



GOVERNMENT TIP CARD

Cybersecurity should be a serious concern for employees across all levels of government – not just the IT department.

DID YOU KNOW?

- The Federal Government millions of cyber attacks on its networks per day; the Department of Defense¹ and National Nuclear Security Administration² alone each report **10 million attacks** on their systems every day. State governments also face hundreds of thousands³ of attacks daily.
- Information security incidents at 24 federal agencies increased **650 percent between** 2006 and 2011 due to a combination of more numerous threats and persistent shortcomings in security controls.⁴ They have continued to rise since 2011.⁵
- In fiscal year 2012, more than **two-thirds of cyber incidents** reported to the Federal Government were phishing attempts.⁶
- Between 2009 and 2012, **48 percent of government data breaches** stemmed from accidental exposure from inside the enterprise or the loss and theft of mobile devices like laptops and hard drives.⁷

SIMPLE TIPS

1. Lock and password protect all personal and agency-owned devices including smart phones, laptops, notebooks, and tablets. Encrypt data where applicable. Talk to your information technology department about encrypting your data.
2. Regularly scan your computer for spyware and keep your software up to date.
3. Dispose of sensitive information properly according to your organization's policies.
4. 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.
5. Take advantage of cybersecurity training offered by your agency or department.

¹ Defense News, "U.S. Military Goes on Cyber Offensive," March 2012

² US News & World Report, "U.S. Nukes Face Up to 10 Million Cyber Attacks Daily," March 2012

³ WMMT, "Michigan fends off 187,000 cyber attacks a day," WMMT, March 2013

⁴ "Information Security: Weaknesses Continue Among New Federal Efforts to Implement Requirements," [Washington, DC: Government Accountability Office Report 12-137, October 2011]

⁵ "Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002," [Washington, DC: Office of Management and Budget, Executive Office of the President of the United States, March 2013]

⁶ "Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002," [Washington, DC: Office of Management and Budget, Executive Office of the President of the United States, March 2013]

⁷ Government Computer News, "Forget Hackers, the Fool Next to You is the Real Threat," September 2012

RESOURCES AVAILABLE TO YOU

Several organizations offer resources that can help you prepare for cyber incidents before they happen to maintain a safe cyber environment. These include:

US-CERT.gov

The United States Computer Emergency Readiness Team's (US-CERT) shares cybersecurity tips and best practices, along with responding to cyber incidents and providing specialized software tools.

NIST.gov

The National Institute of Standards and Technology (NIST) 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:

If you believe your computer or your organization's systems have fallen victim to a cyber attack, be sure to work with your organization's IT department and follow its security policies. If you believe criminal activity has occurred:

- Notify your organization and the authorities.
- Report your incident with the [Internet Crime Complaint Center \(IC3\)](http://www.ic3.gov) at www.ic3.gov. IC3 is a partnership between the [Federal Bureau of Investigation \(FBI\)](http://www.fbi.gov) and the [National White Collar Crime Center \(NW3C\)](http://www.nw3c.gov) to receive Internet-related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for an investigation as appropriate.

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>.



Homeland
Security

www.dhs.gov/stopthinkconnect



STOP | THINK | CONNECT™