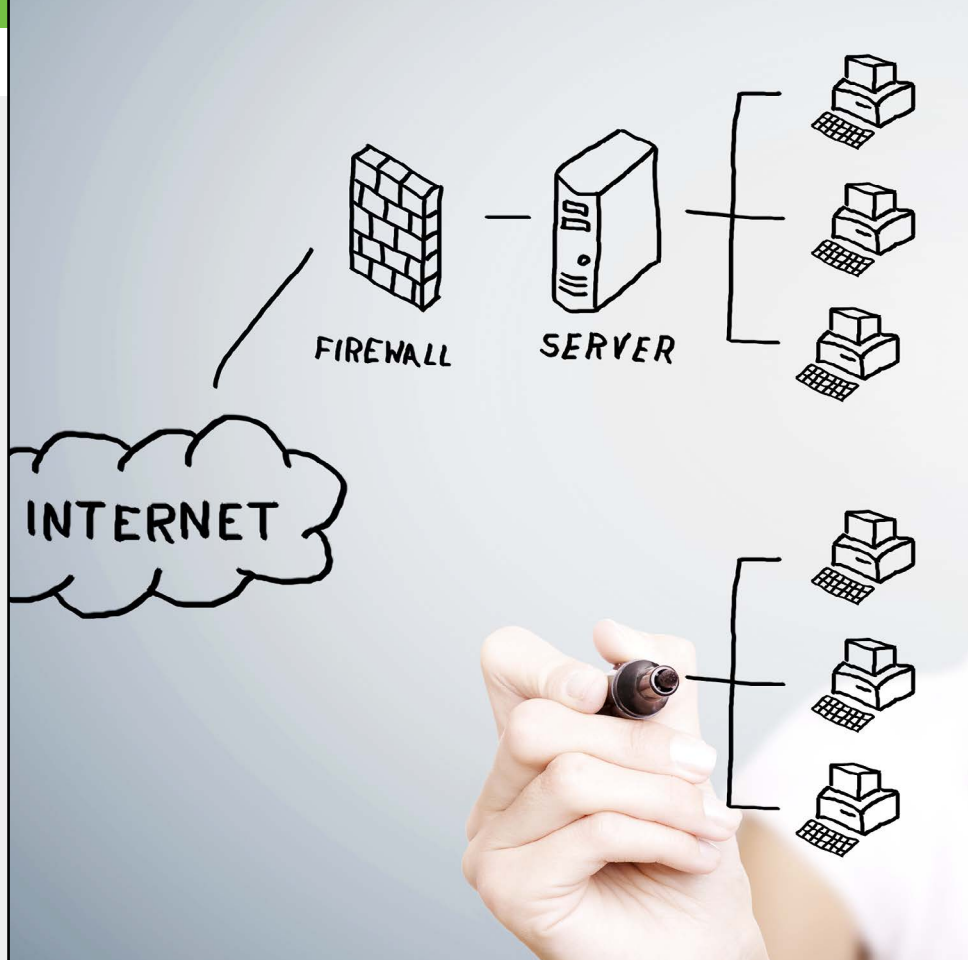
KASPERSKY lab

# TOP 10 TIPS FOR EDUCATING EMPLOYEES ABOUT CYBERSECURITY

# An Inside Job

Cyberthreats to your business are usually blamed on outsiders—nefarious programmers writing malicious code designed to pilfer your corporate intelligence, syphon your confidential customer information, and/or raid your financial data. Sometimes, the threat actually originates from within when employees' ignorance and/or negligence opens the door for cybercriminals.

This eBook is designed to provide you with tips for educating your employees about cybersecurity and helping them learn what they can do (and not do) to keep your business safe.



