KASPERSKY lab

TOP 6 THINGS SMALL BUSINESSES NEED TO KNOW ABOUT CYBERSECURITY

Cybercrime: A Big Problem for Small Businesses

There's nothing "small" about the small business sector. According to the U.S. Small Business Administration, the 28 million small businesses in America account for 54% of all U.S. sales. Small businesses provide 55% of all jobs and 66% of all net new jobs since the 1970s.[1]

Although your data is critical to your success and you are integral to the success of the U.S. economy, many startups and small businesses let cybersecurity slip through the cracks. There is no shortage of negative news stories about business data breaches and it isn't just the large corporations. The data breach costs for small and medium-sized businesses are high, too. **According to a Kaspersky Lab survey, just one cybersecurity incident can cost small- and medium-sized businesses an average of $86,500.**[2]

1. Small Business Trends, SBA.gov, U.S. Small Business Administration
2. Kaspersky Lab Press Releases, Kaspersky Lab Survey Reveals: Cyberattacks Now Cost Large Businesses an Average of $861,000,

Small businesses often lack the budget, staff, and sophistication to assemble strong defenses, making them an easy target where the chances of thieves getting caught is much lower. And no company is "too small to be worthwhile" for the bad guys. Making sure your business is adequately protected can seem like an overwhelming undertaking. We've compiled a list of the top things startups and small businesses need to know about cybersecurity to help you get started.

1

Your Employees Are Your First Line of Defense

Cyberthreats to your business are usually blamed on outsiders, but sometimes the threat actually originates from within. **Small-business employees usually wear many hats and often have to stretch their roles beyond their areas of expertise.**[3]

Explain the potential impact a cyberincident may have on business operations and spell out specific rules for email, web browsing, mobile devices and social networks.

- Have regular, focused sessions with employees to explore different types of cyberattacks and test their security knowledge.
- Include cybersecurity training in onboarding activities for new employees.
- Make training useful, relevant, and responsive to real world examples.
- Train employees to recognize an attack and have policies in place that assume you'll be infiltrated. Communicate step-by-step instructions about what they should do if a cyberattack occurs.

3. Kaspersky Lab, Kaspersky Cybersecurity Awareness Training

2

Strong passwords. Two-factor authentication. Password manager. Another important line of defense.

Research from Kaspersky Lab shows that there are three common password mistakes putting people at risk. People frequently use the same password for several accounts, making it easy for cybercriminals to hack victims on multiple accounts. Weak passwords that are easy to crack are dangerous. Storing passwords insecurely can also put users at great risk.[4] To keep your business safe you and your employees should:

- Use a unique password for each account
- Change passwords often
- Use a mix of letters, numbers and symbols

4. ITP.net, Kaspersky Lab uncovers bad password habits, January 2017

- Avoid the use of personal information or common words as a password
- Make sure your password backup options are up to date
- Keep your passwords complex and unique, and use a password manager to keep them secure
- Select options for two-factor authentication, and require security questions

3

Safeguard Your Important Data

Securing IT infrastructure is often an afterthought for small businesses, but it shouldn't be. According to *Security Magazine*, only 31% of small businesses take active measures to guard themselves against security breaches. Additionally, 41% of small businesses are unaware of the risks they face the human error. This unpreparedness makes SMBs great targets for cybercriminals.[5]

Even when entrepreneurs decide to take steps to secure their new business, too often they can't afford to purchase and install multiple pieces of complex software that are usually designed for much larger enterprises. Even if they have the budget, they'll struggle to properly utilize and manage it.

5. Security Magazine, The Costs and Risks of a Security Breach for Small Businesses, July 2016

By employing a multi-layered solution designed specifically for small businesses, you can ensure that you have the protection in place that meets the needs of your business and is manageable for your IT staff.

4

Protect Your Mobile Devices

Not only are your employees on the move, but it is a safe bet that they're bringing lots of mobiles devices with them. Whether they carry smartphones or tablets, it's inevitable that your corporate data will end up on a device that can be easily lost or stolen.

Complicating matters is the fact that many mobile devices have weak security, making them an attractive target for cybercriminals. **If they gain access to a device, not only is the data on that device wide open to a breach but so is all the data on that network.**

It makes sense to take a close look at your mobile security and ensure that your mobile devices are as secure as your endpoints and your servers.

According to the Corporate IT Security Risks 2016 survey from Kaspersky Lab and B2B International, 51% of businesses agree that the increased number of devices used within their organizations makes managing those devices more difficult. If you struggle to deal with the increasing complexity of your IT security, you are not alone.

Furthermore, 54% of businesses in the same survey say that the inappropriate sharing of data via mobile devices is their biggest area of vulnerability. Add to this the explosion of mobile Trojans designed to breach these devices, and you have multiple layers of complexity that threaten your business.

Mobile security is no longer an optional item for small business cybersecurity. Small businesses need to take it just as seriously as security for their servers and endpoints.

5

Use encryption to protect your most sensitive data.

It may seem like overkill at first, but as soon as you start processing and storing payment or other confidential information of your customers, encryption is vital. Encryption is just as important for your business as it is for your customers. **If a computer or device containing personally identifiable information (PII) is stolen, your company can be sued if the information is leaked or shared.**[6]

Data encryption is a requirement once you start setting up Point of Sale terminals (cash registers) that accept credit cards. If you plan on having a storefront—physical or online—you need to familiarize yourself with Payment Card Industry security standards and the risks of violating these rules.

6 Business News Daily, A Small Business Guide to Computer Encryption, September 2016

6

Install a Multi-layered Security Solution

Implementing a security solution that's managed through a single console makes sense, especially for small companies that may not have a dedicated IT security staff, much less an entire IT department.

Complexity is the enemy of cybersecurity, so it's critical for you to choose cyberprotection that allows you to set, deploy and monitor a single policy across your entire IT infrastructure. This should include all of your devices, systems and platforms.

Most SMBs don't have the expertise, time or budget of a large enterprise. Finding a single solution that meets your anti-malware, mobile security and encryption needs will be much easier to manage than tying together multiple products from different vendors. In short, it's important to look for one product that solves all of your needs and allows you to focus on what you do best—running and growing your business.

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.

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

KASPERSKY lab
THE POWER OF PROTECTION