Cybercrime

How safe is your business?

Find out the risks associated with doing business on the internet and the 6 simple steps you can take to protect your business

Organisations face an average of

66 cyber attacks weekly that cause business disruptions

Hacker

a person who uses computers to gain unauthorized access to data

The total number of breaches in 2013 was

62%

higher than in 2012

Malware

is software specifically designed to disrupt or damage your computer system

Most organisations now use the internet to do business; to advertise and sell; find new markets, customers and staff; communicate with customers and suppliers and carry out financial transactions. The internet is now an indispensable business tool that can yield great opportunities and benefits, but it can also attract risks.

Everyday, cybercriminals unleash waves of new attacks attempting to steal information, money and disrupt UK businesses. Although no one really knows the full size of the global cybercrime market; James Lyne, Director of Technology Strategy at Sophos, a developer and vendor of computer security software and hardware, estimated that on average £30k-£40k per day is stolen by cybercriminals.

Most attacks can be prevented or at least detected with basic security practices, processes and IT systems. Are you confident that your cybersecurity minimises the risks of this happening to your business?

Take the 6 simple steps set out in this paper to protect your business, customers and assets.

Who are the cybercriminals?

Most cybercrimes are committed by individuals or small groups. However, large organized crime groups are on the rise. They treat cybercrime like a business and form global criminal communities that share strategies and tools. They even have an underground marketplace where cybercriminals can buy and sell stolen information and identities.

It is very difficult to catch cybercriminals because they operate anonymously, from any location with the help of the internet. In fact, the majority of computers used in cyber-attacks have already been hacked and are being controlled remotely.

How can you be attacked?

Cybercriminals use automated programs to scan for unprotected computers or computers with software or hardware vulnerabilities. There are 2 ways that you can be affected by cybercrime;

1. Your computer is used to steal your personal information. Trojans are a form of malware masquerading as something you may want to download or install, that can then allow external access to your computer. Kaspersky report that 350,000 unique malware codes are written every single day. That's 350,000 new opportunities a day for the cybercriminals to compromise our computers for their criminal purposes.

2. Your computer is used to facilitate other crimes and attacks on others. Computers can be hijacked to provide storage of illegal images or downloads, as well as a platform to launch attacks or commit crimes against others.

Trojan

is a malicious program that performs actions not authorised by the user

1 in 392

emails contain a phishing attack.

Phishing

is sending fraudulent emails to try to obtain financial or other confidential information

Remember!

Sensitive information should never be sent over public wi-fi hotspots

The tools cybercriminals use:

- Web pages that are created to look like legitimate businesses or copies of actual websites. Once the page has loaded it launches malicious software into your computer via the web browser's cache, which can then hijack your email account or send out user information such as bank account and credit card numbers.

- Spam emails with malware attached. Sometimes sent from a trusted contact (they are most likely unaware but have been infected themselves), because the email is from someone you know, you are more likely to click on the link and infect your system.

- Phishing emails are also on the rise. These emails, often looking very similar to genuine correspondence, pretend to be from your bank or a service provider in order to steal your account details.

- Social media; this works in a very similar way to spam. Users are more likely to click a link if it appears to come from a friend on a network such as Twitter or Facebook. The 'breaking news' and 'popular' features on these sites can tempt unsuspecting victims to click on unsafe links.

- Drive-by downloads; internet users simply need to visit a corrupt website to become exposed to malware that attempts to exploit vulnerabilities in browsers, applications and operating systems.

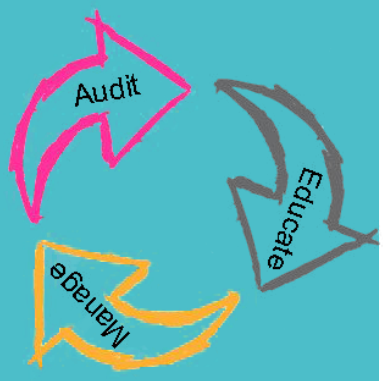
Cybercrime and Wi-Fi hotspots

A major trick hackers are using right now called 'man in the middle' revolves around the personal hotspot feature available on smartphones . As the name implies, the criminals insert themselves between the user and the hotspot to gather all data passing between the two points.