## Tip #1:

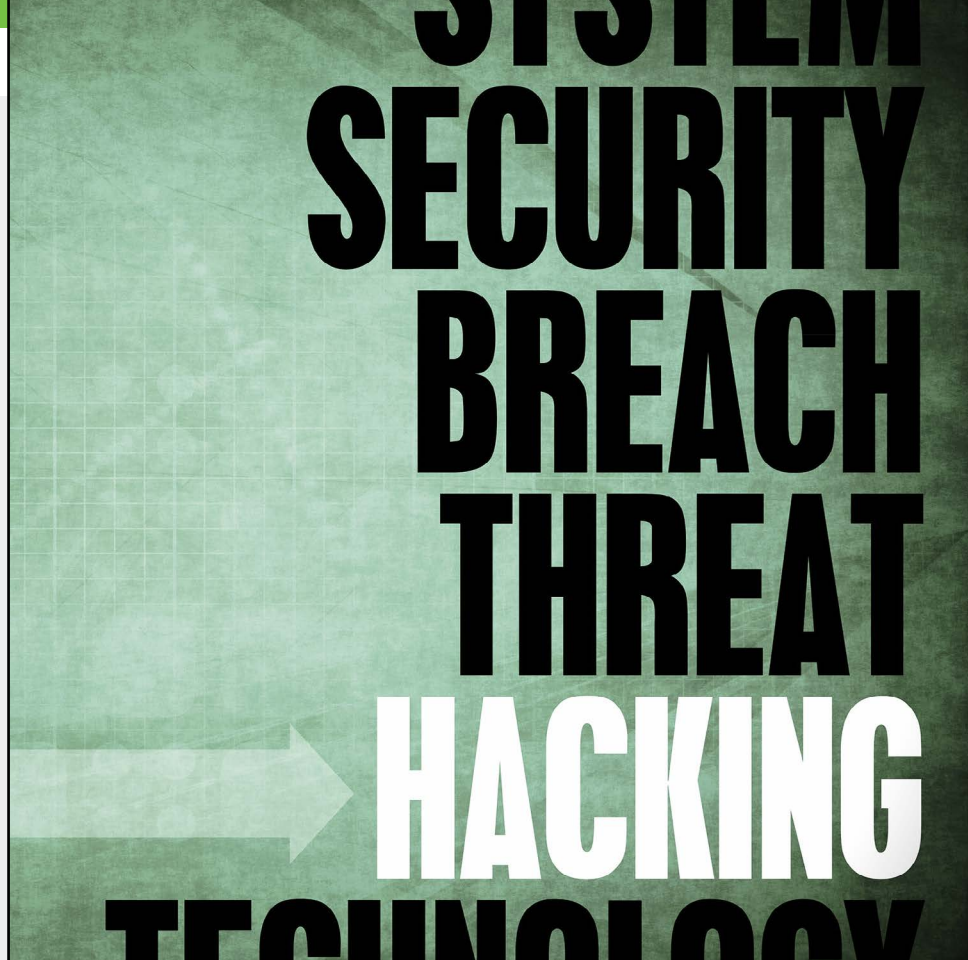
### Create and communicate clear-cut security policies.

Develop a precise set of rules for appropriate employee behavior on company computers. Employees should know the rules for email, web browsing, mobile devices, and social networks. An IT policy should include everything from the need to put a computer to sleep when employees leave their desks to instructions for encrypting sensitive emails and everything in between.  Some companies err on the side of vagueness with these policies in the hopes that they won't have to update them too often to reflect new technology. This is a mistake. If there is any lack of clarity, you run the risk of varied interpretations and inadvertent violations of the rules, putting your company at risk.

## Tip #2:

### Test employees' security knowledge.

In addition to including your organization's internet policy in the new employee orientation process, many successful businesses regularly test employees' knowledge of safe online behavior. These tests can be administered online and include positive reinforcement for completing the requirement. It's also important to regularly update staff about new cyberthreats and continually reinforce the message that employees must stay vigilant to protect customer, colleague, and corporate information, and, ultimately, their jobs.



