CYBERCRIME TAKES A BIG BITE OUT OF SMALL BUSINESS

With Kaspersky, now you can.
kaspersky.com/business

Be Ready for What's Next

KASPERSKY lab

1

Cybercrime targeting small businesses is on the rise and the cost of a data breach among these most vulnerable victims can be a big ticket expense. Thirty-one percent of data breaches have occurred at companies with 100 or fewer employees.[1] Reports vary with the average cost of a small business cyberattack ranging from $8,900[2] to more than $100,000.[3]

To a small business, it can be difficult, and sometimes impossible to recover from such a significant attack. Customers' lack of trust following a data breach can irrevocably stain a company's reputation. Furthermore, the economic impact can devastate the entire small business enterprise, along with the personal finances of its owners and employees when they lose their livelihood. Since only about half of all new small businesses survive five years or more and approximately one-third survive 10 years or more[4], a data breach could have a ruinous impact on an already vulnerable sector. "According to the National Cyber Security Alliance, one in five small businesses falls victim to cybercrime each year. And of those, some 60 percent go out of business within six months after an attack."[5]

This whitepaper will examine why small businesses are so vulnerable, the different types of cyberthreats, and what can be done to prevent an attack and mitigate the damage.

1 Verizon Communications Inc.'s forensic analysis unit
2 The National Small Business Association's 2013
3 CNBC, June 9, 2014
4 U.S. Small Business Administration Office of Advocacy, September, 2013
5 Hackers Put a Bulls-eye on Small Business," PC World, August 2013

Common Vulnerabilities Among Small Businesses

2

Unlike larger organizations with robust IT departments, small business owners often handle cybersecurity on their own because “someone has to do it” and not because they have any particular IT expertise…or sometimes even basic knowledge. These defacto IT managers have core competencies and a long list of duties that have nothing to do with defending the business against cybercrime. Sometimes, they inherit cybersecurity responsibilities along with whatever legacy security software the company first purchased, regardless of whether or not that solution still fits the needs of the business. Perhaps the company has increased its number of endpoints with only an individual license of consumer security software protecting its original PC. Adding insult to injury, no one ever authorizes regular updates, making the business vulnerable via unpatched software as well as defenseless devices. Some tech-savvy business owners make the mistake of installing security software built for a much larger organization, rather than implementing a solution designed specifically to fit a small business. When it comes to cybersecurity, one size does not fit all.

Budget is another risk factor that increases the likelihood that a small business will become a target for cybercriminals. With a limited budget for cybersecurity, small business owners often make software choices based strictly on price and not on performance and protection capabilities. A cheap…or worse, free solution designed for an individual device can’t adequately protect a small business and its valuable data.

