



# NYS Office of Cyber Security

## Monthly Security Tips NEWSLETTER

October 2012

### National Cyber Security Awareness Month: Tips for Staying Safe Online

#### ***From the Desk of Thomas D. Smith, Director***

October is National Cyber Security Awareness Month. 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 or school, virtually every part of our lives is now connected to the Internet. National Cyber Security Awareness Month is an effort coordinated by the U.S. Department of Homeland Security, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the National Cyber Security Alliance in conjunction with governments, businesses, schools and other groups to help improve cyber security preparedness.

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 from 2010 to 2011\*
- Forty percent of social network users have been victims of cyber crime on a social networking site\*

#### **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 New York State Office of Cyber Security (OCS), in coordination with the MS-ISAC, is conducting a Cyber Security Pledge campaign during Awareness Month to help users understand good practices for staying safe on the Internet and to affirm a commitment to online safety. Join people across the State and sign the pledge online by visiting the OCS website at: <http://www.dhSES.ny.gov/ocs/awareness-training-events/events/2012/index.cfm>.

**Tune into the Cyber Security Webinar Series** for webcasts each week during October, with practical tips on cyber ethics, cloud computing, and more.

<http://www.naco.org/meetings/webinars/Pages/CybersecurityWebinarSeries.aspx>

#### **Distribute the New York State Cyber Security Awareness Toolkit Materials**

Posters, calendars, bookmarks, and more, are all free and available online at <http://www.dhSES.ny.gov/ocs/awareness-training-events/events/2012/index.cfm>. Share throughout your organizations, in your community, and with your family.

## Implement Basic Cyber Security Best Practices:

- **Secure your computer.** Keep your operating system and application software updated/patched. Be sure to check that your anti-virus/anti-spyware software is running and receiving automatic updates. Confirm that your firewall is enabled.
- **Use Strong Passwords:** Passwords should have at least eight characters and include letters (uppercase and lowercase), numbers and special characters. It is important to maintain separate passwords for different accounts to reduce the likelihood of one password being compromised, which may make other accounts vulnerable as well. Developing good password practices will help keep your personal information and identity secure.
- **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 you make 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 does your portable devices. Don't let them out of your sight. Never store your laptop in 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, passwords or other confidential information. Don't conduct any sensitive transactions public Wi-Fi sites.
- **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. Disable it if you don't want others to know exactly where the picture was taken.
- **Do not e-mail sensitive data.** Beware of e-mails requesting account or purchase information. Delete these e-mails. Never e-mail credit card or other financial/sensitive information. Legitimate businesses don't solicit sensitive or confidential information through e-mail.
- **Dispose of information properly.** When it's time to dispose of your computer or mobile device, make sure you have the tools and a process in place to completely erase your information or physically destroy the hard drive. Properly erasing your hard drive thwarts efforts to steal your information.

### Additional Information:

#### NYS Office of Cyber Security

- **Cyber Security Awareness Month:**  
[www.dhSES.ny.gov/ocs/awareness-training-events/events/2012/index.cfm](http://www.dhSES.ny.gov/ocs/awareness-training-events/events/2012/index.cfm)
- **Newsletters:**  
[www.dhSES.ny.gov/ocs/awareness-training-events/news/](http://www.dhSES.ny.gov/ocs/awareness-training-events/news/)

\*Source: Symantec

*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:**



**MULTI-STATE**  
Information Sharing  
& Analysis Center™

A DIVISION OF  CENTER FOR  
INTERNET SECURITY