Homeland Security

DHS Highlights Personal and Business Preparedness During National Cyber Security Awareness Month

SHARE

Release Date: October 1, 2008

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Fact Sheet: National Cyber Security Awareness Month

The U.S. Department of Homeland Security's National Cyber Security Division is sponsoring the fifth annual National Cyber Security Awareness Month this October, designed to educate the public on the shared responsibility of protecting cyberspace. The department will recognize this important initiative through a series of events aimed at raising awareness of the ways in which citizens and businesses can better safeguard themselves in cyberspace.

"Cyber attacks are increasing in sophistication and frequency every day. They include a broad spectrum of nefarious activity – from an individual hacker, to an organized criminal group stealing information or identities, to nation states engaged in cyber espionage," said Homeland Security Secretary Michael Chertoff. "We have embarked on a massive effort to guard federal systems and to work with industry to defend our critical infrastructure. Because no single entity owns the Internet, the federal government needs the cooperation of both the private sector and everyday citizens to protect against a range of cyber threats."

Everyone can practice good cyber security in their homes and offices. Installing virus detection software and updating it as necessary, creating strong passwords and frequently changing them, backing up important files, and ignoring suspicious e-mails or websites can help protect you, your family and your business.

DHS employs numerous strategies to increase the security, resiliency, and reliability of the nation's information technology (IT) and communications infrastructure:

- **U.S. Computer and Emergency Readiness Team (US-CERT)** – The department's 24-hour watch and warning center for the federal government's Internet infrastructure.
- **EINSTEIN Program**
  – Intrusion detection tool that identifies malicious activity on our federal networks. DHS is currently developing an updated version of this software, EINSTEIN 2, which will be able to detect intrusion in real time.
- **National Cyber Security Center**
  – A networked partnership of the federal agencies responsible for cyber defense, created to leverage their strengths and promote best practice sharing and coordination.
- **National Cyber Investigative Joint Task Force** – Team of federal agencies, including the United States Secret Service, charged with coordinating, integrating, and sharing pertinent information related to cyber threat investigations.
- **Cyber Security Exercises**
  – This March, the department led the nation's largest cyber security exercise, known as Cyber Storm II, during which participants from all levels of government, the private sector and the international community engaged in a simulated cyber attack on several critical sectors of our economy.
- **Expanded Cyber Education**
  – DHS engages in partnerships with academia and industry to expand cyber education for all U.S. government employees, particularly those specializing in IT, and to continue recruiting a capable and knowledgeable workforce to combat emerging threats.
- **Increased Funding**
  – The President's FY 2009 Budget requested $7.2 billion for IT efforts, a $600 million increase over last year's budget.

For more information on how you can protect yourself against cyber attacks, please visit www.staysafeonline.org. To report an incident or cyber vulnerability, please visit www.us-cert.gov.

###

This page was last reviewed/modified on October 1, 2008.