LIMITED BUDGETS MAKE SMALL BUSINESSES VULNERABLE TO CYBERCRIME

Types of Cyberthreats

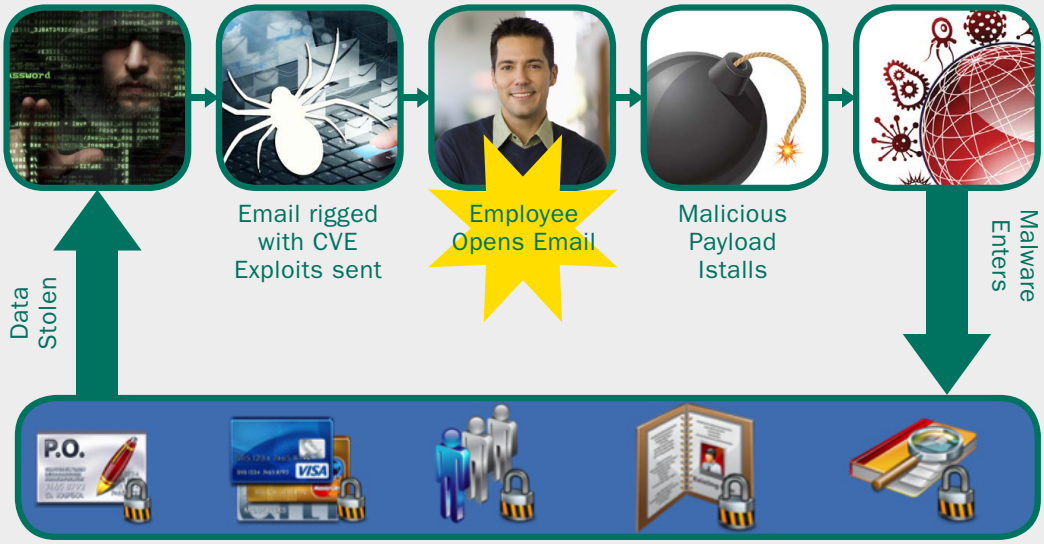
3

Cybercriminals are armed with an entire arsenal of methods to gain access to users' confidential financial information. Most attacks that target financial data have social engineering as their basic element. This can be used either to spread malware or to steal user credentials directly.

Phishing (or **spearphishing** in targeted attacks) is a classic example of using social engineering to defraud users of their financial information by deceiving them into handing over confidential information to cybercriminals. For instance, a disoriented victim may receive an "official" letter in the name of a reputable bank, payment system, or online store, stating that there was a failure on the organization's server, so all clients need to urgently provide their personal data for verification. The pretexts can vary, but in any case the client is prompted to send login credentials in a reply email, type them in an attached web form or on the bank's "official" website, following a link in the email. All information provided by the user will arrive in the cybercriminals' hands.

Phishers use fake websites that are expertly designed to imitate the originals. To make the fraudulent website less conspicuous, the cybercriminals use URL addresses that are similar to those of the original sites with different variations on the line in the address bar. The phishers' fabrications are often hard to distinguish from the original sites. Therefore, experts advise users to access financial sites from bookmarks in their browsers rather than by following an email link. Phishing remains the primary method for infecting users via social engineering, especially for corporate employees.

TYPICAL PHISHING ATTACK



Trojans are dedicated malicious programs designed to steal financial information. Typically, they automatically collect information about payments made from infected computers. Sometimes, they automatically carry out financial transactions in the name of users. When bank clients are attacked with the help of Trojans, phishing emails can also be sent in the name of the attacked bank. In these fake emails, users are not asked to send information, but to open an attached document under some pretext. The attachment, in fact, is a malicious file.

Cybercriminals use both multipurpose banking Trojans capable of attacking the clients of various banks or payment systems, and single-purpose Trojans designed to attack the clients of specific banks. Once on a user's computer, a banking Trojan establishes a foothold in the system, and then begins its assigned task, which is to steal all types of financial information from the user.

In most cases, cybercriminals prefer to use combinations of various techniques to improve their chances of a successful infection and increase the effectiveness of the malicious program. The banking Trojan ZeuS (Zbot) is one of the most advanced, high-tech Trojan programs used by cybercriminals. There are many varieties of this malicious program around the globe, including its functional clone, The Spy Eye Trojan.

Primary ZeuS Features:

- The Trojan steals all information that the user has "remembered on the computer" (e.g., by checking the "Save password" box).
- The Trojan tracks which keys the user presses. If a virtual keyboard is used, ZeuS captures the screen area around the cursor at the time the left mouse button is clicked. As a result, the cybercriminal obtains information about which keys were pressed on the virtual keyboard, and thus knows the user's login credentials.
- ZeuS uses web injections. When a user opens a web page that is listed in the ZeuS configuration file, the Trojan adds new fields in which the user is asked to enter confidential financial information that is of interest to the cybercriminals.
- ZeuS is capable of bypassing the most advanced bank security systems.
- This malicious program is spread with the help of social engineering and by exploiting vulnerabilities in popular software by Microsoft®, Oracle, Adobe® etc. when users visit compromised web sites. Links to these sites are mostly distributed in spam.
- ZeuS is used to steal confidential information to gain unauthorized access to accounts in the world's largest banks. In 2012, researchers recorded 3,524,572 attempts to install this malicious program on 896,620 computers with Kaspersky Lab products installed on them, located in different countries.