# Tip #3:

## Require complex passwords that must be updated regularly.

It doesn't take a genius criminal mind to decipher the most popular passwords. According to Splash Data, the most popular password in 2013 was "123456."[1]

According to security experts at Threatpost, weird works best when it comes to passwords.[2] Even with complex passwords, it's important to change them regularly to avoid potential data breaches. Computers infected with keylogging malware can capture keystrokes and steal sensitive information from users as was the case in a recent hotel data breach.[3] Savvy organizations build in system requirements that require employees to change their passwords on a regular basis. Employees should also be instructed not to post passwords in their public workspaces.

1 Gizmodo, "The 25 Most Popular Passwords of 2013: God Help Us", January, 2014
2 Threatpost, "Weird Works Best When It Comes to Passwords," August, 2010.
3 Krebs on Security, "Beware Keyloggers at Hotel Business Centers," July 2014

# Tip #4:

## Teach employees to avoid phishing scams.

Cybercriminals use social engineering to defraud users of their financial information by deceiving them into handing over confidential information. Phishing remains the primary method for infecting users via social engineering, especially for corporate employees. Employees should know that, when in doubt, they should not click on or repost suspicious links in email, tweets, posts, online ads, messages,or attachments – even if they know the source. Phishing schemes are probably one of the most prevalent methods that cybercriminals use to target businesses via employees.

Phishers use fake websites that are expertly designed to imitate the originals. To make the fraudulent website less conspicuous, the cybercriminals use URL addresses that are very similar to those of the original sites with different variations on the line in the address bar. Advise employees to access financial sites from bookmarks in their browsers rather than by following an email link and avoid clicking on links from unknown email addresses.

Some business owners are under the impression that, if there is a data breach conducted via a false bank phishing scheme, the named financial institution is liable. Not true. In fact, “recent court rulings suggest that banks need to only show that they have ‘reasonable security measures’ to protect their business customers.”[4]

4 Forbes, “Don’t Let Your Business Pay the Price for Bank Fraud,” July 2014

# Tip #5:

## Create systems to automatically back up work.

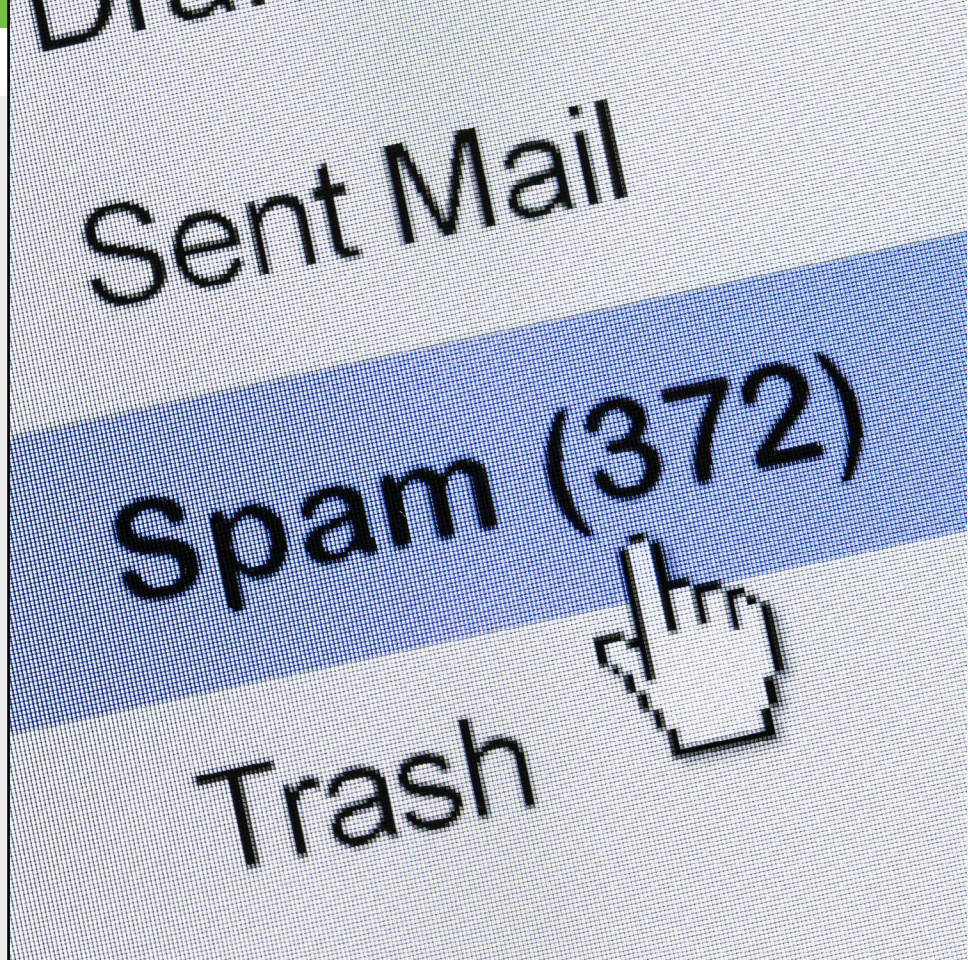
Even if your organization has protection in place to prevent a cyberattack, a data breach is still a real possibility and it can be a financially devastating event. Mitigating the damage can mean the difference between recovery and ruin. According to a recent Ponemon study, the average total cost of a data breach increased 15 percent from 2013 to $3.5 million in 2014.[5] It's important to encourage and even require employees to regularly back up their work in the event of a breach. Some systems will not allow people to shut down computers without first backing up the day's work.

