



INDUSTRY EMPLOYEES TIP CARD

DID YOU KNOW?

- Nearly **two-thirds (64%) of data breaches** can be accounted for by employee negligence and system glitches together. These can include employees mishandling information and violations of industry and government regulations. ¹
- **Fifty-three percent of companies** in a study said that employees use their company-issued devices to send business related emails to cloud-based accounts like Gmail, leaving the information vulnerable to a data leak. ²
- A combined **92% of human resource professionals** said increased vulnerability of business technology to attack or disaster will have an effect on the U.S. workplace in the next five years. ³

SIMPLE TIPS

1. Read and abide by your company's Internet use policy.
2. Make your passwords complex. Use a combination of numbers, symbols, and letters [uppercase and lowercase].
3. Change your passwords regularly [every 45 to 90 days].
4. Don't share any of your user names, passwords, or other computer or website access codes.
5. Only open emails or attachments from people you know.
6. Never install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
7. Make electronic and physical back-ups or copies of all your most important work.
8. Report all suspicious or unusual problems with your computer to your IT department.

RESOURCES AVAILABLE TO YOU

US-CERT.gov

The United States Computer Emergency Readiness Team's (US-CERT) has numerous tips and resources on topics like choosing and protecting passwords, email attachments, and safely using social networks.

¹ 2013 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2013

² 2013 Data Breach Investigation Report conducted by Verizon, <http://www.verizonenterprise.com/DBIR/2013/>

³ Ibid.



FBI.gov

The Federal Bureau of Investigation leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber frauds.

CyberCrime.gov

The Department of Justice component responsible for implementing national strategies in combating computer and intellectual property crimes worldwide.

StaySafeOnline.org

The Stop.Think.Connect.™ Campaign is a cooperative agreement between the Department of Homeland Security and the National Cyber Security Alliance [NCSA]. Get more information from NCSA about the Stop.Think.Connect.™ Messaging Convention, which is the formal way that industry participates in Campaign activities.

IF YOU'VE BEEN COMPROMISED

- Report it to your manager or contact the IT or legal department to report the incident.
- Keep and record all evidence of the incident and its suspected source.
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.US-CERT.gov, if applicable.
- Report fraud to Federal Trade Commission at www.ongaurdonline.gov/file-complaint, if applicable.

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™
