STOP.THINK.CONNECT.™

Industry Leadership Tip Card

DID YOU KNOW?

- Industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion. [i]
- In a 2010 Data Breach Investigations Report, 70% of security breaches were caused by external agents, largely organized criminals; of the internal security breaches, 90% were the result of deliberate and malicious activity. [ii]
- 96% of breaches were avoidable through simple or intermediate controls. [iii]

SIMPLE TIPS

- Implement a layered defense strategy that includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement technical defenses, such as firewalls, intrusion detection systems, and Internet content filtering.
- Update your anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all of your software.
- Monitor, log, and analyze successful and attempted intrusions to your systems and networks.

RESOURCES AVAILABLE TO YOU

- *US-CERT.gov*
  - The United States Computer Emergency Readiness Team's (US-CERT) has numerous resources and tips for both technical and nontechnical individuals. The tips above were taken from their Protect Your Workplace brochure. The US-CERT desktop software tool can be used to assess control systems and information technology network security practices.
- *FBI.gov*
  - The Federal Bureau of Investigation (FBI) 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 (DOJ) 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 computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.US-CERT.gov.
- Inform local law enforcement of the state attorney general as appropriate.
- Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center at www.ic3.gov.
- Report fraud to Federal Trade Commission at www.ongaurdonline.gov/file-complaint.

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.

---

[i] White House Cyberspace Policy Review http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[ii] 2010 Data Breach Investigation Report conducted by Verizon in cooperation with the United States Secret Service http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

[iii] Ibid