Hackers attempt to trick people into connecting to a hotspot that, superficially, resembles that of the public wi-fi available. They create a wi-fi hotspot from their phone or laptop and rename it to suit the public place they are in, i.e. Costa or Travel Lodge. When you, the unsuspecting customer, connects using this 'network', the hacker is able to obtain your IP address and with free software can see all of your passwords and capture your key stokes.

Phones are a major weak point due to this and once they have control of your phone they can then access your contacts and infect them all with malware as it is coming from a trusted source.

Over 552 million identities were exposed via breaches in 2013



Just 3% of SMBs train staff on safe workplace internet usage

3 most common passwords of 2013:

⇒ 123456

⇒ password

⇒ 12345678

How can you protect yourself and your business?

According to a survey by the National Cyber Security Alliance and Symantec 83% of SMB's take no formal measures against cyber threats, even though almost half of all attacks are aimed at SMBs.

Don't take the risk of remaining vulnerable; Gartner Group say that 43% of companies were immediately put out of business by a 'major loss' of data, and only 6% survive longer than 2 years.

Here are the steps you can take to help shield your business from cyber-attacks:

1. Educate employees.

Security in any company, of any size is ultimately everyone's responsibility, so the best place to start is with your employees. They are the most common cause of data breaches but they can also be your first line of defense. It is all about educating your staff to have the right frame of mind to recognize potential threats and be proactive in taking precautions.

Never click any links in an email which seem odd or suspicious, even if they come from a trusted source, they could have been hacked themselves. Also, remember that reputable and trustworthy companies will never ask for personal details via email, this is a scam known as phishing. Hackers are very good at making their efforts look genuine, therefore even if the email seems legitimate always contact the company directly.

2. Passwords.

Enforce password policies with rules for complexity and frequent changes.

Passwords should be at least eight characters long with a mixture of numbers, symbols and upper and lowercase letters. Alternatively James Lyne, Sophos's global head of security research suggests using a lyric from a song, it's something that is hard for a computer program to guess but easy for you to remember.

Additionally, make sure your employees don't use the same password for more than one account. Passwords should also be changed regularly, the National Cyber Security Alliance suggest every 2 months as a good standard, so I would advise setting up an alert system to remind staff.

43%

of SMBs take no internet safety precautions at all

1 in 8

legitimate websites have a critical vulnerability

59%

of ex-employees admitted to stealing company data when leaving previous jobs

Sources:

BBC – Gagngsters.com documentary

Gartner – Homeland Security Newswire

Splashdata

Symantec – 2014 National Security Threat Report

National Cyber Security Alliance & Symantec

3. Software. All computers should be patched, up-to-date and protected with anti-virus and anti-spyware software to avoid viruses that could compromise the security of confidential information. It is one of the major ways cyber-criminals break into your system, so more up-to-date software means a much lower probability of being attacked.

4. Access to data. It is important to keep your data where you know it is safe, not on hard drives where it could be stolen or cloned, and restrict the use of USB ports to make it as difficult as possible for users to copy the data. This also stops people being able to transfer malicious items from a USB to the computer.

Be cautious of entering personal details into a website where you do not see 'https' in the address bar. 'Https' is an encrypted version of a website, which means that the information between yourself and the website is encrypted.

5. 'Kill Switch'. In an increasingly mobile business world, security for your mobile devices, applications and content is a major concern. Whether it is a company or personal device, employees access company data, email and more from their mobiles, tablets and laptops. Invest in Mobile Device Management software that secures mobile devices with encryption and password protection plus lets administrators remotely wipe data from devices if they are lost or stolen.

6. Next generation firewall (NGFW). Ramsés Gallego, international vice-president at IT trade body ISACA comments that "criminals are forever evolving new tools and looking for new vulnerabilities that leave the door open to get them inside systems. It's no longer just a case of fighting off a virus on its own. Today the task has moved on to ensuring all your defenses work together."

A next-generation firewall does just that. It integrates a wide range of network security functions into a single device. From standard firewall features such as packet filtering, network address translation and VPN capabilities to integrated network intrusion prevention and an 'application awareness' capable of identifying applications and applying controls at the application layer (for example allowing Skype calls but blocking file transfers). It is able to detect and block sophisticated attacks by enforcing security policies at the application, port and protocol level.

This white paper is brought to you by Opus. If you would like to learn more about protecting your data from theft and compromise, please contact us on info@opusteam.co.uk or give us a call 0345 3031 001.

With cybercrime it is a case of when not if. Act now to protect your business.