5 Ponemon Institute, *2014 Cost of Data Breach Study,* May 2014

## Tip #6:

### Use spam and web filters to close windows of vulnerability

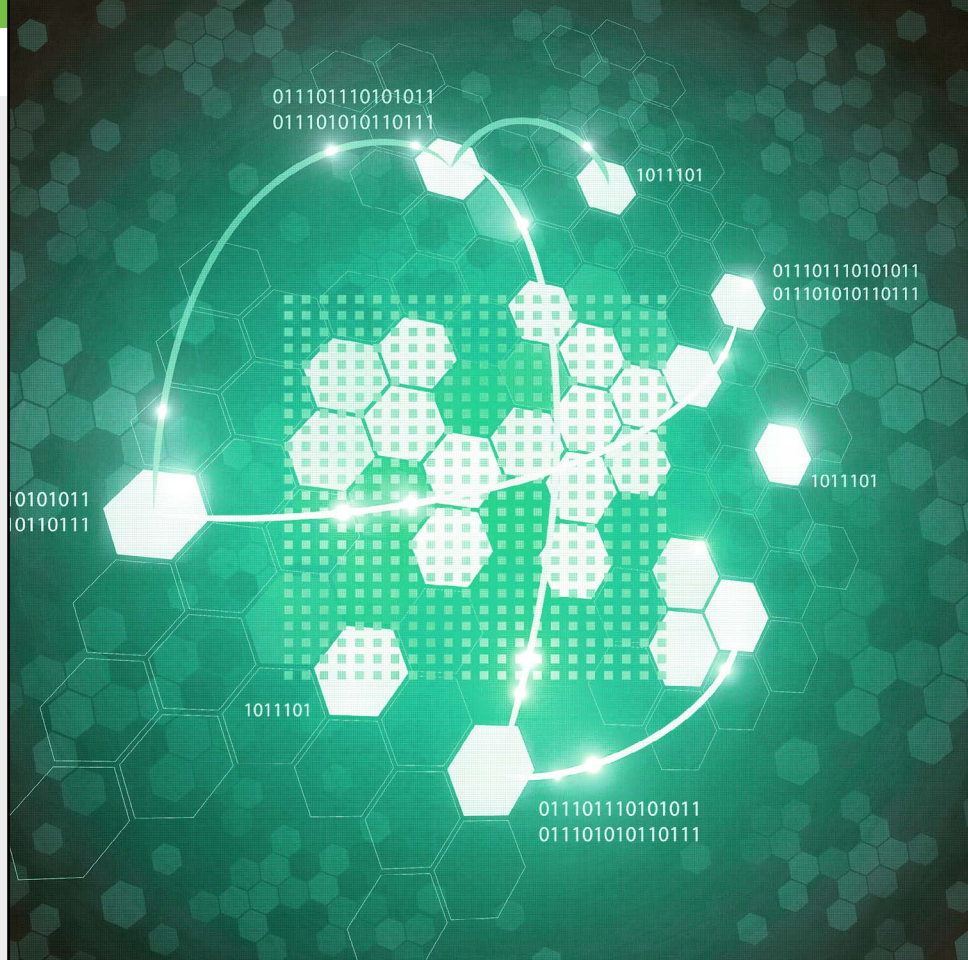
Spam filters allow companies to limit the number of unwanted emails and weed out some of the more obvious criminal communications directed at employees. Web filters allow companies to limit the duration and time of day that employees visit particular websites not required for their work. For instance, some companies allow employees to visit Facebook® on their lunch breaks.