This massive spread of banking Trojans is aided by **exploits** for vulnerabilities in Windows® and other popular software. Without letting the user know, these exploits penetrate the system via software vulnerabilities and download other malicious programs that steal financial information from the victim computer. To make the attack effective, the cybercriminals use so-called exploit packs, or packages of exploits to various vulnerabilities, rather than single exploits. An **exploit** pack analyzes the software installed on the user's computer; if it finds a loophole in the software, it picks a suitable exploit to infect the computer. Exploit packs are hosted either on cybercriminals' servers or on hacked resources. Links to the exploits are distributed by cybercriminals via phishing emails, social networks, hosting on compromised sites, or even legitimate, online advertising banners. Exploits, in turn, download Trojans to victim computers. Infections of popular sites are especially dangerous because they are visited by so many users, and when a malicious link is present, each visitor's computer is unobtrusively attacked by exploits that are trying to attach malicious programs to them.

Web injections, or modifying the contents of an HTML page, are a popular method with cybercriminals. A malicious program adds extra fields when the bank's web page is displayed in the browser, prompting the user to enter confidential information. For example, the Trojan Carberp uses a web injection to add extra fields to the online banking entry page, in which it prompts the user to enter his/her bank card number, name of the holder, expiration date, and the CVV/CVC code. If the user refuses to do so, the Trojan displays an error message and blocks the banking session.

The extra information entered by the user falls into the cybercriminal's hands, but does not reach the bank as it is intercepted when the data is sent to the banking server. Therefore, neither the victim nor the bank knows anything about the fraud.

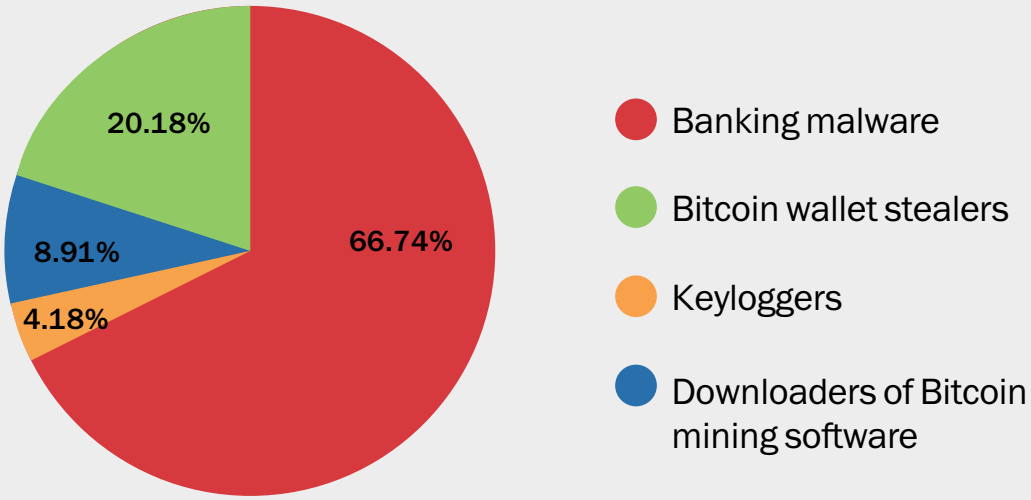
These malicious programs use the following techniques:

- **Keylogging** – Trojans intercept keystrokes when the user types information that is of interest to cybercriminals, such as login credentials.
- **Screenshots** – The cybercriminals take screenshots of the victim's device to capture confidential financial information typed using the regular keyboard. In this case, the cybercriminals only get to know the information shown during the type-in, but cannot access the user's login and password, as typed characters are replaced with asterisks on the screen.
- **Bypassing a virtual keyboard** – The cybercriminal captures an image of the screen area around the cursor at the time when the user clicks the left button of the mouse. In this way, the cybercriminal captures the characters that the user types using the virtual keyboard, and thus knows the user's login and password.

