



---

# EMPLOYEE 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?

- Nearly **two-thirds 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.<sup>1</sup>
- **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.<sup>2</sup>
- 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.<sup>3</sup>
- There was a **91 percent increase** in targeted cyber attack campaigns in 2013.<sup>4</sup>

## 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).
- Don't share any of your user names, passwords, or other computer or website access codes.
- Only open emails or attachments from people you know.
- Never 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.

---

<sup>1</sup> Symantec, "Mistakes are costing companies millions from avoidable data breaches," 2013.

<sup>2</sup> Business News Daily, "Inside Job: How to Prevent Employee Data Breaches," 2013.

<sup>3</sup> SHRM, "SHRM Workplace Forecast: The Top Workplace Trends According to HR Professionals," 2013.

<sup>4</sup> Symantec, "2014 Internet Security Report," 2014.



## 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.

### 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

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](http://www.US-CERT.gov), if applicable.
- Report fraud to the Federal Trade Commission at [www.onguardonline.gov/file-complaint](http://www.onguardonline.gov/file-complaint), if applicable.
- If someone has had inappropriate contact with you or a colleague, report it to [www.cybertipline.com](http://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](http://www.justice.gov/criminal/cybercrime/reporting).

[www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect).

[www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect)

