THE ONE POINT

INSIDER DEBUNKED

Microsoft

Uncovering common myths
and misconceptions

The what, why, and how of cybercrime

Around the globe, cybersecurity is a constant headline in the news. What is this new digital norm everyone's talking about, and what can we do to stay safe and secure in this ever-changing connected world?

We'll explore 3 common cybersecurity myths, and we'll arm you with resources to meet this growing threat head on and fight back with strong cybersecurity defense.

Myth #1 – I'm not a large enterprise, hackers won't attack me

Did you know that 61% of the data breach victims in this year's report are businesses with under 1,000 employees?[1] Hackers are intelligent, and sophisticated, but they're also often looking for something quick and easy. Small and medium businesses who believe they are not at risk, tend not to invest as much in cybersecurity; thus, making them an easier target. They collect and store a wealth of data, but often don't realize it's true value, and therefore don't put the right measures in place to protect it.

Key takeaway: No one is exempt from cyber-attacks, and the more you do now to learn and defend, the better prepared you will be if something does happen.

Myth #2 - I don't have the funds or resources for cybersecurity

It might feel like you're not in a financial position to invest in cybersecurity yet - especially if you believe your business is too small to attract the attention of would-be-hackers. But have you stopped to think about the cost implications of a breach? There's loss of business due to reputational damage, legal fees, loss of competitive edge, and so much more at stake.

Key takeaway: Cybersecurity Ventures predicts £1 trillion will be spent globally on cybersecurity from 2017 to 2021. Ensure you're a part of that investment, so you don't get left behind.

Myth #3 - Technology will fix everything

It's true that customers need robust technology systems and tools to be prepared against cyberthreats, but it's also critically important to focus on education. If employees are properly trained to detect a scam or raise a suspicion, that can prevent an attack before the malware is even in the system.

And training shouldn't just stop there. Employees who have data handling compliance training, who understand the processes for implementing security measures, and who help enforce the company policy, all contribute dramatically to prevention.

Key takeaway: Train your staff to identify cybersecurity threats and handle sensitive information appropriately, to reduce the risk of cyber security breaches.

In this digital age, businesses of all sizes are susceptible to cyber-attacks. It doesn't take much to invest upfront in the right education, resources, tools, and technologies to put prevention and mitigation at the forefront of your customer's strategy, rather than reacting to an expensive cyber security crisis after the fact.

For more information, visit Microsoft Secure