1 in 5

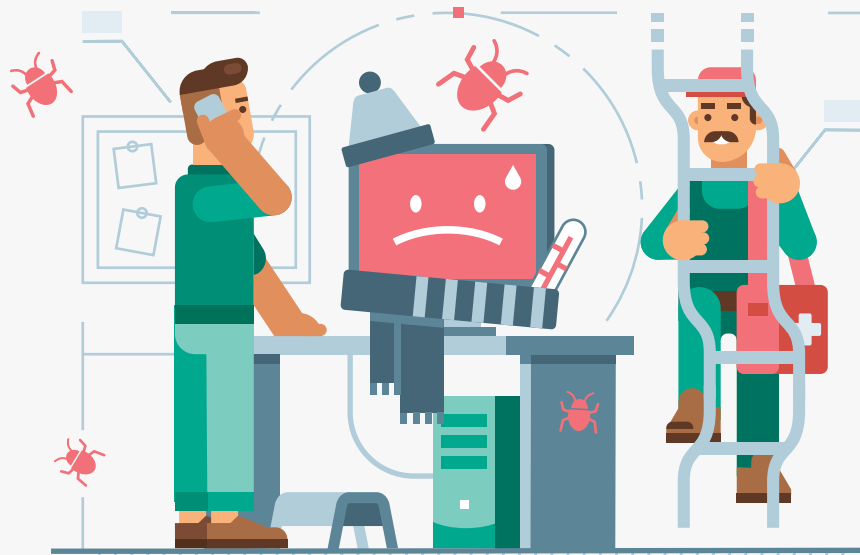## Serious breaches caused by careless or uninformed employees

Corporate IT Security Risks Survey 2016

Employees make up the front line of your organization's cybersecurity defenses. Give them the knowledge and motivation they need to keep cybercriminals away from your data.

What employee risks do businesses fear most?

47%	46%	44%	43%	43%
Inappropriate sharing of data via mobile devices	Physical loss of mobile devices exposing organization	Inappropriate IT resource use by employees	Incidents affecting suppliers involving shared data	Incidents involving non-computing, connected devices

Source: Kaspersky Lab's *The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within*

10 Ways to Teach Employees to Catch Cyberthreats

Keep on talking.

Plan regular cybersecurity chats to keep employees engaged. After all, it only takes one wrong click or download to let cybercriminals in.

1

Start at the top.

2

Don't bend the rules for executives. They're often targeted because they can access more information—and lead to a bigger payoff.
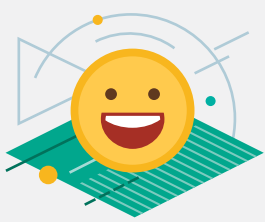
Set expectations.

Explain that a system is only as secure as its weakest link, and you can't cover every angle of attack. Mistakes will be made, but everyone must participate.

3

Train often.

4

Hold regular sessions and make them useful for work *and* home. Use real-world examples that frequently appear in social media and the news.
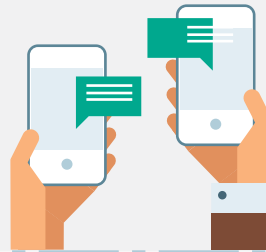
Beware social engineering.

Social engineering exploits employees who want to be helpful. Train your team in proper procedure, so cybercriminals move on to an easier target.

5

Emphasize early detection.

6

Communicate step-by-step instructions on what to do if an employee believes there's a cyberincident happening.

Create a safe space.

It's a problem if people feel reluctant speak up. Train your IT staff to be respectful when employees raise an issue—then stop false alarms with additional training.

7

Plan for incidents.

8

If you don't have a plan in place, you might increase the impact of an attack. Who talks to the press? Do you need insurance? Are you all on the same page?

Test their knowledge.

Don't let a real cyberattack be the first time an employee's knowledge is tested. Plan regular, relevant testing. Make it fun and rewarding!

9

Listen to feedback.

10

Encourage honest discussions to find out when policies are unmanageable for employees—and the real reasons behind mistakes, workarounds and violations.

For more information about employee cybersecurity risks and education, download our eBook, *The Threats from Within*.