

Topics

1. What is Ransomware?
2. What are the Types of Ransomware Attacks?
3. How Ransomware Affects a Business
4. The Cost of Ransomware Attacks for Business
5. Can Antivirus Detect Ransomware?
6. How to Prevent Ransomware
7. How to Detect Ransomware
8. How to Stop a Ransomware Attack
9. How to Remove Ransomware
10. How to Recover from Ransomware Attack?
11. **How to Protect Yourself From Ransomware**
 - The ransomware playbook
 - Essential ransomware protection strategies
 - People also ask
 - Layered security will make you a hard target.
12. Ransomware Attacks on Businesses Statistics

Share    

How to Protect Yourself From Ransomware

Published: **June 25, 2025**

By:  **Brenda Buckman**

Key Takeaways

- Train your team: Phishing attacks are the #1 entry point. Well-trained employees can stop attacks that even the best security techs miss.
- Backups are your parachute. Immutable, offline backups are your last line of defense. And like a parachute, you'd better know it works before you need it.
- Patch or be prey. Most ransomware exploits known vulnerabilities. Don't be the unpatched server when ransomware is prowling.

Ransomware is a cyber nightmare. It's a digital stick-up, and your business is the bank. One attack can freeze your operations, encrypt critical files, and leave you staring at a demand for cryptocurrency while your revenue burns. Learning how to protect from ransomware isn't only an IT issue. It's about business survival.

Cybercriminals who traffic in ransomware are organized. But unlike the gangsters of the 1920s, they don't kick down your door brandishing Tommy guns. They study your habits, find the weak spots, and wait for the perfect moment to strike. As they've become more sophisticated, their playbook has evolved from simple encryption to full-blown digital extortion.

[Try Huntress for Free](#)
[Get a Free Demo](#)

The ransomware playbook

Modern **ransomware attacks** aren't smash-and-grabs. They're surgical operations that follow a cold, calculated script:

- ✓ Break in. Phishing emails, compromised credentials, or unpatched vulnerabilities let them inside.
- ✓ Set up shop. Attackers plant backdoors and map out your network like they own the place.
- ✓ Steal first, lock later. Sensitive data is exfiltrated before encryption, setting up a double-extortion play.
- ✓ Paralyze everything. Files get locked down, operations grind to a halt, and the ransom note arrives.
- ✓ Apply pressure. Countdown clocks, threats to leak data, and public humiliation tactics force your hand.

It's like watching a team of professional bank robbers case the joint, disable the alarms, take hostages, clean out the vault, and then demand ransom—except they can do it to dozens of targets simultaneously while sitting safely behind their keyboards. Understanding this attack sequence is your first step to implementing effective protection from ransomware.

Average Activity Before Ransomware Takes Hold

Average number of actions taken before triggering ransomware

✓ 18

Of incidents observed by Huntress in 2024 saw data exfiltration as the top action taken before ransomware dropped

✓ 71%

Pre-ransomware notifications sent by the Cybersecurity Infrastructure and Security Agency (CISA) in 2024 (as of Nov. of same year)

✓ 2,131

Number of pre-ransomware notifications CISA sent in 2024 over 2023

✓ 2x

Before Ransomware Strikes: [Attack Playbook](#)

Essential ransomware protection strategies

Lock down your network

Your network perimeter is your perimeter fence. Leave the gate open, and attackers stroll right in.

- ✓ Use enterprise-grade firewalls with deep packet inspection.
- ✓ [Secure remote desktop protocol \(RDP\)](#)—a way to close your hacker's favorite open door.
- ✓ Enforce multi-factor authentication (MFA) for all remote access.
- ✓ Patch like your business depends on it. Because it does!
- ✓ Segment your network so an attacker in one area can't own the whole system.

Harden your endpoints

Every computer, server, and device is a potential entry point. Treat them like front doors to your digital fortress.

