

STOP.THINK.CONNECT.™

Government Tip Card

DID YOU KNOW?

- The Federal Government faces an average of 15,000 cyber attacks on its networks per day. ⁱ
- Information security incidents at 24 federal agencies have increased 650% during the past five years due to a combination of more numerous threats and persistent shortcomings in security controls. ⁱⁱ
- In 2010, 55% of security staff members within state governments identified accidental breaches of information originating from inside the enterprise, including the loss of unencrypted lap tops and hard drives. ⁱⁱⁱ

SIMPLE TIPS

- Lock and password protect all personal and company-owned devices including smart phones, laptops, notebooks, and tablets.
- Regularly scan your computer for spyware and keep your software up to date.
- Dispose of sensitive information properly.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

RESOURCES AVAILABLE TO YOU

- *USCERT.gov*
 - The United States Computer Emergency Readiness Team's (US-CERT) has a desktop software tool to assess control systems and information technology network security practices.
- *NIST.gov*
 - The National Institute of Standards and Technology (NIST) Computer Security Division Computer Security Resource Center (CSRC) provides computer security resources and oversees the national guidance on setting the security configuration of operating systems and applications.
- *MSISAC.org*
 - The Multi-State Information Sharing and Analysis Center (MS-ISAC) comprises members of all 50 states, local governments, and U.S. territories and districts, and provides downloadable awareness materials including newsletters, posters, bookmarks, and briefings.

IF YOU'VE BEEN COMPROMISED

- Notify your organization and the authorities.
- Report your incident with the Internet Crime Complaint Center at <http://www.ic3.gov>.

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 your community. For more information visit <http://www.dhs.gov/stophinkconnect>.

ⁱ Nextgov, <http://www.nextgov.com/governing-security-in-a-networked-world/>

ⁱⁱ Government Accountability Office, <http://gcn.com/articles/2011/10/24/fbi-official-alternate-internet.aspx>

ⁱⁱⁱ Deloitte-NASCIO Cybersecurity Study, 2010