LAW ENFORCEMENT & CYBERSECURITY

CYBERSECURITY IN YOUR COMMUNITIES

Cyber attacks on individual citizens, communities, or organizations 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 thwart risks alone. We all have a role to play in stopping cybercrime – criminal activities that either target or are facilitated through a computer or network, such as through hacking, fraud, identity theft, and copyright infringement.

Across America, more than 800,000 law enforcement officers work to keep our nation safe and secure. Law enforcement professionals 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.

In 2012, Norton reported that cybercrime costs the world significantly more than the global black market in marijuana, cocaine, and heroin combined.[1]

DHS LAW ENFORCEMENT RESOURCES

DHS components such as the United States Secret Service, Immigration and Customs Enforcement, Travel Security Administration, and the U.S. Coast Guard have law enforcement responsibilities across the nation, including working to protect the nation against cyber threats. DHS works 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 a way to collaborate securely 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. More information is available at www.dhs.gov/homeland-security-information-network.
- **Project iGaurdian**. Project iGuardian is a first-of-its-kind national cyber safety campaign spearheaded by U.S. Immigration and Customs Enforcement's Homeland Security Investigations in partnership with the National Center for Missing & Exploited Children. Its mission is to help kids, teens and parents to be smart about online safety and stay safe from online sexual predators. For more information, visit www.ice.gov/cyber-crimes/iguardian.htm.

[1] Norton 2012 Cybercrime Report 2012

- **Stop.Think.Connect.™ Campaign**. Together with the National Cyber Security Alliance, DHS leads Stop.Think.Connect.™, a national public awareness campaign to increase the understanding of cyber threats and empower the American public to be safer and more secure online. It offers several ways of connecting the law enforcement community with cybersecurity resources through its website, www.dhs.gov/stopthinkconnect, and other programs:
    - **National Network**. To increase cybersecurity awareness across the country among people of all ages, the Campaign established the National Network, a group of non-profit organizations that advocate and promote cybersecurity. Law enforcement organizations including the International Association of Chiefs of Police, the National Sheriffs' Association, and D.A.R.E. are members of the National Network and work with the Campaign on local outreach efforts and resource distribution.
    - **Cyber Awareness Coalition**. Federal agencies and State, local, tribal and territorial governments across the country are engaged in the Campaign's Cyber Awareness Coalition. Coalition members use existing communications channels and outreach capabilities to share cybersecurity information through alerts, teleconferences, newsletters, and meetings.
    - **Speaking engagements**. The Campaign directly engages communities in promoting awareness and dialogue about the dangers Americans face online. Through speaking engagements, the Campaign–with the help of law enforcement and other Campaign partners–emphasizes the impact Internet safety has on entire communities.

The Stop.Think.Connect.™ Campaign works with law enforcement officers to give cybersecurity presentations in schools and communities across the nation.

HELP SPREAD THE WORD

HOW TO GET INVOLVED

As trusted community leaders, law enforcement officials can advance the DHS cyber mission of arming citizens with resources and tools needed to protect themselves, their families, and the nation against growing cyber threats.

- Join the Campaign through the National Network or Cyber Awareness Coalition. Or work with existing Campaign members in your local or State government or non-profits 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

- **U.S. Secret Service Electronic Crimes Task Forces**. The Secret Service's Electronic Crimes Task Forces 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 Secret Service provides information on how to respond to credit card fraud and identity theft. For more information, visit www.secretservice.gov/ectf.shtml.
- **Internet Crimes Complaint Center (IC3)**. The IC3 was established as a partnership between the Federal Bureau of Investigation 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. For more information, visit www.ic3.gov.
- **United States Computer Emergency Readiness Team (US-CERT)**. US-CERT leads efforts to make sure the nation is prepared to handle cybersecurity incidents, including sharing information about threats. 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. For more information, visit www.us-cert.gov.
- **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. For more information, visit www.staysafeonline.org.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and you community. For more information visit http://www.dhs.gov/stopthinkconnect.