National Cybersecurity Awareness Month

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

Special Edition of

The Front Burner

Cybersecurity

The ACIO for Cybersecurity
Issue No. 13
October 2012

National Cybersecurity Awareness Month
October 2012

The Department of Energy is joining forces with the Department of Homeland Security and other Federal and State agencies and private industry to recognize October 2012 as National Cybersecurity Awareness Month (NCSAM). The primary goal of NCSAM is to engage and educate the public, private, and Federal sectors about cyber risks in an effort to increase the resiliency of the Nation against cyber incidents. The following is a message from our Associate Chief Information Officer (ACIO) for Cybersecurity, Mr. Gil Vega.

As the Department's Chief Information Security Officer, I would like to take a moment to discuss the critical role that cybersecurity plays in our daily lives – both at work and at home. The technology that has greatly enhanced our lives with immediate access to resources and communication tools has also exposed us to tremendous adversarial threats such as identity thieves that attempt to steal our personal information or terrorists that desire to destroy our Nation's infrastructure. In addition, we are more interconnected than ever before. From the kitchen table to the classroom, from business transactions to essential government operations and services, cybersecurity is an issue that touches all of us on a daily basis. Yet for all of its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. No country, industry, community, or individual is immune to cyber risks.

*National Cybersecurity Awareness Month reminds us that being safer and more secure online is a shared responsibility. In other words, during the month of October we pay special attention to "**Achieving Cybersecurity Together**." Each of us has an important role to play in securing our personal and professional cyberspace. Individual actions have a collective impact, and safe use of the Internet makes it more secure for everyone. If all Americans do their part by implementing stronger security practices, raising community awareness, educating young people and training employees, together we can foster a literate, resilient, and secure online society.*

NATIONAL CYBERSECURITY ALLIANCE

National Cybersecurity Awareness Month

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

Special Edition of

The Front Burner

Cybersecurity

Throughout National Cybersecurity Awareness Month and beyond, each of us should become more aware of cybersecurity risks and consistently implement common security practices on our home and business computers. By following these simple practices detailed on the following pages, we will significantly enhance the security of our online presence, therefore making the Internet a safer place for ourselves, our families, our communities and businesses, and our Nation.

One last comment, although October is the month set aside to focus on cyber threats and enhancing knowledge, let us not limit our awareness and actions to one month – instead remember to be vigilant in understanding and securing your personal cyberspace every day.

NATIONAL CYBERSECURITY ALLIANCE

National Cybersecurity Awareness Month

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

Special Edition of

The Front Burner

Cybersecurity

STOP | THINK | CONNECT™

Take Responsibility for Your Online Presence…

Keep a Clean Machine.

- **Keep security software current:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- **Protect all devices that connect to the Internet:** Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information.

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you to verify who you are before you conduct business on that site.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.
- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.

Connect with Care.

- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

NATIONAL CYBERSECURITY ALLIANCE

National Cybersecurity Awareness Month

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

Special Edition of

The Front Burner

Cybersecurity

- **Get savvy about Wi- Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- **Protect your $$:** When banking and shopping, check to be sure the site is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information.

Be Web Wise.

- **Stay current. Keep pace with new ways to stay safe online:** Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Think before you act:** Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- **Back it up:** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen.

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Post only about others as you have them post about you.**
- **Help the authorities fight cybercrime:** Report stolen finances or identities and other cybercrime to http://www.ic3.gov (Internet Crime Complaint Center), the Federal Trade Commission at http://www.onguardonline.gov/file-complaint.
  Visit http://www.stopthinkconnect.org for more information.

Cyber Hero Answers Your Security Questions

Q: Cyber Hero, what is Geotagging?

A: Geotagging is the process of adding geographical location, or labels, to photographs, videos, Web sites, SMS messages, QR Codes, or RSS feeds; a geotag usually consists of latitude and longitude coordinates, altitude, distance, place names, and other details about the origin of the media being tagged helping users find a variety of online location-specific information.

For additional Cybersecurity awareness information, please visit http://energy.gov/cio/training/training-warehouse.

NATIONAL CYBERSECURITY ALLIANCE