- **Modifying the host file** -- The information stored in this file takes priority over the information that the web browser receives from a DNS-server. Trojans add bank URLs to this file, and assign the IP-addresses of cybercriminals' servers to them. As a result, users who type these bank URLs into their browsers are taken to fraudulent sites, even though they still see a legal bank URL in their browser. If users enter their login credentials on a fake site, this information is sent to the cybercriminals.

- **Intrusion into a running browser process** – With this method, a Trojan can control the browser's connection to the server. In this way, cybercriminals can obtain the login credentials that users enter on the bank site, as well as modify the web-page's content (via a web injection), thus obtaining further confidential information. To complete the vast majority of online financial operations, users need web-browsers. The techniques employed by modern banking Trojans are one way or another related to this software.

DISTRIBUTION OF MALICIOUS BANKING MALWARE IN 2013



Bypassing Two-factor Authentication

4

Banks invest a lot of effort in protecting their clients. Banking Trojans have been so effective that banks have to introduce an extra protection layer – user identification tools. With standard login credentials, customers create a user name and password. With two-factor authentication in place, it is not sufficient to know a user's login and password to gain control over the bank account. With two-factor authentication in place, banks use one-time passwords (Transaction Authentication Number, TAN). In practice, that may be an ATM slip with codes printed in it; SMS messages with one-off passwords that a bank sends to the user's mobile phone (mTAN), or even a dedicated device (chipTAN).

However, cybercriminals see upgraded protection as a new challenge, and keep looking for new ways to bypass it. To bypass the above security systems, cybercriminals have created new methods of stealing data, and modified their social engineering techniques.

One-time Passwords (OTP)

5

The banking Trojan ZeuS has a set of tools in its arsenal which can bypass different types of two-factor authentication. ZeuS uses an interesting tool to collect the one-time passwords that users print out at an ATM.

- As soon as a user is registered with an online banking system and enters a one-time password, Zeus steals the authentication data, displays a fake notification saying that the current list of one-time passwords is invalid, and prompts the user to receive a new list of passwords.
- To receive the "new" list, users must enter their current TAN codes into the appropriate fields, allegedly to have them blocked.
- All login details that are entered are sent to the cybercriminals, who immediately use them to transfer the victim's assets to their accounts.

mTAN

6

Working together with the mobile Trojan ZeuS-in-the-Mobile (ZitMo), ZeuS can steal users' one-time passwords that arrive to the mobile phone.

- When users visit the login page of an online banking system, ZeuS uses web injections to create an extra field in this page, where users are asked to enter a phone number, allegedly to receive a certificate update.
- If users enter the login credentials required for authorization and the phone number, the Trojan steals this information and sends it to its owners. After some time, an SMS arrives to the user's smartphone, containing a link to the "new" security certificate. When users try to install this fake certificate, the smartphone gets infected instead.
- This way, cybercriminals gain access to all the data needed to remotely operate the user's bank account, and they steal money from it.

ChipTAN

5

chipTAN is another method of two-factor authentication. It is used by Western European banks and requires each client to have a special TAN generator device. Having set up a transaction on a banking site, users put their bank cards into the chipTAN and enter the PIN code.

Users then put the device next to their computer's monitor to check the details of the transaction in progress. Having checked the transaction details against the data displayed on the device screen, users enter an additional code from the device to confirm the transaction.

chipTAN is now the most advanced and effective banking security tool. Unfortunately, however, the creators of the banking Trojan SpyEye have learned to bypass this high-tech security tool as well.

