October is National Cyber Security Awareness Month

Improving national cyber security is a crucial part of keeping America safe.

National Cyber Security Awareness Month was established to raise awareness and understanding about the importance of cyber security. Awareness Month activities help Americans learn about computer security essentials including: protection against viruses, worms, hacking, spyware, phishing, account hijacking, identity theft, and more, thus empowering all Americans to better protect themselves.

Annual programs in October focus on cyber security education for the following audiences:

- Home Users
- Small Businesses
- Education (K-12 and higher education)

Last year, we worked with nearly 90 public and private organizations to promote cyber security best practices nationwide during the October National Cyber Security Awareness Month and throughout the following year. We invite you to participate in a variety of National Cyber Security Awareness Month programs this October and watch for high-impact programs throughout the rest of the year.

National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) is the go-to resource for cyber security awareness and education for the home user, small business, and education professionals. A public-private sector partnership, NCSA sponsors and partners include the Department of Homeland Security, Federal Trade Commission, Department of Commerce, and many private sector corporations.

Our mission is to increase awareness and help all Americans learn effective responses to pressing cyber security and safety issues. NCSA provides tools and resources to empower home users, small businesses, schools, colleges, and universities to stay safe online.

Look for our Stay Safe Online national awareness programs or visit us at **www.staysafeonline.org** for easy-to-understand information on how to improve your cyber security.

For more information on the National Cyber Security Alliance initiatives and membership, please contact:

Alyssa Marlow
ncsaalyssa@aol.com
Manager of Programs and Communications
National Cyber Security Alliance

STAYSAFEONLINE.org
National Cyber Security Alliance

National Cyber Security Alliance

Is your business everybody's business?

Come in WE'RE OPEN
And so is access to our inventory and sales records, server passwords, profit margins, staff and customer information, bank account numbers and business start-up costs.

STAYSAFEONLINE.org
Make it a habit.

Stay safe! Here's 6 information security tips for small businesses

Small businesses and organizations may be daunted by the perceived resources it takes to secure their systems, however, not making cyber security a priority could be a costly decision. The following six tips represent key security principles that we recommend implementing in any business setting, and provide a starting point for a more effective information security plan.

It's our cyberspace. Let's keep it that way.

STAYSAFEONLINE.org
National Cyber Security Alliance

1 Ensure that all employees use effective passwords. Encourage passwords that are comprised of different characters and change them every three months. For example, use C@tandD0g. instead of catanddog.

2 Protect your systems. Install and use anti-virus, and anti-spyware, programs on all computers in your business. Install a software firewall on all computers that connect to the Internet.

3 Keep all software up to date. Ensure that all computer software is up to date and contains the most recent patches (i.e., operating system, anti-virus, anti-spyware, firewall, and office automation software). Without updates, your systems will not be well protected against new cyber threats.

4 Create backups. Make regular (weekly) backup copies of all of your important data/information. Store a secured copy away from your office location, and if that CD has sensitive information on your company or customers, use encryption to protect it.

5 Be prepared for emergencies. Create a contingency plan for your business so you can recover if you experience an emergency. Include plans to continue business operations at an alternate location when necessary. Test your plan at least annually.

6 Report Internet Crime. Locate and join an organization of your peers for information sharing purposes. If you suspect fraud or criminal intent, report it to the local law enforcement agencies, the local Federal Bureau of Investigation, Secret Service, or State Attorney General's offices.

Resources for Small Businesses

General Cyber Security Information for Small Business:

National Cyber Security Alliance (NCSA):
http://www.staysafeonline.org
Small Business Administration (SBA):
http://www.sba.gov
Federal Trade Commission (FTC) OnGuard Online:
http://onguardonline.gov/index.html
Better Business Bureau (BBB):
http://www.bbb.org/securityandprivacy/SecurityPrivacyMadeSimpler.pdf
Multi-State Information Sharing Analysis Center:
http://www.cscic.state.ny.us/msisac
United States Computer Emergency Readiness Team (US-CERT):
www.us-cert.gov
Carnegie Mellon CERT, Software Engineering Institute:
http://www.cert.org

Law Enforcement Resources:

If you suspect fraud or criminal intent, report it to: Internet Crime Complaint Center, which receives, develops, and refers criminal complaints regarding cyber crime.
www.ic3.gov
Local US Secret Service Office, list of field offices that handle crimes against businesses
http://www.secretservice.gov/field_offices.shtml
Federal Trade Commission (FTC):
http://www.ftc.gov
State Attorney Generals Office, National Association of Attorney Generals Cyber Crime Contact List
http://www.naag.org/issues/20010724-cc_list_bg.php

Other Helpful Information:

Locate and join an organization of your peers for information sharing/helping purposes, such as collaborative partnerships which educate consumers to prevent them from becoming victims of Internet fraud schemes: www.lookstoogoodtobetrue.com. Consider organizations such as InfraGard, www.InfraGard.net, which is an InfraGard National Members Alliance and Federal Bureau of Investigation's (FBI) critical infrastructure protection initiative. Be cognizant of diverse resources such as the FBI's http://www.fbi.gov/cyberinvest/cyberhome.htm.