STOP.THINK.CONNECT.™

Law Enforcement & Cybersecurity

CYBERSECURITY IN YOUR COMMUNITIES

Unlike other threats currently facing the country, cyber attacks on individual citizens can have instant, wide-ranging consequences for the nation's broader national and economic security interests. No country, industry, community, or individual is immune to cyber risks, and no one government agency, company, or individual can solve the riddle of cybersecurity.

> Cybercrime costs the world significantly more than the global black market in marijuana, cocaine, and heroin combined. [i]

Across America, more than 800,000 law enforcement officers work to keep our nation safe and secure. As a law enforcement professional, you play a vital role in the Department of Homeland Security's (DHS) mission to proactively fight Internet-related crime, promote safer online behavior, and remind the public that behavior in the cyber world, just like the physical world, has real consequences.

DHS LAW ENFORCEMENT RESPONSIBILITIES

DHS components such as the United States Secret Service (USSS), Immigration and Customs Enforcement, Travel Security Administration, and the U.S. Coast Guard have law enforcement responsibilities across the nation in counterterrorism, border security, maritime security, and federal law enforcement. Through these various organizations, DHS upholds the larger law enforcement mission of protecting and defending the nation against all threats.

DHS collaborates with law enforcement in combating cybercrime through many ways including the following programs:

- **The Homeland Security Information Network** (HSIN) provides law enforcement officials at every level of government with a means to securely collaborate with partners across geographic and jurisdictional boundaries. Law enforcement organizations use HSIN to quickly share information with mission-specific contact lists including Be On the Lookouts (BOLOs), Requests for Information (RFIs), For Your Information (FYIs), Intelligence Reports, and other sensitive documents.
- **National Network**. To increase cybersecurity awareness across the country to people of all ages, the Stop.Think.Connect. Campaign established the National Network, which is comprised of not-for-profit groups and organizations that advocate and promote cybersecurity. D.A.R.E. is a member of the National Network and has collaborated with the Campaign on local outreach efforts and resource distribution.

> Stop.Think.Connect. trained over 1,500 D.A.R.E. officers to give cybersecurity presentations in schools and communities.

- **Cyber Awareness Coalition**. Federal agencies and State, local, tribal, and territorial governments from the Federal Bureau of Investigation (FBI) to the State of California are engaged in the Campaign. Coalition members through alerts, teleconferences, newsletters, and meetings make effective use of existing communications channels and outreach capabilities to spread the Stop.Think.Connect. messages.
- **Cyber Tours.** Stop.Think.Connect. Cyber Tours directly engage communities in promoting awareness and dialogue about the dangers Americans face online. Through a series of events and forums, Cyber Tours–with the help of law enforcement–bring together Federal, State and local entities, industry, academia, non-profits, and individual citizens to emphasize the impact Internet safety has on all segments of a community.

Help Spread the Word

HOW TO GET INVOLVED

As trusted community leaders, law enforcement officials are instrumental in advancing the DHS cyber mission of arming citizens with resources and tools needed to protect themselves, their families, and the nation against growing cyber threats. To get involved:

- Join the Campaign through the 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.
- Lead a cybersecurity awareness educational session or activity in a local school, library, recreational, or community center.
- Download and distribute Stop.Think.Connect. cybersecurity materials, including the Toolkit with resources for all ages and organizations.
- Blog, tweet, or post about Stop.Think.Connect. and safe online behavior.
- Provide feedback to the Campaign on how Stop.Think.Connect. can better equip law enforcement to talk about and promote cybersecurity.

RESOURCES AVAILABLE TO YOU

- **USSS Electronic Crimes Task Force.** The USSS' Electronic Crimes task Force seeks to prioritize investigative cases that involve some form of electronic crime by bringing together state and local law enforcement, prosecutors, private sector interests and academia in an effort to prevent cyber-crime and identity theft. The USSS provides information on how to respond to credit card fraud and identity theft.
- **Internet Crimes Complaint Center (IC3).** The IC3 was established as a partnership between the FBI and the National White Collar Crime Center to provide a central referral mechanism for complaints involving internet related crimes for law enforcement and regulatory agencies at the federal, state, local, and international level.
- **United States Computer Emergency Readiness Team (US-CERT).** US-CERT leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation. US-CERT responds to incidents; provides technical assistance to information system operators; and disseminates timely tips and notifications regarding current and potential security threats and vulnerabilities.
- **National Cyber Security Alliance (NCSA).** NCSA's mission is to educate and empower a digital society to use the Internet safely and securely. NCSA provides downloadable educational materials for the home, classroom, and office.

Stop.Think.Connect. The DHS Stop.Think.Connect. Campaign is a national public awareness effort, initiated by President Obama, that seeks to guide the nation to a higher level of Internet safety by empowering the American public to be more vigilant about practicing safe online behavior. The Campaign seeks to persuade Americans to view Internet safety as a shared responsibility—at home, in the workplace, and in our communities.

---

i. 2012 Norton Cybercrime Report