If you, your family, or your organization is interested in more information about cybersecurity and the "Stop. Think. Connect." campaign, please visit www.dhs.gov/stopthinkconnect.

Be Aware of Phishing Scams!

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!

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.

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 it directly. Never enter your personal information in a pop-up screen.
- Keep your personally owned computers clean with up-to-date spam filters, anti-virus and anti-spyware software, and a firewall.
- Remember phishing attempts can be made by phone. If someone contacts you and says you have been a victim of fraud, verify the person's identity before you provide any personal information.
- Act immediately if you think you have been hooked by a phisher. If the phishing attempt happens at work, contact your Help Desk. If the attempt happens in your home environment, you can access http://www.consumer.ftc.gov/features/feature-0014-identity-theft for more information.