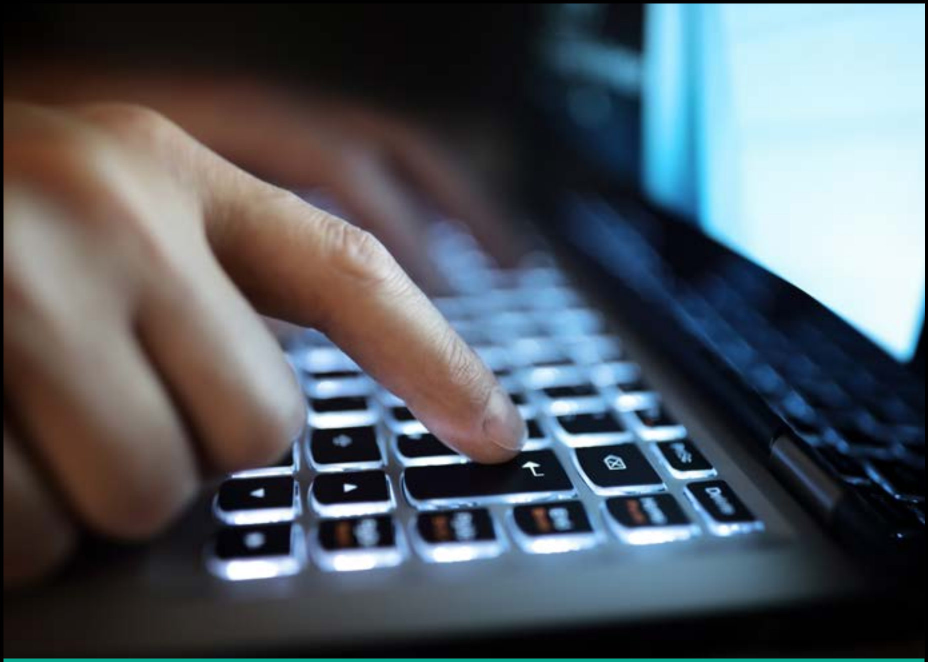
SECURITY SPOTLIGHT



The Threats from Within

How educating your employees on cybersecurity can protect your company

KASPERSKY lab

Human beings are the weakest link within any organization, presenting new opportunities for cybercriminals to infiltrate your company. But your employees can also be your first and best line of defense. With a robust security education program in place, your company can protect its most sensitive information by ensuring that cybercriminals cannot break through your employee firewall.

1 in 5

Careless or uninformed employees were involved in almost 1 in 5 serious data breaches.[1]

Your Employees Are Your First Line Of Defense

Most organizations view their employees as their most valuable asset. They are the engine of the company that grows revenue and builds relationships with clients.

At the same time, most cybercriminals view your employees as the path of least resistance. For businesses in North America, two of the top causes of the most serious data breach were careless/uninformed employee actions (59 percent) and phishing/social engineering (56 percent).[2] Cybercriminals know and exploit this fact every day. If they want access to your clients, employee records or future plans for growth, social engineering tactics that target employees are often the easiest way to infiltrate an organization.

But my employees are a lot smarter than that.

The hard truth is that well-meaning employees threaten data security every day, usually without realizing it. According to leading industry and government reports, over 90% of all cyberattacks are successfully executed with information stolen from employees who unwittingly give away their system ID and access credentials to hackers.[3] Add in password insecurity and social engineering, and even the best employees can compromise your company's security.

In the case of large enterprises, 45% of large companies worry about the threat posed by careless or uninformed employees. They are right to be worried when the average total impact of a single data breach at a large organization is $891,000.[4]

Many employees have a false sense of security around IT issues or they believe that they do not play a role. By putting into place a multi-layered system of defense that includes employee education, your company can ensure that your people understand the important responsibility they have in keeping your company and its data secure.

[1, 4] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

[2] Employees Are One of the Biggest Cyberthreats to Businesses in North America

[3] Employee Errors Cause Most Data Breach Incidents in Cyber Attacks

34% Incidents attributed to insiders, including trusted third parties and employees.[5]

Security Matters All the Way Up the Ladder

Building a culture of cybersecurity awareness starts at the top.

Boards of directors and C-level executives need to understand that they ignore cybersecurity at their peril and that their communications to employees about this topic are a vital piece in building that culture.

In a recent survey by Kaspersky Lab and B2B International, the second biggest type and cause of security incidents is careless and uninformed employees. With the extraordinary costs of just a single data breach, it is prudent for executives to educate employees.

With CEOs seeing cybersecurity as a top business risk, the tides are certainly shifting. Recent widely publicized security breaches have certainly contributed to this mindset. It's important to build on this awareness by making education a priority at every level, keeping executives informed about IT security issues and making them understand their role in helping to educate and inform employees.

In other words, don't assume that your company's leadership understands everything about cybersecurity. Educate at all levels of your organization, and that will go a long way towards building a strong line of defense against threats.

