State of Illinois
Central Management Services
Monthly Cyber Security Tips
NEWSLETTER

October 2012 Volume 7, Issue 10

National Cyber Security Awareness Month: Tips for Staying Safe Online

October is National Cyber Security Awareness Month. This is an effort coordinated by the U.S. Department of Homeland Security, the Multi-State ISAC, and the National Cyber Security Alliance along with many governments, businesses, schools, and other groups to help improve cyber security preparedness. It's a great time to evaluate your online activities and take some basic steps to protect yourself.

Why Is National Cyber Security Awareness Month So Important?

In our online, mobile society, we are faced with an increasing barrage of cyber threats every day. Whether at work, home, school…virtually every part of our lives is now in some way or another connected to the Internet. Did you know…?

- Someone becomes a victim of cyber crime every 18 seconds
- Cyber crime costs an average of nearly $200 *per victim*
- Mobile device vulnerabilities doubled in 2011 from 2010
- 40% of social network users have been victims of cyber crime on a social networking site (Source all: Symantec)

What Can You Do to Participate in Cyber Security Awareness Month?

The theme of National Cyber Security Awareness Month is: Cyber Security Is Our Shared Responsibility. Each one of us plays an important role in securing cyberspace, and there are many actions we can take to make a positive impact.

Take the Cyber Pledge!

The Multi-State ISAC is conducting a national Cyber Security Pledge campaign during Awareness Month to help users understand good practices for staying safe on the Internet and affirm a commitment to online safety. You can join thousands of people across the country and sign the pledge online by visiting MS-ISAC at https://msisac.cisecurity.org/cyber-pledge/

Join the MS-ISAC on October 11 at 2PM for a free, one-hour webinar on how to stay safe from online scams, hackers, viruses, and more! Details and registration: www.cisecurity.org

Tune into the Cyber Security Webinar Series for additional webcasts each week during October, with practical tips on cyber ethics, cloud computing, & more.
http://www.naco.org/meetings/webinars/Pages/CybersecurityWebinarSeries.aspx

Distribute the MS-ISAC Awareness Toolkit Materials

Posters, calendars, bookmarks, and more that you can share throughout your organizations, in your community, and with your family are all free and available online:
http://msisac.cisecurity.org/resources/toolkit/oct12/index.cfm#toolkit

Implement Basic Cyber Security Best Practices

- ***Secure your computer.*** Be sure to have a firewall installed and enabled on your computer. Use spyware and adware protection software. This software is designed to protect you against spyware or malware, which can extract private information from your computer without your knowledge. Set these programs to auto-update to avoid missing a critical update.
- ***Use strong passwords on all your accounts.*** Use a minimum of eight characters and a mix of special symbols, letters, and numbers. Use separate passwords for each account, so that if one account password is breached, an attacker will not automatically have access to all of your other accounts. ***Do Not*** re-use your work password on other systems.
- ***Secure your online transaction***. When submitting your sensitive information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission. Also be sure that "https" appears in the website's address bar before making an online transaction. The "s" stands for "secure," and indicates that communication with the webpage is encrypted.
- ***Don't reveal too much personal information online.*** The less information you post, the less data available for a cyber criminal to use in a potential attack or scam.
- ***Protect your laptop, smartphone, or other portable devices when traveling***. Just as your wallet contains lots of important and personal information that you wouldn't want to lose, so too do your portable devices. Don't let them out of your sight! Never store your laptop as checked luggage. If there is a room safe available at your hotel, use it to securely store your devices. In

addition, make sure you have strong passwords on these devices in case they are lost or stolen.

- ***Be aware that public computers and public wireless access are not secure.*** Cyber criminals can potentially access any information you provide, such as credit card numbers, confidential information, or passwords. Don't conduct any sensitive transactions at the local free Wi-Fi site.
- ***Understand if and how location data is used.*** Check to see if GPS location data is being stored when you upload pictures to your social media site from your mobile device, and disable it if you don't want the world to know exactly where the picture was taken.
- ***Do not e-mail sensitive data.*** Beware of emails requesting account or purchase information. Delete these emails. Never e-mail credit card or other financial/sensitive information. Legitimate businesses don't solicit sensitive or confidential information through email.
- ***Dispose of information properly.*** Before discarding your computer or portable storage devices, you need to be sure that the data contained on the device has been erased or "wiped." Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DOD) compliant software.

For More Information

MS-ISAC Awareness Month Resources*: http://msisac.cisecurity.org/resources/toolkit/*

Stop.Think.Connect *http://stopthinkconnect.org/*

National Cyber Security Alliance *http://www.staysafeonline.org/ncsam/*

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY