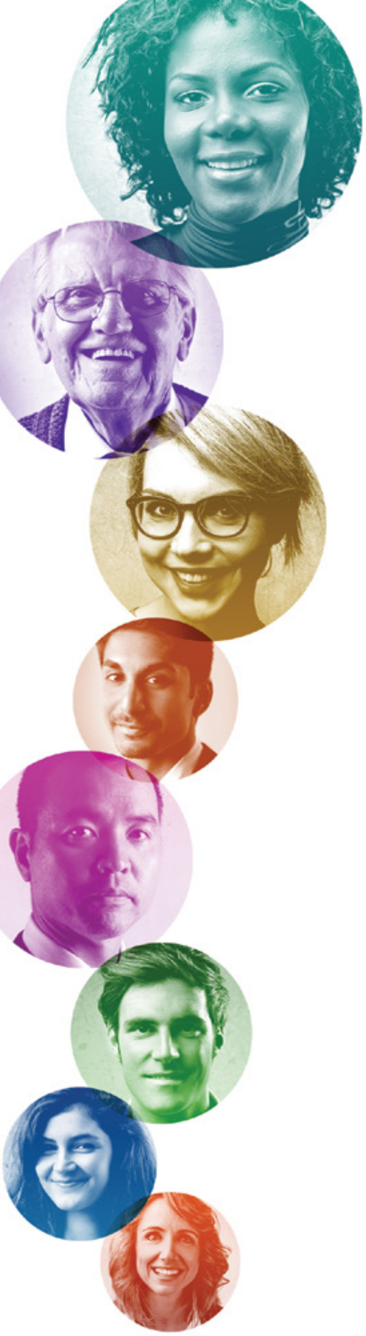


INDUSTRY EMPLOYEES
TIP CARD

All employees play an important role within their organization. Each person must employ proper cybersecurity practices to ensure that all work-related information stays safe and secure. When each person makes a conscious and proactive effort to learn about cybersecurity, they enhance the company's ability to guard and protect the organization from vulnerabilities.

DID YOU KNOW?

- A combined **92 percent 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.**[1]

SIMPLE TIPS

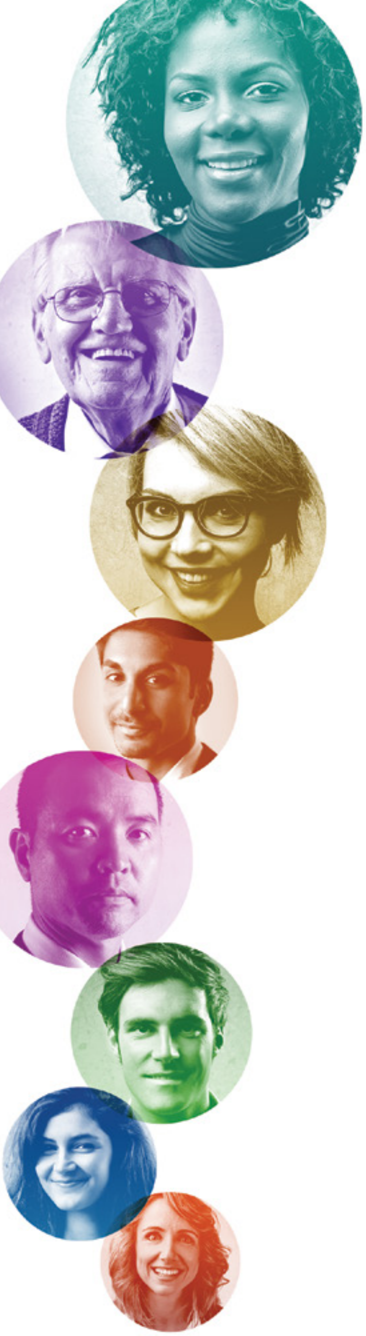
1. Read and abide by your company's Internet use policy.
2. Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
3. Change your passwords regularly (every 45 to 90 days).
4. Don't share any of your user names, passwords, or other computer or website 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 (US-CERT) has numerous tips and resources on topics like choosing and protecting passwords, email attachments, and safely using social networks.

[1] SHRM, "SHRM Workplace Forecast: The Top Workplace Trends According to HR Professionals," 2013



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 crimes.

CyberCrime.gov

Cybercrime.gov is the Department of Justice component responsible for implementing national strategies in combating computer and intellectual property crimes worldwide.

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 the Federal Trade Commission at www.onguardonline.gov/file-complaint, if applicable.
- If someone has had inappropriate contact with you or a colleague, report it to www.cybertipline.com and they will coordinate with the FBI and local authorities. You can also report it to the Department of Justice at www.justice.gov/criminal/cybercrime/reporting.html.

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™