[5] 2017 Global State of Information Security Survey conducted by PwC, CSO and CIO

31%

Cyberattacks directed at businesses with less than 250 employees, according to The U.S. Department of Homeland Security.

Every Size Company is a Target

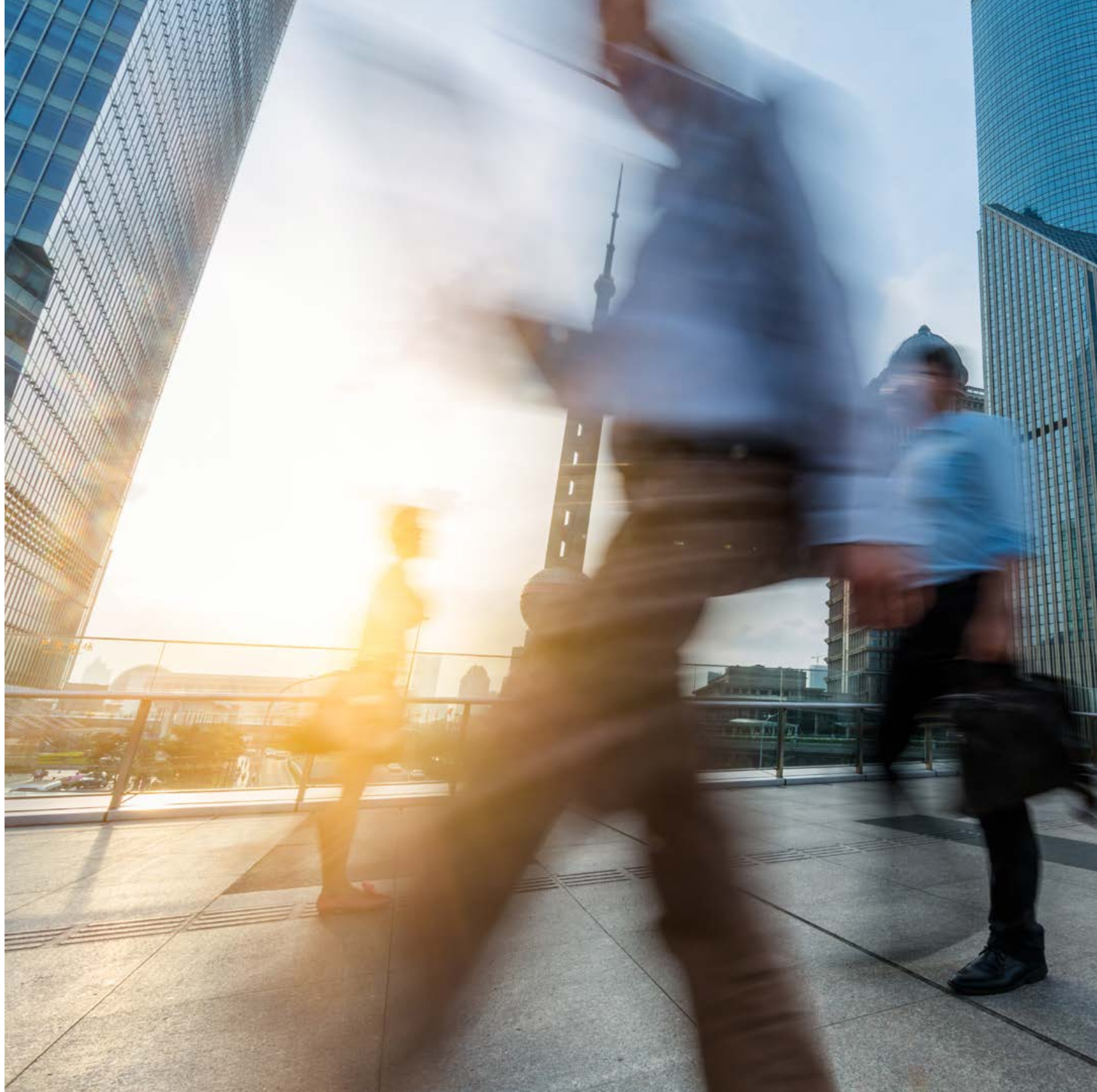
Cybercriminals don't care who you are. You could be a small 100 person shop or a medium-sized business that provides SaaS. If you have any access to the data of a large enterprise, then you are a prime target.

In many cases, small businesses act as vendors or suppliers to large enterprises and, therefore, have access to sensitive insider information. Furthermore, many small businesses do not have the time or resources to combat security threats. As large enterprises continue to build up their security perimeter and educate their employees about what to avoid, small- and medium-sized businesses are even more susceptible to cybercriminals who are looking at the whole marketplace for areas of vulnerability.

