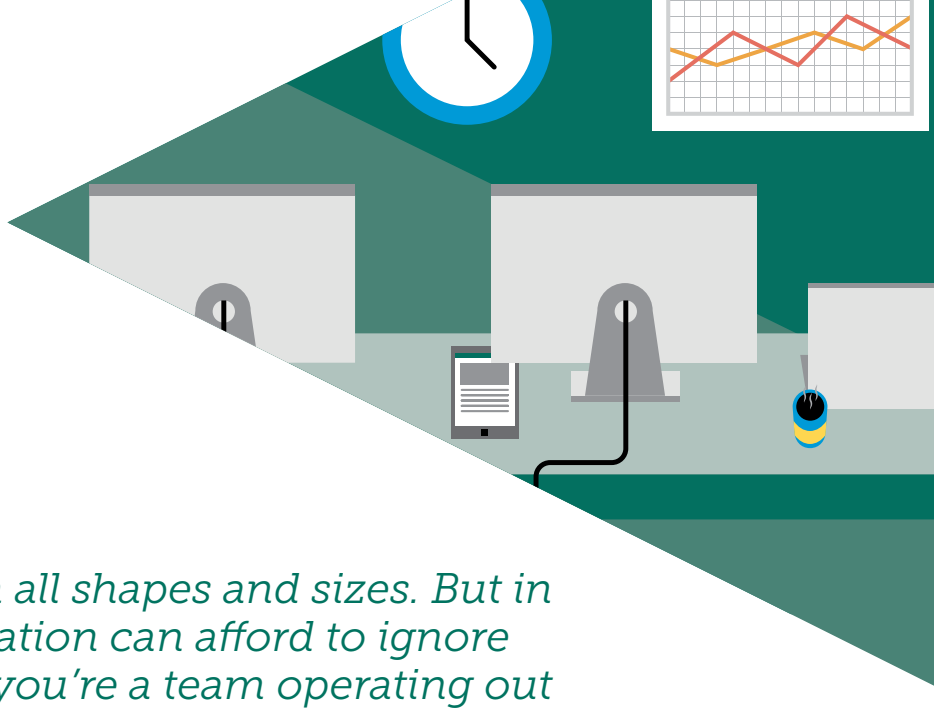
SMALL BUSINESS IT SECURITY PRACTICAL GUIDE

How to make sure your business has comprehensive IT security protection

KASPERSKY lab



Small businesses come in all shapes and sizes. But in today's world, no organization can afford to ignore online security. Whether you're a team operating out of an office, or an individual working from home,it's an issue that affects everyone.

Though cybercrime frequently grabs the headlines, it's usually when a government or a huge multinational organization is the victim. But arguably the smaller cases are the bigger story.

In 2014 alone, 143 million new instances of malware were detected.[1] And the majority of these were directed against individuals and organizations who wouldn't regard themselves as likely targets.

The truth is, everyone's a target. The good news is there's still a huge difference between being a target and a victim.

For the most part, it simply comes down to being prepared. We've put together this guide to give you the know-how to keep your business safe.

WHAT IS MALWARE?

The term "malware" refers to computer programs designed for a malicious purpose. These generally attack devices without the user's knowledge. Kaspersky Lab is a world leader in the detection of malware, having been awarded more top scores than any other security vendor.[2]

WHY DO I NEED PROTECTION?

Cybercriminals don't need to drain your bank account to have a costly impact on your business. Disruption caused by malware can interrupt your productivity and cash flow, causing a chain of undesirable effects. Given that you can protect against these eventualities with relatively simple steps, it doesn't take much to give yourself peace of mind.

1. AV Test, http://www.av-test.org, January 2015
2. Top 3, http://media.kaspersky.com/en/business-security/TOP3_2014.pdf, February 2015

YOUR SECURITY CHECKLIST

THE FIRST STEP TO SECURING YOUR BUSINESS IS TO TAKE A LOOK AT HOW YOU WORK AND SEE WHERE YOU COULD REDUCE RISK. SO GIVE YOURSELF A QUICK IT SECURITY HEALTH CHECK:

ANTI-MALWARE PROTECTION ✔

As with business insurance, when it comes to products that protect your company, you want the best you can get. If you haven't already got highly capable software guarding your devices against infection, you should make it a priority.

