

A Shared Responsibility: Protecting Against Unseen Cyber Threats

By National Cyber Security Division
Office of Cybersecurity and Communications
U.S. Department of Homeland Security



STOP | THINK | CONNECT™

What would you do if you received a somewhat suspicious email from a friend that only included a link? Would you click on it? What would your spouse, children, friends, or colleagues do? Phishing attacks are only one of the many complex cyber threats we face every time we go online regardless of whether we are at home, at work, or on the go. As technology advances, so do the techniques cybercriminals use to gain access to our computer networks.

In the 21st Century, almost all aspects of society rely on computers and the Internet - communication (email, mobile phones), entertainment (digital cable, mp3s), transportation (car engines, airplane navigation), shopping (online stores, credit cards), medicine (prescriptions, medical equipment, medical records), and the list goes on. Our growing dependence on technology demands greater security online at home, at work, and in school.

Despite our dependence on technology, many individuals don't think about the inherent risks that come from being connected to a global network of people through the Internet. While the devastating effects on individuals, families, and communities caused from a fire, hurricane, tornado, or man-made disaster are easy to see, it is much more difficult to understand the impact of a sluggish computer infected with malware or viruses. Unlike physical threats that prompt immediate action - like stop, drop, and roll in the event of a fire - cyber threats are often difficult to identify and comprehend, yet can be just as dangerous.

Many of the crimes affecting individuals- including credit card fraud, sexual harassment, identity theft, child pornography, and embezzlement - are increasingly conducted, or at least facilitated through the Internet. Cybercriminals use malware and spyware to capture keystrokes, screenshots, passwords, and other personal information that may be used to execute financial crimes, identity theft and fraud, or spam. Malware can be installed by simply clicking on a suspicious URL, a malicious advertising banner or an infected image. Youth face the threat of cyberbullying and cyber predators and even the youngest children can be at risk for identity theft.

The problem with cybersecurity is not that our communities are unaware these crimes exist. Instead, the challenge is that many Americans are either unfamiliar with how to protect

themselves from cybercrime or they are simply unaware of their high potential of becoming victims in the first place. Because cybersecurity impacts everyone, it is becoming increasingly important for Americans of all ages to take part in the shared responsibility to secure cyberspace.

Cybersecurity involves protecting everything from our nation's critical infrastructure to Personally Identifiable Information or PII by preventing, detecting, and responding to cyber incidents. The spectrum of cyber risks is limitless; threats, some more serious and sophisticated than others, can have a wide-range of effects on the individual, community, organization, and even at the national level. Even though there is no guarantee against a cyber-attack, there are steps that individuals, communities, and organizations can all take to minimize the chances of becoming a victim of cybercrime.

Stop. Think. Connect.

Preparing for the unexpected fire, hurricane, tornado or man-made disaster may bring to mind routine safety procedures such as "72-hour" kits, evacuation plans, and other ways to help individuals, families and communities prepare for a disaster. Emergency preparedness is critical for helping Americans understand what to do before, during, and after an emergency. Similarly, cybersecurity awareness enhances understanding of how to prevent, detect, and respond to cyber incidents.

Recognizing that increasing awareness is a critical step towards improving the nation's overall cybersecurity posture, the Department of Homeland Security responded to the presidential directive for a national cybersecurity awareness campaign. The Stop.Think.Connect.™ Campaign was created to guide the nation to a higher level of Internet safety by challenging the American public to be more vigilant about practicing safer online habits.

Since its inception in 2010, the Stop.Think.Connect. Campaign has promoted cybersecurity as a shared responsibility working with all levels of government, industry, small business, non-profit organizations, and the general public to engage Americans of all ages in an ongoing cybersecurity dialogue.

The National Sheriffs' Association recently issued a resolution officially recognizing the Stop.Think.Connect. Campaign and its commitment to advancing cybersecurity awareness and

cybercrime prevention. As an organization representing law enforcement professionals across the country, the National Sheriffs Association plays a vital role in the DHS Stop.Think.Connect. Campaign's mission to proactively educate citizens about Internet-related crime, promote safer online behavior, and remind the public that in the cyber world—just like the physical world—there are real consequences.

Simple Tips to Protect Yourself Online

Across America, law enforcement officers work tirelessly to keep our nation safer and more secure. Despite your best efforts, it is simply impossible to do everything on your own. As trusted community leaders, you are instrumental in arming citizens with resources and tools needed to protect themselves, their families, and the nation against growing cyber threats. Individuals are our country's first line of defense in guarding against online risks, and the law enforcement community is crucial to preventing, detecting, and responding to cybercrime.

Increasing cybersecurity awareness is as simple as teaching the general public how to set up the proper controls. Stop.Think.Connect. recommends the following tips for protecting individuals, families, and communities before a cyber incident occurs.

- Only connect to the Internet over secure, password-protected networks.
- Do not click on links or pop-ups, open attachments, or respond to emails from strangers.
- Always enter a URL by hand instead of following links if you are unsure of the sender.
- Do not respond to online requests for Personally Identifiable Information or PII; most organizations – banks, universities, companies, etc. – do not ask for your personal information over the Internet.
- Limit who you are sharing information with by reviewing the privacy settings on your social media accounts.
- Trust your gut; if you think an offer is too good to be true, then it probably is.
- Password protect all devices that connect to the Internet and user accounts.
- Do not use the same password twice; choose a password that means something to you and you only; change your passwords on a regular basis.
- If you see something suspicious, report it to the appropriate authorities.

National Cyber Security Awareness Month occurs each October to remind us that being safer and more secure online is a shared responsibility.

Community Involvement in Stop.Think.Connect.

To encourage communities to embrace a more sustained, proactive approach towards online safety and cybercrime prevention, law enforcement professionals can join the Stop.Think.Connect. Campaign in enhancing cybersecurity awareness across the nation. The activities below are a few ways you can help better inform your community of growing cyber threats and how to protect against them.

- Join the Campaign through the Stop.Think.Connect. National Network or Cyber Awareness Coalition by working with your local or State government or nonprofits like D.A.R.E. or the National Sheriffs' Association.
- Become a Friend of the Campaign and receive a monthly newsletter with tips and resources for spreading cybersecurity awareness in your communities.
- Participate in Stop.Think.Connect. Cyber Tours that will occur across the country in 2013. To date, Boston, MA, Miami, FL, Twin Cities, MN, and Atlanta, GA have hosted Cyber Tour events to engage communities in an ongoing cybersecurity dialogue.
- Lead a cybersecurity awareness educational session or activity in a local school, library, recreational, or community center.
- Download and distribute Stop.Think.Connect. resources for all ages and organizations, which can be found on the Campaign's website.
- Blog, tweet, or post about Stop.Think.Connect. and provide tips for safer online behavior.
- Provide feedback to the Campaign on how Stop.Think.Connect. can better equip law enforcement to talk about and promote cybersecurity. 🌟

Cybersecurity Resources

The Stop.Think.Connect. Campaign: www.dhs.gov/stophinkconnect

United States Secret Service Electronic Crimes Task Force: www.secretservice.gov/ectf.shtml

Internet Crimes Complaint Center (IC3): www.ic3.gov

United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov

National Cyber Security Alliance (NCSA): www.staysafeonline.org