Unsplash © Franck

5 cybersecurity myths that are compromising your data

As the importance of cybersecurity has increased, so has our awareness of it. Poor cybersecurity has been identified as the most pressing threat to businesses today.

Issues with cybersecurity often stem from a lack of cybersecurity awareness. In fact, according to the 2020 Cyberthreat Defence Report, a lack of cybersecurity awareness was identified as the biggest detriment to an organisation's cyber-defences.

The reasons for this lack of awareness include no training on cybersecurity and persistent misinformation. Despite more media attention than ever, there are still some common misconceptions about cybersecurity that put businesses at risk.

Here, we bust the top myths around cybersecurity and how you can address them.

Cybersecurity isn't my responsibility

IT security is still viewed as the IT team's problem when that's not the case at all. All employees have a responsibility to ensure the security of their business. Your people are the frontline of your defence and represent its biggest attack surface. They are the people hackers are targeting with phishing campaigns because they're banking on a lack of security knowledge.

This myth can have serious consequences if your people don't practise basic cybersecurity hygiene. If they don't take care when clicking links in emails or downloading software, they could compromise your business' security. Education is critical because your employees need to understand why cybersecurity is so important and that they have a role to play. Training will also equip them with the skills to spot threats and change their behaviour for the better.

Hackers don't target small businesses

If media coverage is anything to go by, only large organisations like Yahoo, Uber and Marriott get attacked, right? This is wrong.

This myth is particularly persistent because of mainstream news and the fact that hackers can potentially extort higher sums of money from these businesses. But the Federation of Small Businesses (FSB) reports that *UK small businesses* are targeted with over 10,000 cyber-attacks a day. The same report highlights widespread weak security procedures in small businesses, including a lack of formal password policies, not installing updates and not using security software.

While the financial gain from targeting enterprises is more lucrative, the stakes are higher for small businesses. Cybercriminals know this. A cyber attack could destroy a small business and force it to close, and that's why one small business is *successfully hacked every 19 seconds in the UK*. Small businesses that have a limited cybersecurity budget should tap into the knowledge of an IT support service, who can advise on the most suitable defences.

My passwords will keep me safe

There are still two long-held misconceptions around passwords. The first is that adding capital letters, numbers or special characters to your one-word password will make it uncrackable. This myth is perpetuated by a lot of business accounts that have these requirements.

However, the real measure of password security is length. Software can crack short passwords, no matter how "complex", in a matter of days. But the longer a password is, the more time it takes to crack. The recommendation is using a memorable phrase – from a book or song, for example – that doesn't include special characters.

But determining a strong, (almost certainly) uncrackable password is only the first step. If the service you're using is hacked and criminals gain access to your password, you're still vulnerable. That's where two-factor authentication

(2FA) and multi-factor authentication (MFA) come in. These methods require you to set up an extra verification step. When you log in, you'll be prompted to enter a security code that will be sent to your phone or even accessed via a dedicated verification app. That means if a hacker ever gets their hands on your password, they'll still be thwarted.

A basic anti-virus will be enough to protect my business

Gone are the days where your McAfee or Avast anti-virus solution will be enough to protect your business. Now, there are dedicated tools to fight against specific threats like ransomware. A synchronised approach to security, whereby your solutions all interact with one another, is generally accepted as the most robust. Your security solutions should cover your endpoint, firewall, network connections, email and more. In addition, backup and disaster recovery solutions are recommended to mitigate any potential incidents.

We only need to protect against hackers

While hackers pose an enormous threat to your business, you can't ignore the possibility of malicious insiders or even staff accidents. One of the most highly-publicised accidental breaches was a Heathrow Airport staff member losing a USB stick with sensitive data on it. Luckily, the person who found it handed it in rather than using it maliciously. The company was still fined £120,000 for its failings in data protection. It's also all-too-easy for an employee to accidentally email a spreadsheet with sensitive data outside of the company.

Equally, a disgruntled employee who has access to sensitive employee or customer information could willingly steal or share it. Locking down access to your core systems and ensuring fewer employees have access to them can help you protect against this. For accidental breaches, implement policies that state removable devices must be encrypted. You can also configure your email settings to block certain attachments from being shared outside of your organisation.

Barry O'Donnell is the chief operating officer at *TSG.*

Article by BARRY O'DONNELL