SECURITY [SNAPSHOT]

Foolproof Employee Security Checklist

KASPERSKY lab

$86,500 The average financial impact of a data breach on small- to medium-sized companies.

$891,000 The average financial impact of a data breach on large enterprise companies.

1 in 5 Careless employees were the single biggest cause of serious incidents involving data loss or leakage—involved in 1 in 5 serious data breaches.[1]

42% 42% of companies say that the single largest loss of confidential data loss is by employees.

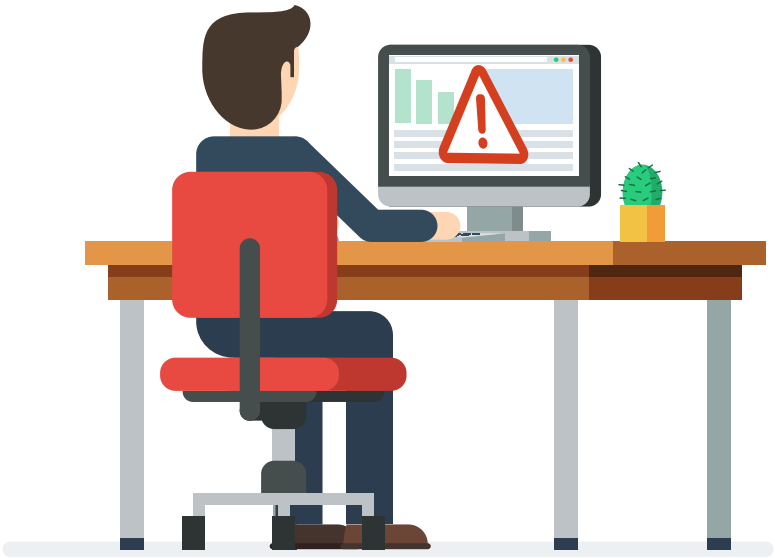
73% Companies who have been affected by internal information security incidents.[2]

[1] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International
[2] *Corporate IT Security Risks Survey 2015* from Kaspersky Lab and B2B International

The threat inside your company

Take a look around your company, and you will see one of the biggest IT security threats you face—the people you work with. Even the most well-intentioned employees who are the biggest advocates for your company risk leaking sensitive data or inadvertently letting in malware that can wreak havoc on your network and systems.

For companies of all sizes, the threats from within are an ongoing concern and the hardest to predict. With employees using multiple devices—often in multiple locations—your IT department faces the challenge of monitoring a perimeter that is a moving target. But there are steps you can take to ensure that you're protected. By carefully looking at the issue of IT security from every possible angle, you can strike that important balance between allowing employees the access they need while ensuring data security.



Top ten tips for employee security

1. Your employees are your first line of defense.

TAKEAWAY:
In any organization, the more your employees know about how to help protect your company, the safer your business will be. Ensure that all employees know and observe company security policies. Post the policies clearly and answer any questions they may have on a regular basis.

2. Employee education sessions are well worth your time.

TAKEAWAY:
80% of cyberincidents start with a human mistake. Reducing that percentage begins with educating employees on the dangers of attacks that specifically target them via social engineering. Phishing, ransomware, and spear phishing are all ways that cybercriminals gain entry to your organization through employees. Kaspersky Lab's own data shows that when companies educate their people about cybersecurity, they have a 93% success rate at getting employees to put their new knowledge into practice. Training works, especially when you use varied and creative methods. In-person sessions, coupled with webinars, infographics and videos all help to get the message across.

3. Educating employees starts right at the top—with your company leaders.

TAKEAWAY:
Most executives understand that cybersecurity is an issue, but many do not understand how big a role they can play. By encouraging a culture of cybersecurity awareness from the top levels of your organization, executives can help ensure not only that employees take it seriously but also that your organization is better protected. Moreover, many boards now recognize that they can often be held legally accountable in the event of a breach and must prove that they exercised due care in protecting customers and assets. When approaching executives about this topic, it's important not to assume that they understand all of the issues involved in IT security. Filling in the gaps for them will help them to understand the complexities of this topic and to advocate for awareness across your organization.

4. All employees should know how to inform IT about any security incident.

TAKEAWAY:
Walk them through the signs of a breach and who to call. Numbers and contacts should be clearly posted. Many employees may be hesitant to sound the alarm, but their vigilance is a vital protection. They should err on the side of caution and ask the IT department right away if something seems suspicious.

5. Maintain control over user access rights and privileges.

TAKEAWAY:
One of the most important things your IT department can do is maintain control over who has access to certain programs, devices and sensitive information within the company. This involves understanding many different roles and possibly limiting access to certain employees, but it will ensure a much higher level of protection.

6. Record all rights and privileges.

TAKEAWAY:
When you have a security incident, knowing who has access to which part of your organization can save you a lot of time. By recording all user access rights and privileges, you can save your IT department many steps and help mitigate the damage faster.

7. Perform regular scans in order to catch system vulnerabilities and keep your network services up to date.

TAKEAWAY:
Your systems and network are constantly changing. With new employees and regular attrition, there are new devices and programs that need to be checked continually. In addition, users will often need new tools to do their jobs, adding new devices and programs to your network on a regular basis. It's important to catch vulnerabilities by scheduling regular scans of your entire system.

8. When you detect vulnerable network services and applications, analyze if you need to institute new policies.

TAKEAWAY:
Scans of your network can reveal some unexpected vulnerabilities. After you perform the scan, it's important to re-assess whether or not you need to update your policies and procedures in order to stay protected.

9. Update vulnerable components and applications.

TAKEAWAY:
Patches for vulnerable components and applications are continually sent out by vendors in order to address vulnerabilities. Performing these updates is essential and can often be done on a regular weekly schedule.

10. Install a multi-layered security solution.

TAKEAWAY:
Human error will always happen. Implementing a multi-layered solution ensures that threats are assessed from multiple angles and should be an essential component of your overall security plan.

Try Kaspersky Lab

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


Like us on Facebook


Follow us on Twitter


Join us on LinkedIn


Watch us on YouTube

Review Our Blog

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 usa.kaspersky.com.

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

usa.kaspersky.com/business-security

(866) 563-3099

corporatesales@kaspersky.com

KASPERSKY lab

THE POWER OF PROTECTION