Ransomware is a type of malicious software designed to encrypt sensitive data, or confidential customer information. Once encrypted, you lose access to a system until a sum of money is paid. The quickest way to retrieve your files is to pay the ransom. However, cybersecurity professionals don’t recommend it. There’s no guarantee that paying the ransom will give you access to your files again.

You're vulnerable if...

Patch your system

Educate users

Back up files

Train: 3 layers of security

What can you do if you're infected?

Three levels of ransomware

Low grade

Middle grade

Most dangerous

Frequency

Data

Money

Reputation

Ransomware: a type of malicious software designed to encrypting files to your business? Yes, unpatched.

Frequency

Data

Money

Reputation

Anti-terrorists or legal entities. The best protection is prevention. Take these steps to keep ransomware from harming your business.

How dangerous is encrypting ransomware to your business?

How to Protect Your Business from Ransomware

Take these proactive steps to keep your business safe and clean. Patch your system, educate users, back up files, and train: 3 layers of security.

Three levels of ransomware

Low grade

Middle grade

Most dangerous

How to Protect Your Business from Ransomware

How dangerous is encrypting ransomware to your business?

How to Protect Your Business from Ransomware

How dangerous is encrypting ransomware to your business?

How to Protect Your Business from Ransomware

How dangerous is encrypting ransomware to your business?

How to Protect Your Business from Ransomware

How dangerous is encrypting ransomware to your business?

How to Protect Your Business from Ransomware

How dangerous is encrypting ransomware to your business?