- Using web injections, the Trojan modifies the user's list of bank transactions. Because of this, when users log on to the online banking system, they see that a bank transfer for a large sum has arrived, and the account balance has changed accordingly.
- SpyEye, in the name of the online banking system, notifies users that this operation was made in error, and that the account will be blocked until they returns the sum they have allegedly received.
- To prevent this, users initiate a new payment operation to return the money. SpyEye prompts users with the required bank account and the sum of money. The Trojan does not need to steal the generated chipTAN code, as users enter the code with their own hands and confirm the transaction.
- After this, the Trojan tampers with the web page so that it displays the original balance in the bank account, while the money is sent to the cybercriminals.
- This method does not even require extra technical gimmicks on the part of cybercriminals; the attack is based on web injections and social engineering.

USB Tokens

7

A token is a USB device, used as an extra security tool and containing a unique key that the system requests each time the user makes a payment operation. The creators of the banking Trojan "Lurk" found quite an effective way to bypass this protection:

- Users initiate payment operations in the online banking system and enter the details.
- The Trojan Lurk intercepts the payment details and waits for the system to request the token.
- The online banking system requests the token, and users present their credentials by inserting a USB token into the appropriate socket.
- The Trojan intercepts this event, after which it demonstrates a fake "blue screen" which informs users that a dump of the physical memory is being created for subsequent analysis, and asks users not to switch the computer off before the operation completes.
- While users wait for the "operation" to complete (and while their tokens are in the USB port), the cybercriminal accesses these accounts to complete the payment order in the users' names, and transfers the money to another account.

Ransomware

8

Ransomware is a type of malicious software used by cybercriminals that's designed to extort money from their victims, either by encrypting data on the disk or by blocking access to the system. Ransomware is commonly installed by triggering a vulnerability in the victim's computer, which is generally exploited by users inadvertently opening a phishing email or accessing a malicious website that was created by the attackers. In March, Kaspersky Lab's experts found ransomware attachments being sent out in phishing emails from attackers claiming to be from popular online booking services.

Ransomware is commonly installed by exploiting a vulnerability in the victim's computer, which is generally exploited by users inadvertently opening a phishing email or accessing a malicious website that was created by the attackers.

Once the program is installed, it will encrypt the disc of the victim's computer or block access to the system while leaving a "ransom" message that demands a fee in order to decrypt the files or restore the system. This will appear the next time the user restarts her/his system. Essentially, the attackers are holding the computer hostage and are trying to extort money in exchange for allowing access to the computer. However, it's important to note that the victim often doesn't regain access to the computer, even after the "ransom" is paid. It's a scam.

Ransomware is increasing in popularity worldwide, although the ransom messages and scams for extorting money will differ based on geography. In countries where piracy is common, such as Russia, ransomware programs that block access to the system often claim to have identified unlicensed software on the victim's computer and ask for a payment.

In Europe and North America, where software piracy is less common, this approach is not as successful. Instead, popup messages from fake law enforcement agencies will appear that claim to have found child pornography or other illegal content on the computer. This is accompanied by a demand to pay a fine.

RANSOMWARE POSING AS THE DEPARTMENT OF JUSTICE

Protection Against Exploits

9

Since targeted attacks use unique malware, signature-based detection is not enough to identify the malicious code that is used. However, security programs have long had more weapons at their disposal than mere signature-based detection.

Even if the fraudsters have managed to attack the system – via an exploit or a malicious program launched by the user – network traffic control and application control will help to prevent further penetration into the corporate network.

Network Traffic Control

10

Once malicious code (a Trojan or exploit shell code) gets in the system, it usually attempts one or more of the following:

- Establish connection with a command center (outbound connection)
- Open ports for incoming connections
- Download additional modules
- Implement malicious code in other processes to maintain the connection with the command center
- Gather information about the network, its systems and users
- Send the harvested information (IP addresses, computer names and accounts, logins, passwords, etc.) to the fraudster's server.