Unfortunately, simply being vigilant online isn't enough. We all know not to open attachments from unknown senders or download from suspicious sites, but the truth is many infections come from trusted sources that have been compromised.

BROWSING BEHAVIORS ✔

Educating your staff as to the importance of their actions online can save you a lot of headaches. Hopefully, your people understand that there are certain types of sites they shouldn't be visiting at work. But if they're also using a mobile device (such as a smartphone or tablet) for personal use, once they've left the building they may become less security conscious. So it's a good idea to block inappropriate sites to ensure they're inaccessible from work machines. Increasing general awareness of IT security threats will also help employees stay safe in their personal use.

? HOW MIGHT IT AFFECT ME?

Ever received an email from a friend or family member containing an interesting link which, once opened, seemed suspicious? Once malware has infected a computer, it can take actions without the user's knowledge. That's why trusted sources can't always be trusted.

PASSWORDS ✔

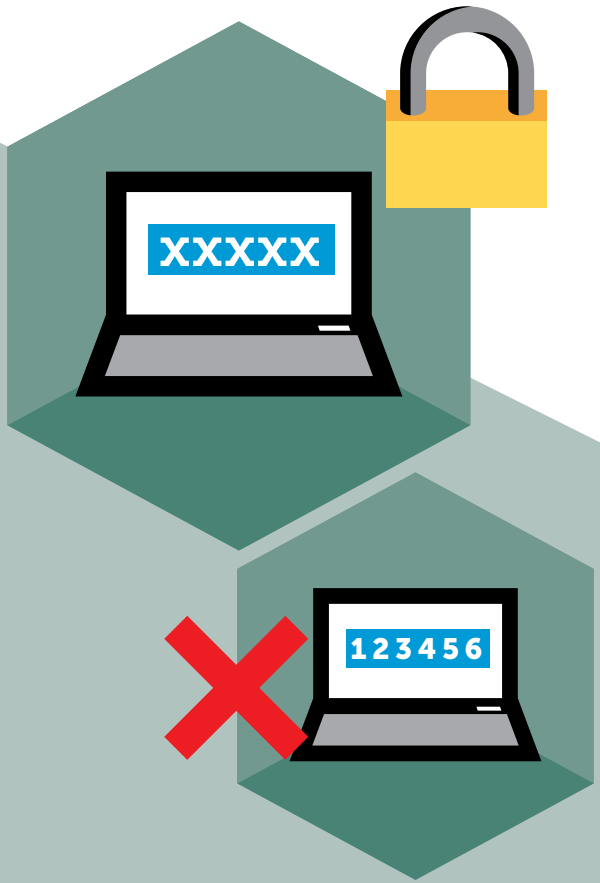
Employees also need to make sure they're using strong, unique passwords that mix symbols, numerals and letters of both cases. Everyday words can be cracked by programs that simply scan through dictionaries until they find the right one. And even if it's strong, if a compromised password is used for multiple purposes, it could lead to an even bigger breach.

UPDATES ✔

Four new pieces of malware are detected every second.[3] You need to stay ahead. That means using automated updates to strengthen your security software every day, updating all your other software whenever possible – and making sure everyone in the business does the same. Remember, programs that haven't been updated are the number one route cybercriminals use to hack businesses.

MAKE SURE YOU DON'T MAKE ANY OF THESE CLASSIC PASSWORD ERRORS:

1. Using easy-to-remember but easy-to-guess options such as "password" or "123456"
2. Using your email address, name or other easily obtainable piece of data as a password
3. Setting password reminder questions a hacker could answer with just a little research – your mother's maiden name for example
4. Making only slight, obvious modifications to regular words, such as placing a '1' at the end
5. Using common phrases. Even small sentences such as "iloveyou" are easily cracked



For more hints on how to put together hard-to-hack passwords, see our blog post on the subject.