With the average cost of a serious data loss event at $86,500 for an SMB, most small businesses are not prepared for the sudden budget drain that a data loss event can cause.[6]

So, what can an SMB do to reduce this risk?

By building a multi-layered security strategy that takes into consideration the technologies that they need the most, as well as setting aside time and resources for employee education, smaller businesses can make sure that they don't act as a portal for a serious data breach to any of their clients or customers.



[6] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

77% Percentage of U.S. businesses that have suffered between 1 and 5 separate incidents of data loss, leakage or exposure in the past 12 months.[7]

Common Attack Methods

Creativity is the secret weapon of the cybercriminal.

Each year, Kaspersky Lab identifies more innovative tactics that cybercriminals use to get to your company's information through your employees. Let's take a look at some of the most common methods that every employee at your company needs to know about.

Social Engineering

Trust is the currency on which social engineering is based. It involves tricking employees into breaking normal security procedures, and it is an effective method that has been the root cause of a lot of recent high profile attacks. Many employees assume that they are protected from these kinds of targeted attacks when using a company computer. We recommend an approach of "trust but verify." Employees should feel comfortable using company equipment, but if something seems suspicious, they should trust their instincts and alert IT colleagues.

Phishing

The majority of targeted attacks are delivered via email to employees. Attackers try to trick employees into opening phishing communications and clicking on dangerous links. Recent, widely publicized targeted attacks that affected tens of millions of users usually started with a simple email to employees. Although these attacks are not very sophisticated, they have been incredibly successful in infecting organizations across all sectors.

Tell your employees to be alert and to ask themselves certain questions, such as:

- Does the email list one URL but point to another?
- Does the message ask for personal information?
- Does the header information not match the sender?

By being alert and contacting IT, employees can stop many damaging security breaches right at the door to your organization.

Waterholing

The basic idea behind waterholing is to find and infect the sites that employees visit most often. When the employee opens the infected site, the code injected in the body of the page redirects the browser to a malicious site that contains a set of exploits. Most employees are surprised to learn that they don't have to do anything more than visit a site to be infected. Clicking "Allow" or "Confirm" often executes the malicious code and hides the attack from your IT security team.

[7] Kaspersky Lab's *The Financial Impact of IT Security on US Businesses*

54%

Businesses who say that the inappropriate sharing of data by employees via mobile devices is where they are most vulnerable.[8]

BYOD Security

Finding the right mix between employee device preference and IT security is a delicate balancing act. And a key component of it is employee buy-in to your security policies.

A recent study showed that more than 60% of employees at small- to medium-sized businesses use company-issued mobile devices to work from home or when traveling. According to Kaspersky Lab's recent Mobile Virusology mobile malware report, there were three times as many malware installations in 2016 as in 2015 and a total of 8.5 million malicious installations were identified.[9]

At Kaspersky Lab, our mobile security products detected a rapid rise in malicious mobile programs with a more than threefold increase from Q1 to Q3 2015. With bring your own device (BYOD) becoming the norm in most companies, this number is sure to increase and cybercriminals are certain to seize the opportunities that come with it.

Clearly, employees need to understand the risks and stay invested in mitigating them, and organizations need to invest the time and resources in the right mobile security products. With mobile security as an important item on your employee education agenda and the right technology in place, your company can avoid being a victim of the latest point of entry for cybercriminals.

[8] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

[9] In 2016, there were three times as many mobile malware installations than 2015

52%

Businesses who now assume that their IT security will be compromised at some point and that they need to be prepared for these events.[10]

Building Your Employee Education Program

Employee education about cybersecurity is not just a nice add-on item. It's the core element of prevention. With companies paying tens of thousands of dollars to repair the damage to their brands, the risks associated with not acting are immense and long-lasting.

The best place to start is by keeping your IT staff on top of current trends and risks and then implementing certain key policies, such as:

- ✓ Ensure that all users know and observe company security policies
- ✓ Inform users about possible consequences of key Internet threats, such as phishing, social engineering or malware sites
- ✓ Instruct all users to notify IT security staff about all incidents
- ✓ Maintain control over user access rights and privileges; any rights and privileges should be granted only when necessary
- ✓ Record all rights and privileges granted to the users

- ✓ Scan the systems for vulnerabilities and unused network services
- ✓ Detect and analyze vulnerable network services and applications
- ✓ Update vulnerable components and applications. If there is no update, vulnerable software should be restricted or banned

Many of these measures can be automated. For example, if security policies are violated, special software shows the user a warning message. Systems management technology can be used to search for network services and unauthorized devices, as well as vulnerabilities and automatic updates of vulnerable applications.

[10] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

True Cybersecurity

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

Join the conversation.

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Get your free trial now >

Learn more at
kaspersky.com/business

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.

To learn more about Kaspersky Endpoint Security for Business, call Kaspersky Lab today at 866-563-3099 or email us at corporatesales@kaspersky.com.

www.kaspersky.com/business

KASPERSKY lab