STOP.THINK.CONNECT.™

Industry Employees Tip Card

DID YOU KNOW?

- 66% of employers monitor Internet connections for inappropriate Web surfing. [i]
- The 30% of bosses who have fired workers for Internet misuse cite the following reasons: viewing, downloading, or uploading inappropriate/offensive content (84%); violation of any company policy (48%); excessive personal use (34%); other (9%). [ii]
- The majority of people use poor passwords; 42% used only lower alpha passwords and 19% used numeric only with the most common password being 123456, according to an analysis of 10,000 leaked passwords in 2009. [iii]

SIMPLE TIPS

- Read and abide by your company's Internet use policy.
- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your user names, passwords, or other computer or website access codes.
- Do NOT open e-mails or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
- Make electronic and physical back-ups or copies of all your most important work.
- 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) US-CERT has numerous tips and resources on topics like choosing and protecting passwords, e-mail attachments, and safely using social networks. The tips above were taken from their Protect Your Workplace brochure.
- *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.

Homeland Security

STOP | THINK | CONNECT™

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.

[i] 2007 Electronic Monitoring & Surveillance Survey from American Management Association (AMA) and The Policy Institute http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/

[ii] Ibid

[iii] http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/