



National Cyber Security Awareness Month

How Business Owners Can Support NCSAM

One aim of **National Cyber Security Awareness Month (NCSAM)**, held each October, is to provide independent business owners with the resources to protect their intellectual property and customer data. In an era of growing cybercrime, a safe and secure Internet is vital to building a prosperous business.

As a business owner, you can help make the Internet safer and more secure by participating in National Cyber Security Awareness Month. Whether you are able to show your support for just one day or every day this October, consider the following ways you can make a difference to raise cybersecurity awareness.

What you can do...

...in one minute:

- Display an NCSAM banner on your company website. Download NCSAM Web banners at <http://www.staysafeonline.org/ncsam/promote-ncsam/>. You can link to the NCSAM “About” page to provide more info at <http://staysafeonline.org/ncsam/about>.
- Send an email informing your employees, clients and business contacts that October is National Cyber Security Awareness Month. Encourage them to review tips and advice from the national cybersecurity awareness campaign, **STOP. THINK. CONNECT.**, at <http://www.stophinkconnect.org/tips-and-advice/>.

...in one hour:

- Strengthen your company's email and online accounts by adding extra layers of security and enabling technologies like 2-factor authentication. To learn more about these services, visit STOP. THINK. CONNECT.'s 2 Steps Ahead campaign page: <http://www.stophinkconnect.org/2stepsahead>.
- Review Verizon's **2013 Data Breach Investigations Report**. By knowing today's threats, you can better protect your organization tomorrow: <http://www.verizonenterprise.com/DBIR/2014/>.
- Download the Federal Communications Commission's **Small Biz Cyber Planner 2.0** to help you chart a path to a more cyber-secure business: <http://www.fcc.gov/cyberplanner>.

...in one day:

- Hold a brown bag lunch for employees to discuss your company's IT security and acceptable use policies. Find talking points for employees at <http://staysafeonline.org/business-safe-online/train-your-employees>.

... all month long:

- Work with your IT staff to host employee training on cybersecurity. **Internet Security Essentials for Business 2.0** by the U.S. Chamber of Commerce provides a number of employee-training toolkits: <http://www.uschamber.com/issues/technology/internet-security-essentials-business>.
- Create a contingency plan in the event of a data breach. You can refer to the **AllClearID Data Breach Incident Response Workbook** for ideas: www.allclearid.com/data-breach/data-breach-response-plan.

... all year round:

- Display **STOP. THINK. CONNECT.** posters in your employee break room and work areas. Download posters from <http://www.stophinkconnect.org/resources/>.
- Include **STOP. THINK. CONNECT.** tips in employee handbooks and company newsletters: <http://www.stophinkconnect.org/tips-and-advice/>.
- Routinely review and update your Internet security policies to ensure that they address current threats and best practices, and provide clear guidance on workplace technology trends such as "bring your own device." Get more ideas for your business cybersecurity plan: <http://staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan/>.