How can SMEs protect themselves in the world of Cybercrimes?

It could be you…

According to the research conducted by Federation of Small businesses (FSB), SMEs are highly vulnerable to cybercrime. SMEs do not have as much cyber protection as the larger enterprises, hence they act as the easiest and the weakest link in the chain of victims.

Also, most of the SMEs have a notion that they are not at risk because they are not as big or important to be a target.

With the increasing cybercrimes and the very latest Wannacry Ransomware attack, the cause of cybersecurity measures needs to be prioritized. Experts suggest SMEs to adopt the following ways to protect their digital space:

Create Backup Plans

The very first and the basic activity is to have updated backups of all the data and files as to be secured at the time of major emergencies and data loss. You do not want to lose anything essential. Backup solutions can protect the systems from catastrophic data loss. Automate and schedule the backups.

Install Anti- Virus Software

The next step being installation of anti-virus software to protect from various amount of malicious cyberattacks. It is essential to have Business- Specific software installations and it should be configured to update itself, it should do so every time the system is connected to internet. Leading software can detect, remove, and protect the machines and network from malware.

Spread Awareness

Most of the employees hardly care regarding the rules of digital security of the company, it is most of the times human error and unawareness that make the enterprise more prone to the attack. Thereby, it is of utmost importance to train the employees, make them aware and educate them in preventive measures. The employees should be made aware of the common hacking tactics like Phishing, social engineering, packet sniffing etc.

Take Expert Advice.

SMEs should always seek the advice of industry experts. It is crucial to choose a right partner in case of security provider. Cost does not always equate best; hence right guidance is the key.

Build Cyber Resilience

Cyber Resilience suggests an entity's ability to consistently deliver the intended outcome despite unfavorable cyber events. Disaster recovery operations are a part of this concept. It is also known as active cyber defense. Hence, any enterprise should act in anticipation to oppose an attack.

By following all the above-mentioned measures, an SME can assure its cyber security to a considerable extent.