



National Cyber Security Alliance

Topic: Assess the Nature of Our Cyber Security Vulnerabilities
Contact: Manager of Programs and Communications, Alyssa Marlow-Sunley
202-756-2284, ncsaalyssa@aol.com

Ensuring Consumers Do Not Become Our Biggest Cyber Security Vulnerability – Increasing Cyber Security, Safety and Ethics Education within the United States

The Internet, computers and now mobile devices continue to play a big part in our lives, helping us conduct research, find better paying jobs and connect with loved ones. However, if not properly secured and used, home users' computers and Internet connections can be accessed by cyber criminals to commit cyber crime with little detection, thereby creating a huge cyber security vulnerability that directly affects other consumers, businesses and our government. That is why the National Cyber Security Alliance is calling on state and national leaders to work with States' Departments of Education to develop a flexible framework for finding a way to ensure that comprehensive cyber security, safety and ethics lessons and programs are taught in every school across that state.

According to the Federal Bureau of Investigation (FBI), more than 1 million computers in the United States are already infected with malicious programs that allow cyber criminals to remotely use the computer to conduct criminal activity like phishing, spamming, distributing child pornography, extortion and even attacking our nation's critical infrastructure. Since the criminal activity is conducted on unsuspecting home users' or businesses' computers, there is very little anyone can do, short of notifying the computer owner, to stop these computers from continually being used to commit cyber crimes.

Americans' general lack of cyber security awareness and education within the United States is a probable cause for why so many computers are infected. According to a recent study conducted by McAfee and the National Cyber Security Alliance, 78% of Americans lack the protection to fight off a variety of cyber threats.

While the percentage of unsecured computers and lack of cyber security education is staggering, there is a way to bridge this cyber security knowledge gap. We need to enlist our nation's education system – schools, libraries, after school programs and PTA's – at the time these technologies are introduced in the classroom, to help make sure children, as future cyber citizens, learn how to properly secure and use a computer and the Internet. This education must continue throughout their primary and secondary scholastic careers.

Currently, very few states require cyber security, safety and ethics lessons and programs be taught within their schools and libraries. Moreover, there are even fewer states taking a statewide approach to ensuring schools, libraries and after school programs have the resources, know-how and the means to teach cyber security, safety and ethics programs. Only Virginia has a statewide approach that requires schools to teach cyber security, safety and ethics lessons, but also allowing the much needed flexibility on the local level to ensure local schools can pick the lessons they feel best address their local student population's needs.

This void can be filled if state and national leaders work with each States' Department of Education to develop a framework that can be used to incorporate comprehensive cyber security, safety and ethics lessons within already existing prevention curriculum. To find an example on such a framework go to:
<http://staysafeonline.org/whitepapers/CSAC3WhitePaper-Final081507.pdf>

Consumers' unsecured computers and Internet connections creates enormous cyber security vulnerability for other Internet users, businesses and our nation's critical infrastructure. Working with States' Departments of Education to develop a statewide approach to ensuring comprehensive cyber security, safety and ethics lessons taught in classrooms and libraries will help increase the education and awareness level of students and future home users. These lessons will thereby decrease the number of unsecured computers cyber criminals can access to conduct criminal activity online and help close this major cyber security vulnerability.