10 Ways to Protect Your Business from Cyber Attacks

FUSION MANAGED IT

1. Multi-Factor Authentication

Prevent hackers by adding an extra layer of security to employee logins and other high-risk areas of your network with multi-factor authentication. Even if your passwords are leaked or stolen, your data will stay protected.

2. Regular Software Updates

Outdated software is one of the most common ways hackers gain access to systems. You can automate your software to update so that you're never left vulnerable. We take care of your updates so that you can have peace of mind.

3. Endpoint Detection and Response

Endpoint detection and response (EDR) is a type of security software that helps you detect, investigate, and respond to malicious activity on your system. EDR can give you visibility into what's happening on your network and help you contain and mitigate threats.

4. Data Backup and Disaster Recovery

Backing up your data is one of the simplest and most effective ways to protect yourself from cybercrime. Have multiple backup locations (physically and in the cloud). Create a plan for recovering your data in the event of a disaster—our experts can help you make a strategic plan for bouncing back after any roadblock.

5. Security Awareness Training

Make sure all your employees are aware of the dangers of cybercrime and how to protect themselves. Teach them your data policies, how to recognize phishing emails, and what to do in case of a breach. Require security awareness training on a regular basis.

6. Application Control

Applications can be a major vulnerability in your network. Control which applications are allowed to run on your system and use mobile device management (MDM) to secure and monitor devices that connect to your network.

7. Firewalls & Intrusion Prevention Systems

A firewall is a critical part of your cybersecurity infrastructure. Make sure it's enabled and up-to-date and consider using an intrusion prevention system (IPS) to help detect and prevent unauthorized access to your network.

8. Web Filtering

Web filtering helps you control which websites employees can visit and can also block malicious websites that could infect your system. It's a simple way to boost your security and protect your data.

9. Data Encryption

Encrypting your data makes it unreadable to anyone who doesn't have the key. It's a simple way to protect your information and ensure that only authorized people can access it.

10. Mobile Device Security

With the switch to at-home work, so many cyberattacks occur through mobile devices. Make sure you have a comprehensive mobile security policy in place and use mobile device management (MDM) to secure and monitor devices that connect to your network.

FUSION MANAGED IT

+1 (864) 475-9370

fusionmanagedit.com

info@fusionmanagedit.com