Generally, having connected to the system, the scammers try to collect information about the corporate network on which the computer is located. In order to collect local finroamtion, the fradstes do not need extra privileges. The list of the running processes, installed software and patches, connected users, etc. can be foound quite easily. Information about the corporate network, including searchers for other vulnerable systems, protection systems, shared folders, network services, servers, etc., is collected using special scripts and utilities capable of masking their activity and bypassing security systems. All this information is sent to the cybercriminals via the Internet for analysis before they prepare the next stage of the attack.

Using network traffic control technology (e.g., Firewall, IPS / IDS), your business can, not only block dangerous network activity, but also detect any penetration into your network. These network traffic control technologies block incoming/outgoing connections by port, domain name, IP address, protocol, and generate statistical analysis of traffic (Net flow) for anomalies while collecting suspicious network traffic for further analysis. They also detect and block outgoing commands or similar output sent via the Internet; downloads of suspicious files from the Internet; and transmissions of confidential information (e.g., IP addresses, logins, computer names, corporate documents, credit cards numbers, etc.).

Firewall and IPS / IDS can detect anomalies in the way network nodes interact as soon as the malicious code tries to contact the command center or actively scans the corporate network for other systems, open ports, shared folders, etc. This anomaly detection allows IT security experts to promptly respond to the threat, preventing further intrusion which might compromise the corporate network.

Application Control

11

Having accessed the target system, the criminals aim to consolidate their success: additional modules and utilities are downloaded onto the system and malicious code providing connection with the command center is often incorporated into trusted processes like explorer.exe, csrss.exe, smss.exe, etc.

Application Control can block the launch and download of untrusted programs and modules from the scammer's hacker set and the HIPS policies should be used to block non-standard - and potentially dangerous - behavior from legitimate software. For example, browsers should not open the ports for incoming connections, the system processes (explorer.exe, csrss.exe, smss.exe, etc.) and other applications (calc.exe, notepad.exe, etc.) should not be connected to external servers and deploy malicious code to other trusted processes – this behavior should be prohibited.

To prevent criminals from gaining control of the system, small businesses should:

- Prevent trusted or potentially vulnerable programs from implementing code in other processes
- Restrict applications' access to critical system resources and files only
- Block potentially dangerous functions that are not a default feature of the applications (network access, installation of drivers, creation of screenshots, access to a webcam or microphone, etc.)

Systems that require the highest protection level should be safeguarded by the Default Deny mode which can block any program from starting up if it is not included in the white list stored locally or in the cloud.

Keeping Your Small Business Safe

12

- Any rights and privileges should be granted only when necessary
- All rights and privileges (access) granted to the users should be properly managed.
- Regularly 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.
- Deploy an effective security solution.
- Use common sense
- Educate your employees (and yourself!)

Many of these measures can be automated. For example, if security policies are violated, special software shows the user a warning message. For some small businesses, systems management technology makes sense to search for network services and unauthorized devices, vulnerabilities, and automatic updates of vulnerable applications.

WHAT IS THE RIGHT SMALL OFFICE SECURITY SOLUTION?

- It includes key security technologies you'll want to use, and not complicated add-ons you don't need and shouldn't have to pay for
- Its efficiency is confirmed by independent research labs
- It has the right tools to grow with an expanding business
- It provides extra protection for financial transactions
- It offers encryption and automated backup/restore functionality to keep your vital business data safe

