7 CYBER SECURITY MYTHS

THE MYTH

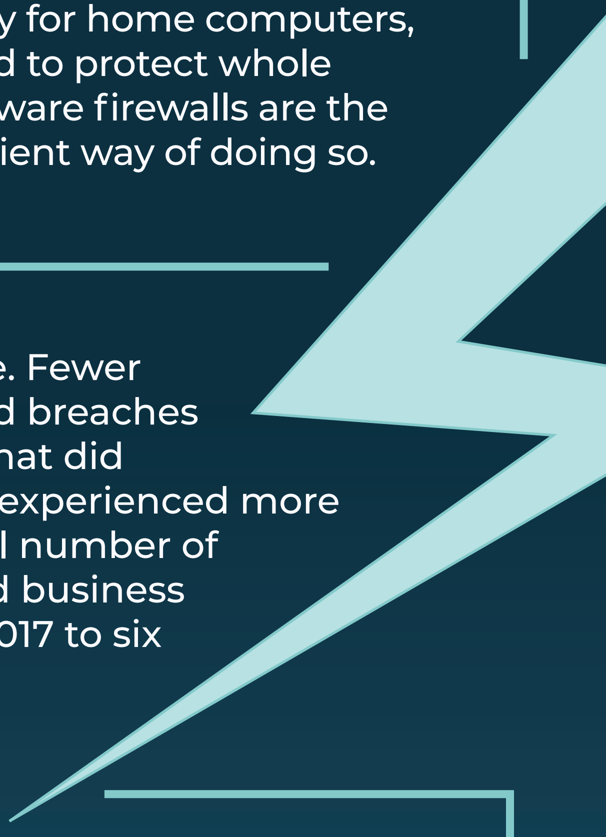
THE REALITY

Cyber crime only affects big organisations

31% of micro and small businesses reported breaches in 2018. Meanwhile, 60% of medium firms were attacked – just 1% less than large companies.

You only need antivirus and firewall software

Antivirus is important, but it's difficult to defend against new threats before they make into malware databases. Software firewalls, meanwhile, are okay for home computers, but businesses need to protect whole networks, and hardware firewalls are the most effective, efficient way of doing so.



You've already suffered an attack. It won't happen again

The opposite is true. Fewer businesses reported breaches in 2018, but those that did indentify breaches experienced more of them. The typical number of attacks per affected business went from two in 2017 to six in 2019.

Only IT people should deal with cyber security

Everyone needs to be vigilant and informed when it comes to security. Major breaches can start with any employee, computer, server or device in your business.

Apple devices don't get viruses

Macs can be hit by malware, and so can mobile devices, including iPads and iPhones. It's true malware is less common for Apple systems, but it does exist. Mac malware detections leapt up 60% in just three months around the beginning of 2019.

You can stop all cyber attacks

Sadly not. Good cyber security technology and practices can radically reduce your chances of being hacked, but full protection can never be guaranteed. That's why backup and disaster recovery are so important.

You don't have anything worth stealing

If the data stored on your systems has value to you, it has value to criminals. With ransomware, they can lock down your data and cripple your business.

Statistics from Malwarebytes Q1 2019 Cybercrime Tactics and Techniques report and the Cyber Security Breaches Survey 2019.

tmb technology means business

www.tmb.co.uk
info@tmb.co.uk
0333 900 9050