- ✓ Deploy next-gen antivirus with behavioral analysis (not just signature-based scans)
- ✓ Use application whitelisting. If it's not on the list, it doesn't run.
- ✓ Implement DNS filtering to block shady connections.
- ✓ Enable [Microsoft's Attack Surface Reduction rules](#).
- ✓ Consider [endpoint detection and response \(EDR\)](#) for rapid threat hunting.

When looking at how to protect your business from ransomware, endpoint protection should be a top priority.

Train your human firewall

Your employees are both your weakest link and your strongest defense.

- ✓ Run [phishing](#) simulations [to train them against](#) real-world threats.
- ✓ Create an open security culture. If something looks fishy, they should report it without fear of criticism or blowback.
- ✓ Give them clear security policies. Don't be vague or haphazard.

Protect backups from ransomware

Protect backups from ransomware

Attackers love destroying backups, so yours need to be untouchable. To protect backups from ransomware:

- ✓ Follow the 3-2-1 backup rule (3 copies, 2 different media types, 1 offline).
- ✓ Use immutable storage that attackers can't alter.
- ✓ Test your restores, because a backup that doesn't work is worthless.
- ✓ Keep backup credentials separate and locked down.

Detect threats early

If ransomware is a break-in, early detection is your silent alarm.

- ✓ Deploy [Huntress Ransomware Canaries](#), which are files that trigger alerts if encrypted.
- ✓ Monitor for unusual logins and network activity.
- ✓ Set up honeypots. Fake data lures can expose intruders.
- ✓ Use anomaly detection to catch attackers before they strike.

Prepare for the worst

When ransomware hits, every minute counts. To respond as quickly as possible, you should:

- ✓ Have a tested incident response plan.
- ✓ Define roles and responsibilities.
- ✓ Pre-write communication templates.
- ✓ Establish contacts with law enforcement and legal teams.
- ✓ Know your stance on ransom payments before you're forced to decide.

People also ask

What is the best protection against ransomware?

The best protection combines multiple defensive layers: robust endpoint security, regularly tested backups, user training, network segmentation, and early detection, like ransomware canaries.

How can ransomware be prevented?

Stopping ransomware means making attackers work harder than they're willing to. Patch everything, lock down email, train your team to spot threats, secure remote access, deploy endpoint protection, and build backup systems that attackers can't reach. The harder you make it, the quicker they move on to an easier target.

How do I enable ransomware protection?

Start with the basics. Built-in ransomware protection is a good first line of defense. Then go pro by deploying serious endpoint security, whitelisting only trusted apps, locking down backups, and bringing in heavy-hitting detection like Huntress Ransomware Canaries.

Layered security will make you a hard target.

No magic bullet will take out ransomware, but layered security is the best defense.

- ✓ Think like an attacker. Anticipate their moves.

- ✓ Think like an attacker. Anticipate their moves.
- ✓ Build resilience with strong backups, detection, and response plans.
- ✓ Stay paranoid. In cybersecurity, paranoia is just another word for preparedness.

Protect your business before ransomware comes knocking. Because when it does, you won't have time to wish that you had.

To learn more, [book yourself a demo](#) with Huntress.



Brenda Buckman

[Read More >](#)

[Continue Reading](#)

Ransomware Attacks on Businesses Statistics >

Protect What Matters

Secure endpoints, email, and employees with the power of our 24/7 SOC. Try Huntress for free and deploy in minutes to start fighting threats.

[Try Huntress for Free](#)



Platform

Huntress Managed Security Platform
Managed EDR
Managed EDR for macOS
Managed ITDR
Managed SIEM
Managed Security Awareness Training
Book A Demo

Solutions

Phishing
Compliance
Business Email Compromise
Education
Finance
Healthcare
Manufacturing
State & Local Government

Why Huntress?

Managed Service Providers
Value Added Resellers
Business & IT Teams
24/7 SOC
Case Studies

Resources

Resource Center
Blog
Upcoming Events
Support Documentation

About

Our Company
Leadership
News & Press
Careers
Contact Us