## Tip #7:

### Utilize systems management tools to ensure all software updates are installed across multiple endpoints.

Systems Management technology can be used to search for network services and unauthorized devices as well as vulnerabilities and automatic updates of vulnerable applications. With a centralized management system, a security solution with systems management technology can scan all endpoints for vulnerabilities and unused network services; detect and analyze vulnerable applications; and update vulnerable components and applications. If there is no update available, vulnerable software can be restricted or banned. Many of these measures can be automated, reducing the workload for overtaxed IT departments.



# Tip #8:

## Don’t forget mobile.

Last year, 472 million smartphones entered circulation, and that number is expected to grow to nearly 1 billion by 2015.[6] Research analyst firm Gartner forecasts that the total number of tablets sold will climb to 326 million by 2015.[7] All of these mobile devices are finding their way into work environments. By 2016, 38% of organizations will have stopped providing mobile devices to employees, instead allowing employees to choose and use their own devices in the workplace. By 2017, half of employees will be using their own devices for work. At the same time, personal mobile devices used for work-related purposes represent one of the main hazards for businesses: 65% of IT Managers surveyed for a recent B2B International report saw their company’s BYOD policy as a threat.[8]

End users are looking to mobility as a means of blending their professional and personal digital lives. Wireless connectivity, cloud services and file-synchronization applications are making these devices highly desirable targets for physical theft. Thieves and hackers with stolen mobile devices will compromise them to lift valuable data or use them to penetrate the networks to which they are connected. The direct monetary damage of device loss and theft is estimated at $30 billion annually; the indirect costs of any associated hackings are unknown.[9] Mobile cybersecurity and Mobile Data Management (MDM) with Encryption for lost or stolen mobile devices is critical for mobile devices used for work.

6 IDC, Worldwide Mobile Phone and Smartphone ASV 2014–2017 Forecast, February 2014.
7 Gartner, September 2011.
8 B2B International, Global Corporate IT Security Risks, May 2013.
9 My Lookout.com, March, 2012

## Tip #9:

### Keep the lines of communications open between IT and other staff.

Employee education isn't a set it and forget it function. IT staff should regularly disseminate news and information about the latest cyberthreats so employees are aware of the risks and know how to defend against them. Employees should also be encouraged to immediately report anything strange happening on their computer without retribution.

## Tip #10:

## Select a trusted security partner.

How do you select the right IT security solution for you? At Kaspersky Lab, our experts are on your side to help you establish, maintain, and teach a security policy designed to protect your organization.

