



TOP 10 TIPS FOR EDUCATING EMPLOYEES ABOUT CYBERSECURITY

INSIDE THREATS

Cyberthreats to your business are usually blamed on outsiders—nefarious programmers writing malicious code designed to pilfer your corporate intelligence, siphon 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. It's important to train employees before you have a data breach. Don't wait to react. Create policies that assume you'll be infiltrated, and then help employees learn what they should do (and not do) to keep your business safe.



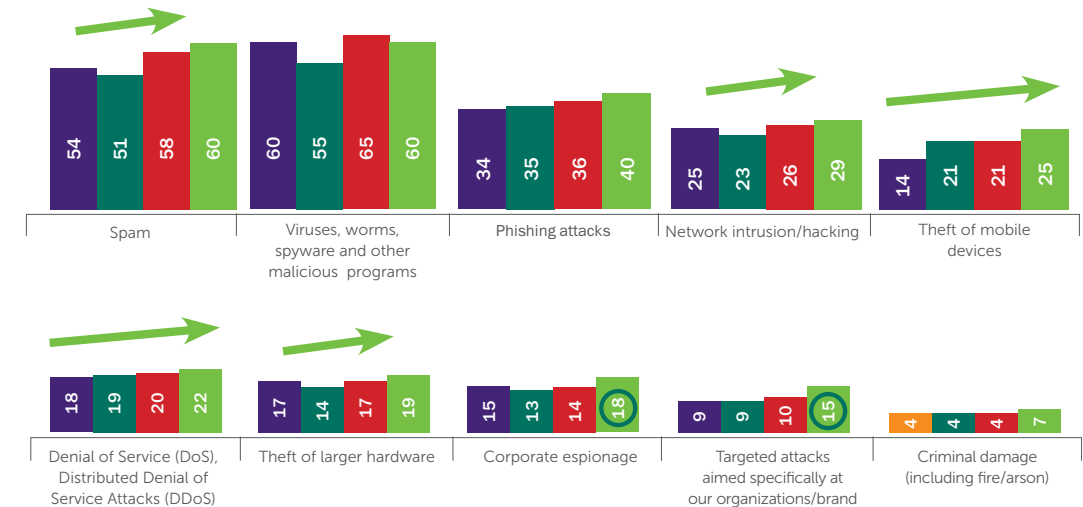
Tip #1

REGULARLY TALK TO EMPLOYEES ABOUT CYBERSECURITY.

- Explain the potential impact a cyberincident may have on your organization's operations, and spell out employee obligations, particularly with the use of mobile phones.
- It's not enough to require an annual review and signing of an "I have read and understand company IT policies."

EXTERNAL THREATS EXPERIENCED

In a recent survey conducted by B2B International and Kaspersky Lab, 94% of companies reported some form of external threat.¹



% Of organizations experiencing each event

2011 (n=1,408) 2012 (n=2,376) 2013 (n=1,912) 2014 (n=2,119)

Significantly higher YOY

1. B2B International and Kaspersky Lab, "IT Security Threats and Data Breaches," October, 2014.

Tip #2

REMEMBER THAT TOP MANAGEMENT AND IT STAFF ARE EMPLOYEES, TOO!

- Top managers are often targeted because:
 - They have access to more information. [The bad guys recently targeted traveling executives using free hotel Wi-Fi without encryption.](#)
 - IT bends the rules for them.
 - The damage/financial payoff can be much bigger.
- With their unlimited power over the network, IT folks are also vulnerable.



Tip #3

**EXPLAIN TO THE EMPLOYEES
THAT, WHILE YOU MAKE THE BEST
EFFORT TO SECURE THE COMPANY'S
INFRASTRUCTURE, A SYSTEM IS ONLY AS
SECURE AS THE WEAKEST LINK.**

- Encourage cooperation, not just compliance.
- Create a policy sophisticated enough to cover all possible attack vectors.
- Recognize that humans have weaknesses and make mistakes.



Tip #4

HAVE REGULAR, FOCUSED SESSIONS WITH EMPLOYEES TO EXPLORE DIFFERENT TYPES OF CYBERATTACKS.

- Since new employees start work all the time, cybersecurity training should be part of your general onboarding activities.
- Consider different formats (e.g., Lunch & Learn).
- Make it useful.
 - Most employees have PCs at home and relatives who also need help.
- Make it useful.
 - Reference topical news stories.
 - Use social media.



Tip #5

WARN EMPLOYEES TO PAY SPECIAL ATTENTION TO SOCIAL ENGINEERING ACTIVITIES.

- Beware of social media, blog and suspicious links from unknown sources while at work or using corporate devices.
- Many cyberincidents begin with a phone call from someone posing as a co-worker asking seemingly innocuous questions, gathering information about the company and its operations.
- A cybercriminal exploiting social weaknesses almost never looks like one.



Tip #6

TRAIN EMPLOYEES TO RECOGNIZE AN ATTACK.

- Have policies in place that assume you'll be infiltrated. Don't wait to react. Have a documented remediation plan in place and update or review frequently.
- Communicate step-by-step instructions about what to do if employees believe witnessed a cyberincident.
- Training needs to happen before there's a problem.

