



## National Cyber Security Awareness Month: Our Shared Responsibility What Community-Based Organizations Can Do

As a community-based organization, you are a trusted source of information for the community you serve. Even though online safety and security may not be part of your mission, the people you serve may turn to you for information about how to protect themselves and their family members. Consider doing the following during National Cybersecurity Awareness Month:

- Join the national campaign for cybersecurity education and awareness: STOP. THINK. CONNECT. Get details at [www.stophinkconnect.org](http://www.stophinkconnect.org).
- Post the STOP. THINK. CONNECT. tips and advice (<http://www.staysafeonline.org/tools-resources/stop-think-connect>) and NCSAM posters and banners around your organization's headquarters and field offices.
- Write an article on cybersecurity that incorporates the STOP. THINK. CONNECT. tips and advice for your organization's newsletter. You can use information found at [www.staysafeonline.org](http://www.staysafeonline.org) or [www.stophinkconnect.org](http://www.stophinkconnect.org).
- Add a section for staying safe and secure online to your website and use STOP. THINK. CONNECT tips and advice. You can use information found at [www.staysafeonline.org](http://www.staysafeonline.org) or [www.stophinkconnect.org](http://www.stophinkconnect.org).
- Encourage IT professionals from the community to visit schools and use NCSA's CSAVE curriculum (<http://www.staysafeonline.org/in-the-classroom/c-save>). It's easy, age appropriate and a fun way to educate kids about online safety.
- Make sure that your organization is taking adequate steps to protect any personal information you have about employees or people you serve.
- Conduct training for employees and volunteers about acceptable use of technology in the office. Create a written policy to address the issues if you haven't already done so. Review existing policies to be sure they address emerging technology if it's been a while since you last updated.
- Hold presentations in senior centers to educate them on online fraud and scams as well as the safe use of social networks.
- Become a fan of the NCSA Facebook page ([www.facebook.com/staysafeonline](http://www.facebook.com/staysafeonline)) and STOP. THINK. CONNECT. Facebook page (<http://www.facebook.com/STOPTHINKCONNECT>).
- Blog about cybersecurity throughout the month. Use social networks such as Facebook and Twitter to disseminate information and encourage employees and clients to learn more about staying safe online. Feel free to use content found at [www.staysafeonline.org](http://www.staysafeonline.org).
- Learn more at [www.staysafeonline.org](http://www.staysafeonline.org) and [www.stophinkconnect.org](http://www.stophinkconnect.org).



STOP | THINK | CONNECT

## Internet Safety & Security Tips for Parents

The Internet is a wonderful place for learning and entertainment, but can pose dangers if precautions are not taken. Allowing free access puts your child, your computer and your personal data at risk. Help to instill good judgment in your children by encouraging them to take some common sense steps.

The first step is **STOP. THINK. CONNECT.** Take security precautions, understand the consequences of your actions and behaviors and enjoy the benefits of the Internet.

### 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:** Computers, smart phones, gaming systems, and other web-enabled devices all need protection from viruses and malware.

### Protect Your Child's Personal Information

- **Help your kids own their online presence:** When available, set their privacy and security settings on websites to your comfort level for information sharing. Remind them that it's ok to limit how and with whom they share information.

### Connect with Care

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

### Be Web Wise

- **Stay current. Keep pace with new ways to stay safe online.** Check trusted web sites for the latest information, share with your children, and encourage them to be web wise.

### Be a Good Online Citizen

- **Safer for me, more secure for all:** What you and your kids 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.