Take these practical steps to keep your company data from being held hostage.

Three levels of ransomware

Low grade

Middle grade

Most dangerous

How dangerous is encrypting ransomware to your business?

Frequency

Data

Money

Reputation

Should you pay the ransom?

We advise businesses to refuse to pay ransom demands. It's illegal to pay ransom, and most experts agree that it only encourages hackers to keep at it. Paying the ransom will give you access to your files again. The quickest way to retrieve your files is to pay the ransom. However, cybersecurity professionals warn that doing so will only help the hackers further. Billions of dollars are lost every year to ransomware.

You're vulnerable if...

Proactive prevention

The best protection is prevention. Take these steps to keep ransomware away from all your business.

1. Patch your system.
2. Educate users.
3. Back up files.
4. Prevent it before it happens.

What can you do if you're infected?

If you've been responsibly backing up your files, not all hope is lost. Scan your backups for malware on another PC that isn't infected. Then run a scan on the infected machine to see if you missed anything.

If backing up onto a USB or external hard drive, be sure the devices are physically disconnected from your network.

Be sure backup files are not stored on a mapped drive. Some strains of ransomware can even encrypt files on a mapped drive. Some strains of ransomware can even encrypt files on a mapped drive.

Reputation investigations report that if 1,000 records are lost, data from hackers. Hospitals paid $17,000 to return them. Once encrypted, you can't get the files back—unless you pay the ransom. The FBI or U.S. Department of Justice investigations report that if 1,000 records are lost, data from hackers. Hospitals paid $17,000 to return them. Once encrypted, you can't get the files back—unless you pay the ransom. The FBI and other law enforcement officials might encourage individuals and businesses to pay the ransom—it's the quickest way to retrieve your files. However, cybersecurity professionals warn that doing so will only help the hackers further. Billions of dollars are lost every year to ransomware.

Invest: It's called security.

It's the most effective strategy. Take these steps to protect your IT environment from ransomware threats:

1. Install multiple layers of cybersecurity protection. We recommend these layers:
   - Antivirus with multiple-factor authentication.
   - Firewall.
   - Active monitoring.
   - High-level encryption and on a secure cloud server with data.
   - Anti-ransomware.
   - Antivirus with multiple-factor authentication.
   - Firewall.
   - Active monitoring.
   - High-level encryption and on a secure cloud server with data.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware.
   - Anti-ransomware. 

Take your first step in proactive prevention today and try out Malwarebytes business products. Go to malwarebytes.com/business to learn more.