

7 Things You Can Do to Protect Your Business From Ransomware

1. Update your Software

Software updates often include security patches and improvements.



Check your applications regularly to make sure you haven't missed any updates.



2. Layer Security Measures



Use a combination of security tools so that if one fails, there are backup protections.

TIP

These can be tools such as firewall, anti-virus software, multi-factor authentication, cyber insurance, and cloud data loss prevention.

3. Security Training

Staff remain the weakest link in a business's cyber security due to a lack of training and awareness.

TIP

Perform regular training sessions to keep employees vigilant and informed.



4. Access Controls



files, programs, and accounts to those who need it.

Only give minimal access to

Administrators should only have the

permissions required to complete a specific task.

5. Multifactor Authentication (MFA)

keys, temporary unique codes, or other factors to a basic username and password.

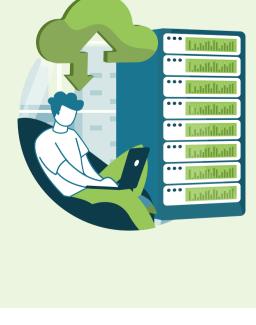
MFA adds biometrics, security





You can avoid paying a ransom

6. Back up EVERYTHING



altogether by regularly backing up your company's data and testing those backups.

TIP

Use a mixture of off-site and cloud-based backups

to maximize backup security.

PRO TIP

Use Microsoft OneDrive to automatically backup files on PCs and Macs.

7. Spam Filters

adding strong spam filters to your

email and other messaging services.

TIP

Authenticate inbound emails by using Sender

Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail

(DKIM) to prevent email spoofing.

Reduce the risk of phishing by

