“Savings” That Could Cost You EVERYTHING

As a business leader, you’re always looking for ways to increase revenue, cut expenses and grow your bottom line. Implementing AI tools, shopping services and running a more efficient operation are great ways to do that. One place you do NOT want to cut corners is using free antivirus or firewall software.

In today’s blog, we’ll share why these ***seemingly*** helpful software solutions are a detriment to your business and why a 10-minute call with our team might just be the best investment you’ll make this year.

Free software often lacks necessary features and is limited in what it can detect.

Free antivirus software and firewall solutions can protect your business against some known viruses but not all of them, and they likely won’t have the ability to protect you against other comprehensive threats, like malicious files, unknown or unidentified threats and more. Cybercriminals are constantly rolling out new and “improved” viruses to trick even the most robust security solutions, which makes it difficult to believe that free, infrequently updated antivirus solutions could offer the level of protection needed to keep you secure.

There’s no such thing as a free lunch.

While free cybersecurity solutions sound like a good way to save a few bucks, you have to stop and realize these programs will make their money somewhere. The most common ways they make money are through ads, sponsored recommendations and collecting and selling user data. They collect and sell your personal information, like age and gender, and installed apps, to third-party advertisers.

Some free solutions are already infected with malware.

Ironically, these free cybersecurity tools can come with malware already installed to infect your computer upon downloading them. It’s also difficult to determine the difference between real free software solutions and fake ones created by hackers looking to trick unsuspecting business owners who hope to save a buck into downloading an infected version that immediately opens up your network to them.

Free antivirus software is mostly reactive, detecting infections after they’ve happened.

The point of having cybersecurity solutions is to try to prevent a data breach from occurring in the first place. Most free solutions are reactive and won’t keep unwanted intruders out; they simply alert you when one has already breached your network. If you're going with a free solution, make sure you have a robust recovery plan in place. You'll likely need it.

Cybersecurity solutions are not as expensive as most business owners think and are more cost-effective than dealing with a data breach. If you have been using free antivirus or firewall software in your organization, it's time to level up. **We will provide you with a FREE Security Risk Assessment that will detail if, and where, you are vulnerable and what to do about i**t!

Get your FREE Cybersecurity Risk Assessment: Click here to schedule a call, call us at 215-769-9980, or visit our website at AOR-ITS.com.