3. AV Test, http://www.av-test.org, January 2015

IN 2014

295,500

NEW MOBILE MALWARE THREATS[4]

BANKING ✔

From directing you to fake versions of trusted sites, to using malware to spy on your activity, cybercriminals have a number of methods for obtaining your financial information. You need to take active measures to stop them.

Stay alert for phishing attempts where scammers impersonate your bank. Always use a secure browser and be sure to take a close look at the URL before inputting your details on any site. It's also best to avoid including such information in emails, which may be seen by eyes they weren't intended for.

MOBILE DEVICES ✔

As working on the move is now part of our everyday life, cybercrime is increasingly directed at mobile devices. In 2014, 295,500 new mobile malware threats (those written specifically for smartphones and tablets) were detected each month.[5] Though it's just as important to protect phones and tablets as Macs and PCs, only 32% of small businesses currently recognize the risk mobile devices present.[6]

ENCRYPTION ✔

If you have sensitive data stored on your computers, it should be encrypted to prevent it from being used if it's lost or stolen. It's important to realize that as a business, the information you hold is a highly valuable asset that needs protecting.

? WHAT IS PHISHING?

"Phishing" is where cybercriminals impersonate a trusted institution, hoping to obtain information – such as passwords and credit card details – which they could use to defraud you.

4, 5 Kaspersky Lab, SecureList, http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/, October 2014

6 Kaspersky Lab, IT Security Risks Survey 2014, http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf, October 2014

UNDERSTANDING THE RISKS

CYBERSECURITY CAN SOMETIMES BE DIFFICULT TO UNDERSTAND. COMING TO GRIPS WITH THE REALITY OF THESE ISSUES THE HARD WAY CERTAINLY ISN'T WHAT ANYONE WANTS. SO WE'VE TRIED TO MAKE IT EASIER BY ILLUSTRATING A COUPLE OF SCENARIOS, THEIR CONSEQUENCES AND HOW THEY COULD BE AVOIDED.

A very expensive cup of coffee

Having waved goodbye to the last client of the day, Thomas locks up and leaves work. There's a café just across from the office, where he is due to meet a friend. Remembering that payment to one of his suppliers is due tomorrow, he decides to take care of it before he forgets.

He uses his laptop to connect to the café's WiFi network, logs into his bank's website and makes the transfer. Pleased it didn't slip his mind, he sits back and enjoys his coffee.

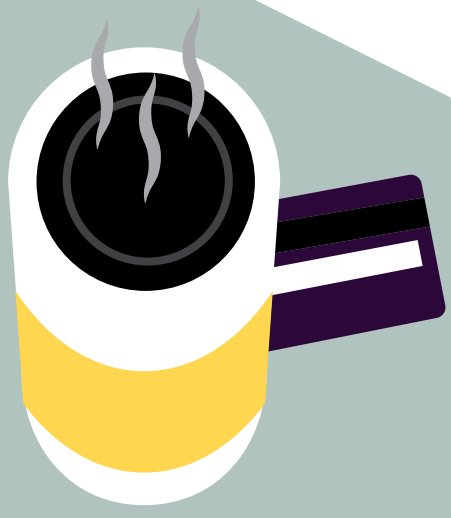
When he next checks the account, it's empty. While he's left trying to figure out why, his staff are waiting for their pay.

HOW DID IT HAPPEN?

Unfortunately, he didn't have any form of anti-malware installed and had picked up a malicious keylogging program. Those who launched the program received a record of all the information he'd entered. And, as he was using unprotected public WiFi, there was also a risk of the transaction data being intercepted.

WHAT COULD HE HAVE DONE?

Banking should only be done on devices that have anti-malware in place, and always through a secure browser.



Increasingly unwelcome mail

Maria is a psychologist and every morning she opens her email to check that her next appointment is confirmed. At the top of her inbox she sees a message from a social network she uses, asking her to update her password to something stronger. She clicks the link provided, confirms her existing password which is the same, and then replaces every other letter with an asterisk.