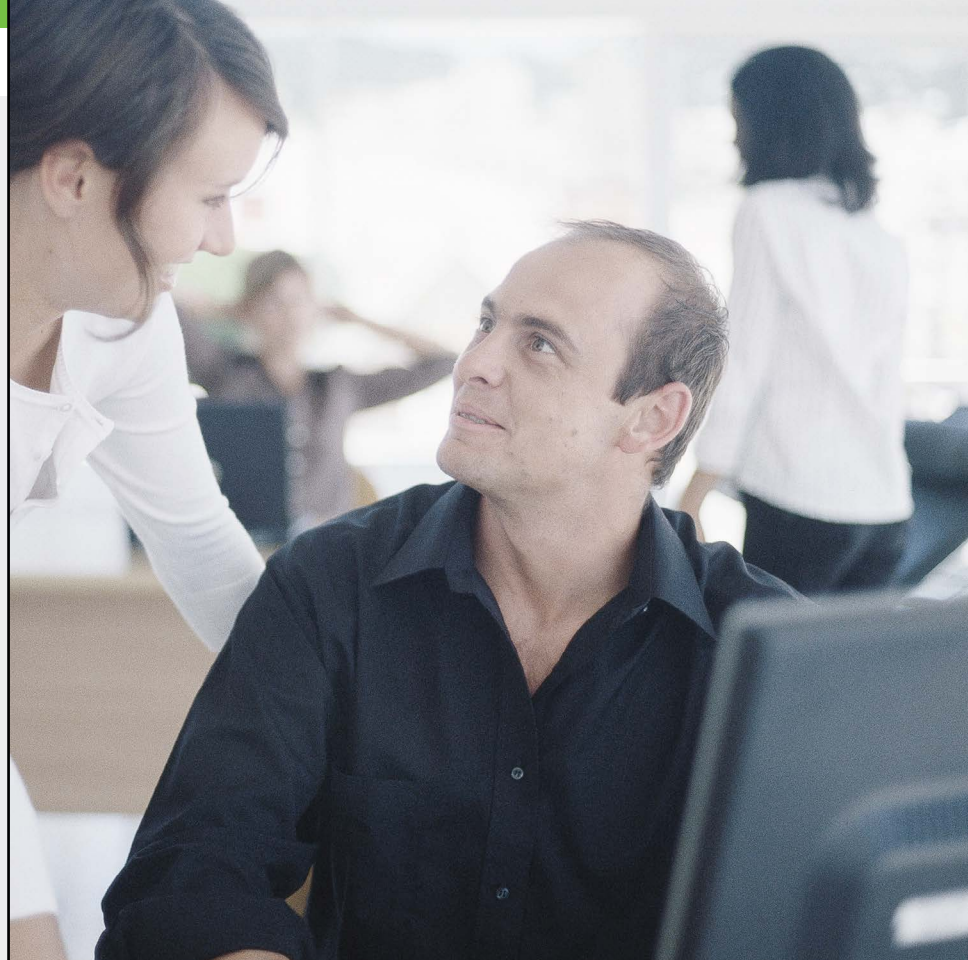
Kaspersky Lab's Endpoint Security for Business; Security for Virtualization; and Mobile Device Management solutions can:

- fully guard your expanding perimeter beyond basic anti-malware protection
- reduce the number of individual tools
- safeguard both physical and virtual servers
- control and patch third-party applications
- establish and administer BYOD and other security policies
- protect and manage all your mobile endpoints
- prioritize fixes from a single console

# An ounce of prevention

In isolation, none of the practices above can effectively prevent a cyberattack on your business, but education can go a long way toward preventing those things that are preventable.

All users must know and practice your organization’s security policies and understand the possible consequences of risky behavior.



## About Kaspersky Lab

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users.* Throughout its 16-year history, Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for educators, consumers, SMBs and Enterprises. The company currently operates in almost 200 countries and territories across the globe, providing protection for more than 300 million users worldwide.

Call Kaspersky today at 866-563-3099 or email us at corporatesales@kaspersky.com to learn more and sign up for a demo or free trial of Kaspersky Endpoint Security for Business.

www.kaspersky.com/business

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC # 242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.

© 2014 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners.