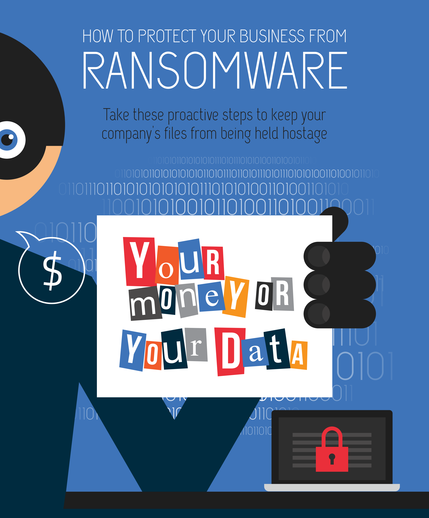
HOW TO PROTECT YOUR BUSINESS FROM

RANSOMWARE

Take these proactive steps to keep your company's files from being held hostage



Three levels of ransomware

Ransomware: a type of malicious software designed to block access to a system until a sum of money is paid.

Low grade

Scareware

Fake antivirus tools pretend to detect malware issues and demand payment to fix them.

Middle grade

Browser or screen locking ransomware

Law enforcement scams use fake FBI or U.S. Department of Justice messages to claim they've detected illegal activity on your computer for which you need to pay a fine.

Most dangerous

Encrypting ransomware

Pop-up messages say your files are encrypted and demand ransom money be paid by a deadline in order to return them.

How dangerous is encrypting ransomware to your business?

Frequency

Millions of ransom attacks are attempted on companies both small and large each year.*

*NPR, All Things Considered, 2/22/16

Data

Ransomware can encrypt your company's most important files, such as accounting, medical data, or confidential customer information. Once encrypted, you can't get the files back—unless you pay the ransom.

Money

In February 2016, Hollywood Presbyterian Hospital paid $17,000 to retrieve patient records from hackers. The Verizon Data Breach Investigations report estimates that if 1,000 records are lost, businesses can expect to lose more than $67,000. As the size of the breach increases, so does the cost to business—exponentially.

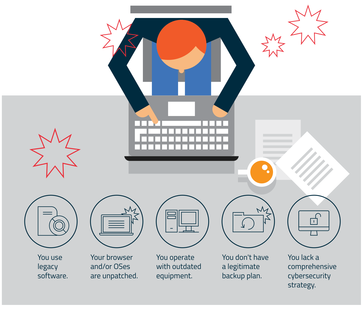
Reputation

Some newer forms of ransomware threaten businesses not only with encrypting files but also leaking them online.

Should you pay the ransom?

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 don't recommend it. There's no guarantee that paying the ransom will give you access to your files again. Also, it makes you a target for future malware infection.

You're vulnerable if...



- You use legacy software.
- Your browser and/or OSes are unpatched.
- You operate with outdated equipment.
- You don't have a legitimate backup plan.
- You lack a comprehensive cybersecurity strategy.

Proactive prevention

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

1 Patch your system

Keep browsers, OSes, and other software applications up-to-date.

2 Educate users

One of the most common ways that computers are infected with ransomware is through social engineering. Educate users on how to detect phishing campaigns, suspicious websites, and other scams.

3 Back up files

Make secure copies of your data on a regular basis and store them offsite.

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

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

We recommend storage on a secure cloud server with high-level encryption and multiple-factor authentication.

4 Invest in layered security

Installing multiple layers of cybersecurity protection can detect and block ransomware attacks before they happen. For the best protection, we recommend these layers:

- Firewall
- Anti-exploit
- Antivirus with active monitoring
- Anti-malware
- Anti-ransomware

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 clean any traces of ransomware or other malware. If your backups are clean, you can restore them to your computer.

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

Malwarebytes