Trainings should include specific rules for email, Web browsing, mobile devices and social networks.

Don't forget to include the basics:

- Physically unplug your machine from the network.
- Notify your administrator of any suspicious emails, unusual activity or if you lose your mobile device.
- If you can't find your emergency IT number in 20 seconds or less, start memorizing!



Tip #7

NEVER DISAPPROVE OR MAKE FUN OF AN EMPLOYEE WHO RAISES A RED FLAG.

- Even if it's a false alarm, it's important not to discourage employees for speaking up in case a real cyberattack happens.
- If false alarms happen regularly, improve your training approach.



Tip #8

IF AN INCIDENT HAPPENS, GIVE YOUR EMPLOYEES A HEADS-UP AS SOON AS POSSIBLE.

- A lack of transparency or improper handling of a cyberincident may significantly increase the impact of the event.
- Issue instructions about how to speak to the public and the press about the incident.
- Have an internal communications plan and PR strategy in place before anything happens.
- Consider insurance for cyberincidents.



Tip #9

REGULARLY TEST EMPLOYEES CYBERSECURITY KNOWLEDGE.

- Make it relevant for their digital lives.
- Make it fun or rewarding (or fun *and* rewarding) with incentives for prompt responses.



Tip #10

INVITE, LISTEN AND RESPOND TO FEEDBACK.


- If you force employees to change passwords every week, be prepared that they will write them down and post them in their workspaces.
- If it's too difficult or complicated to access something they need to do their jobs, they will find less secure work-arounds like using personal email, USB sticks and using colleagues to bypass restrictions.
- Learn the root cause of unsafe behavior.



SYSTEMS MANAGEMENT & ACTIONABLE PATCHING


SYSTEM PROVISIONING

- Create images
- Store and update
- Deploy



LICENSE MANAGEMENT

- Track usage
- Manage renewals
- Manage license compliance




REMOTE TOOLS

- Install applications
- Update applications
- Troubleshoot




VULNERABILITY SCANNING

- HW and SW inventory
- Multiple vulnerability databases




ADVANCED PATCHING

- Automated prioritization
- Reboot options



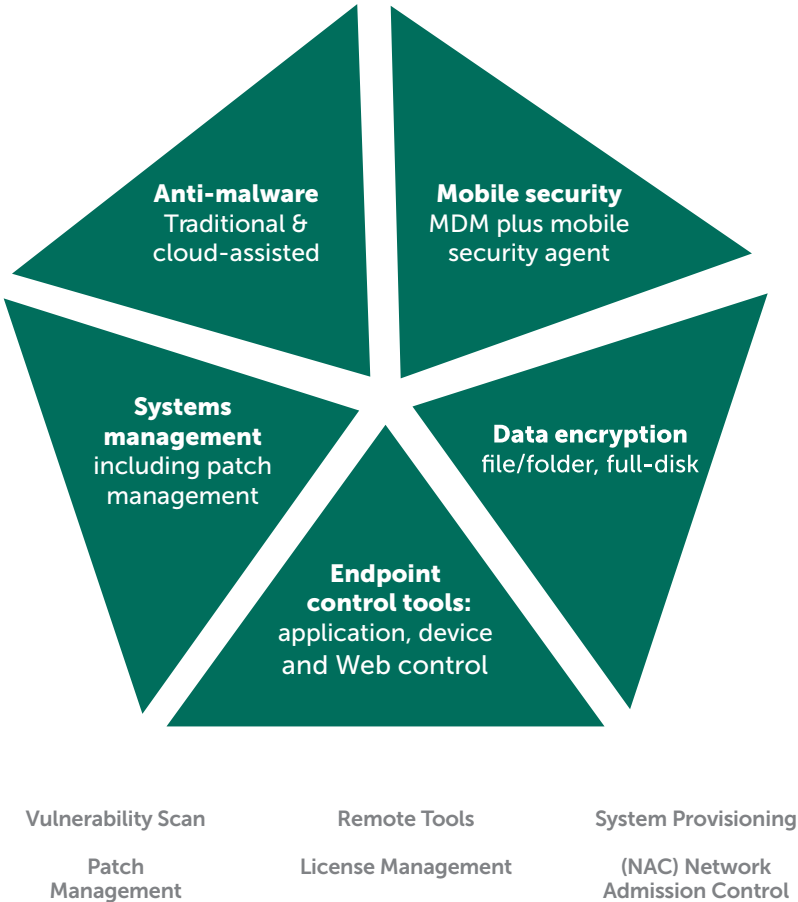
NETWORK ADMISSION CONTROL (NAC)

- Guest policy management
- Guest portal



KASPERSKY SECURITY FOR BUSINESS

PHYSICAL » VIRTUAL » MOBILE »



GET STARTED NOW: FREE 30-DAY TRIAL

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION.



Watch us on
YouTube



Like us on
Facebook



Review
our blog



Follow us
on Twitter



Join us on
LinkedIn

Learn more at <http://usa.kaspersky.com/business-security>

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at www.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:

<http://usa.kaspersky.com/business-security>

(866) 563-3099

corporatesales@kaspersky.com

© 2015 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

KASPERSKY
lab
THE POWER
OF PROTECTION