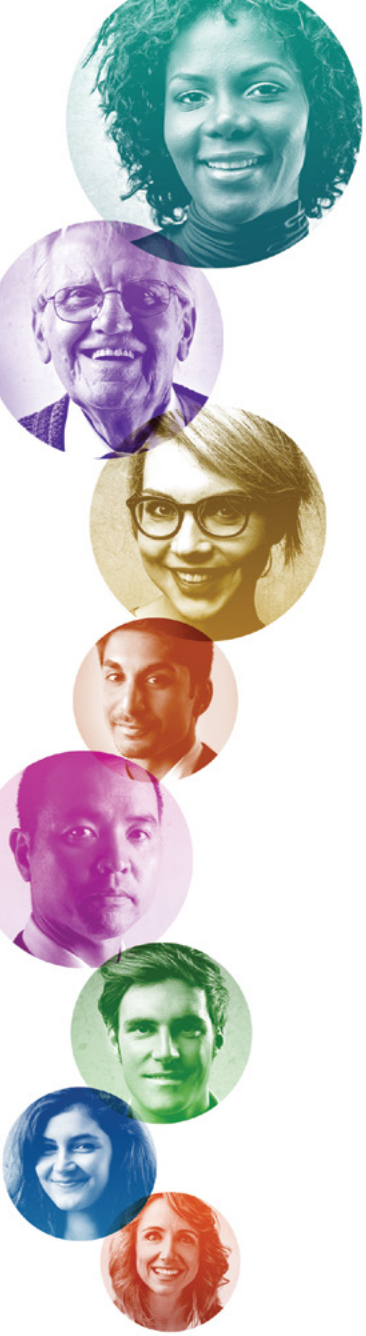


GOVERNMENT TIP CARD

As a government employee, you likely have access to sensitive information whether you realize it or not. Whether you're dealing with sensitive information or seemingly less-important documents, a criminal can utilize this information to their advantage. It is important to safeguard the information you work with to protect yourself and your organization.

DID YOU KNOW?

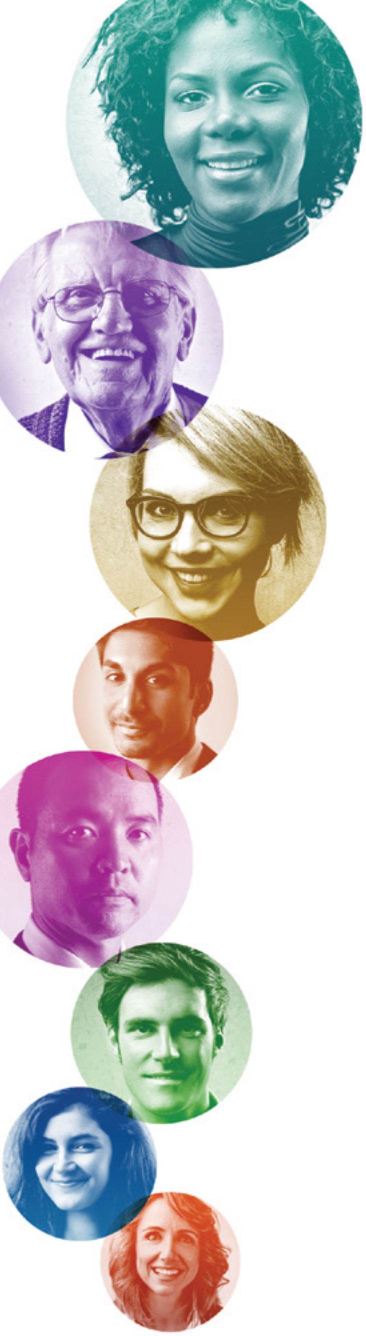
- The number of reported cyber incidents involving federal and state, local, tribal, and territorial government agencies increased by **26 percent** between 2012 and 2013, from approximately 158,000 incidents to 218,000 incidents.[1]
- In fiscal year 2013, more than **69 percent of incidents** reported to The United States Computer Emergency Readiness Team (US-CERT) were phishing attempts.[2]

SIMPLE TIPS

1. Lock and password protect all personal and agency-owned devices including smartphones, laptops, and tablets. This includes locking your computer when you step away from your desk at work. You may not always know the people walking around your office and what their intentions are. Encrypt data and use two-factor authentication where possible.
2. Regularly scan your computer for viruses and spyware and keep your software up to date.
3. Dispose of sensitive information properly and 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 department or agency.
6. Conceal your work badge and identification when outside of your office building, especially when out in public or when using public transportation.

[1] "Fiscal Year 2013 Annual Report to Congress: Federal Information Security Management Act." (Washington, DC: Office of Management and Budget, Executive Office of the President of the United States, March 2014)

[2] Ibid



RESOURCES AVAILABLE TO YOU

Several organizations offer resources that can help you prepare for cyber incidents before they occur. These include:

US-CERT.gov

The United States Computer Emergency Readiness Team (US-CERT) shares cybersecurity tips and best practices, responds to cyber incidents, and provides 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) at www.ic3.gov. IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to receive Internet-related criminal complaints and to further research, develop, and refer criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for 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™