SECURITY WAKE UP LOCAL FOR SMALL BUSINESS


WHAT TYPE OF BUSINESS ARE YOU?
KASPERSKY lab
WHETHER YOUR BUSINESS IS BIG OR SMALL, EXPANDING OR JUST STARTING-UP, KAPSERSKY LAB HAS THE IT SECURITY SOLUTION TO PROTECT YOU.
THE START-UP BUSINESS
Setting up new business
Buying new IT kit
Safety measures mean one less thing to worry about—now and in the future
Start Up Steve
THE BUSINESS THAT'S HAD ITS FINGERS BURNED
Established business that has recently fallen prey to malware or data loss
The threat has meant that there's a real need to invest—and fast
The business needs to be comprehensively covered so it will never happen again
Suffering Suzie
Irritated Irene
THE BUSINESS THAT'S SWITCHING ITS SECURITY
Established business – while IT not high on the agenda, existing security software has become an annoyance
Slows up systems or fails to give adequate protection
The license is up for renewal so it's an opportune time to look elsewhere
Ambitious Andre
THE EXPANDING BUSINESS
Employing more people
Business is becoming more professional in its outlook
Buying new IT kit to support new people
The time is right to invest in IT security software
Risky Ron
THE BUSINESS THAT KEEPS ITS FINGERS CROSSED
An established business that's never really taken IT security threats seriously
Have always had the attitude of "it won't happen to me" or "I hope it doesn't happen"
A story in the press put IT security on their radar
Interested in security if it's fast and affordable
TOP TEN POINTERS TO HELP PROTECT YOUR BUSINESS AGAINST CYBERCRIME, MALWARE AND OTHER SECURITY RISKS:
1 Assess the potential security risks and identify what needs to be protected.
2 Do you need to protect mobile or tablet devices?
3 Be aware of the legal and regulatory obligations.
4 Define some basic security policies to keep information/computers secure.
5 Set up an education program to improve awareness of security issues internally.
6 Evaluate all the security software products suitable to your needs.
7 Will your security software supplier offer the level of support you need?
8 Would you benefit from additional security features for the protection of online banking or financial transactions?
9 Check the suitability of cloud service providers' security and their contract terms.
10 Choose a security software product capable of protecting all of the computers and devices accessing the cloud.
PROTECT YOUR CUSTOMERS.
PROTECT YOUR BUSINESS.
Spend less time on security and more time running your business.
For essential tips on defending your business against malware and cybercrime, download this easy to read, free guide now!
FREE 64 PAGE GUIDE
Download now
Simplifying IT Security for DUMMIES
KASPERSKY lab
©1997-2013 Kaspersky Lab ZAO

Kaspersky Small Office Security

13

Kaspersky Small Office Security provides world class protection that's designed to be powerful, quick and easy for many small businesses.

KEY FEATURES:

- Protects your Windows PCs, servers and Android™ mobile devices in real-time against known and emerging threats.
- Safeguards your online transactions against financial fraud.
- Protects you and your business against online threats.
- Allows you to regulate or block employee internet access.
- Protects your data and your customers' data against theft, loss and corruption.

To learn more about Kaspersky Small Office Security or to request a demo, visit our Small Business Cybersecurity Learning Center.

Kaspersky Endpoint Security for Business

13

Kaspersky Endpoint Security for Business, our advanced business security platform, is available in progressive tiers, allowing you to expand your security as your business grows.

KEY FEATURES:

- Centrally managed anti-malware protection for Windows, Macintosh® and Linux® endpoints.
- Endpoint Controls to manage the use of 'plug-in' devices like USBs; limit what software can run and regulate employee internet access.
- Mobile Device Management to help deploy and manage smartphones and tablets.
- Full-disk, folder or file encryption to protect data that's lost or stolen (for Advanced tier users)
- Systems Management offers a range of tools and security measures designed to reduce risk and simplify your network (for Advanced tier users).

To learn more about Kaspersky Endpoint Security for Business and to use our helpful product selector to determine the right cybersecurity solution for your business, visit the Kaspersky Business Knowledge Center.

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 16-year history, Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for educators, consumers, SMBs and Enterprises. The company currently operates in almost 200 countries and territories across the globe, providing protection for more than 300 million users worldwide.

Call Kaspersky today at 866-563-3099 or email us at **corporatesales@kaspersky.com**, to learn more about Kaspersky Endpoint Security for Business.

www.kaspersky.com/business

SEE IT. CONTROL IT. PROTECT IT.
With Kaspersky, now you can.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC # 242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.