Happy that her account will now be harder to hack, she gets back to her inbox and soon forgets the whole thing...

...Until she receives a letter from blackmailers threatening to publish the details of every one of the clients coming to her for therapy.

HOW DID IT HAPPEN?

Maria was the victim of a phishing scam. Though the site looked just like the one she'd visited thousands of times before, it was just a fake copy. After gaining access to her profile details, they also came across the details of her practice. They tried using the same password, they'd tricked her out of, to hack into her work email. Because she used the same email password for both accounts, they were able to read all her messages and the files attached to them – one of which was a full list of her clients and their contact details.

WHAT COULD SHE HAVE DONE DIFFERENTLY?

Firstly, she should have been aware that legitimate sites and organizations will not ask for your details via email. With good security software in place, she would have been alerted to the fact that the site was fake.

Her other mistake was using the same password in both a professional and a private context.

WHY CHOOSE KASPERSKY LAB

WE'VE MADE IT OUR MISSION TO PROVIDE THE WORLD'S MOST EFFECTIVE, RESPONSIVE AND EFFICIENT PROTECTION AGAINST CYBERTHREATS. KASPERSKY LAB HAS TAILORED ITS BUSINESS SECURITY PRODUCTS INTO SOLUTIONS AS USABLE AS THEY ARE USEFUL. SO YOU CAN GET ON WITH WHAT YOU DO BEST – RUNNING YOUR BUSINESS.

We understand that, when it comes to cybersecurity, small businesses are in a unique position. They face many of the same threats as an enterprise organization, while sharing many of the same vulnerabilities as home users. We think this unique position deserves its own approach to security.

Simply repackaging a consumer product as a small business solution isn't adequate. For instance, it would offer no protection for servers that many small businesses use or plan to use. Unlike home users, businesses need to protect multiple devices easily.

However, simply taking functions away from a solution intended for a large enterprise doesn't work either. Small businesses don't have dedicated IT teams or the time to wrestle with complicated software built for specialists.

Kaspersky Lab security solutions have been designed. to be comprehensive without being complicated – so you can achieve peace of mind, without security becoming a drain on resources. Kaspersky Lab products won't slow you down, and they cover a wide range of devices.

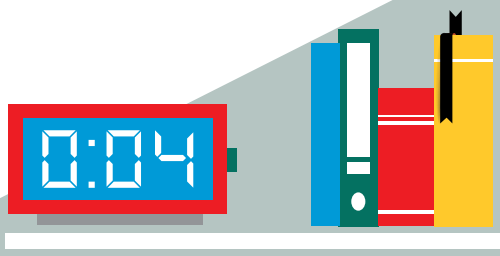
? BUT CAN'T I PROTECT MYSELF FOR FREE?

Though free security solutions are available, they simply don't provide comprehensive protection. In fact, they deliberately leave room for improvement. That's how they encourage users to upgrade to a paid-for version.

When your business is at stake, you need your protection to be the best it can be – all the time.

MAKING IT HAPPEN

NOW THAT WE'VE IDENTIFIED THE AREAS YOU NEED TO CONSIDER AS PART OF YOUR SECURITY POLICY, IT'S TIME TO CONSIDER HOW – WITH THE HELP OF A TAILORED SOLUTION – YOU CAN GET IT IMPLEMENTED.



ENSURE UPDATES OCCUR REGULARLY

When it comes to Kaspersky Lab security solutions, you don't need to worry. We'll automatically update your protection in real time, keeping you ahead of new threats as they emerge.

INCLUDE ALL YOUR DEVICES

Kaspersky Lab offers protection for supported tablets and smartphones. And if devices are lost or stolen, it can help you locate them and remotely wipe any sensitive information.

PROTECT YOUR BUSINESS NOW.

Kaspersky Lab has business security software designed to meet the unique demands of your smaller business. Our security experts can help you pick the right solution to ensure both advanced protection and ease-of-use 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


Visit Knowledge Center

Learn more at kaspersky.com/business-security

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 more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at www.kaspersky.com.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC #250210, August 2014). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.

KASPERSKY lab