threat level: human

The attack vector you can't patch.

Ransomware Basics for Small Business

How ransomware gets in, and the three controls that stop or survive most of it.

48%
of breaches involved ransomware in 2025
Verizon DBIR, 2026

$1.53M
average ransomware recovery cost
Sophos, 2025

62%
of breaches involve the human element
Verizon DBIR, 2026

HOW IT GETS IN

01 Phishing and malicious attachments
One staff click on a lure is a leading way ransomware lands.

02 Exposed remote access
Open RDP or VPN with weak or reused credentials and no MFA.

03 Unpatched, internet-facing systems
Known vulnerabilities left open long after a fix exists.

LIMIT THE DAMAGE BEFORE IT HAPPENS

04 Tested, offline backups
Backups that are offline or immutable, and that you have actually restored.

05 MFA on every remote login
Multi-factor on email, VPN, and admin accounts closes the easy door.

06 A plan you have rehearsed
Know who to call and how to isolate systems before the day you need it.

EARLY WARNING SIGNS

07 Security tools disabled or alerting
Antivirus turned off, mass file changes, or odd admin logins.

08 New accounts or tools appearing
Unexpected admin accounts, remote-access tools, or scheduled tasks.

09 Files renamed or unreadable
Documents with strange extensions and a ransom note dropped in folders.

DO / DON'T

DO

- Keep offline or immutable backups, and test a real restore.
- Put MFA on email, VPN, and every admin account.
- Patch internet-facing systems quickly and close unused remote access.
- Segment the network and limit admin rights to who truly needs them.
- Write and rehearse an incident plan with named contacts.

DON'T

- Do not expose RDP or VPN without MFA.
- Do not run day-to-day on accounts that have admin rights.
- Do not pay the ransom before contacting law enforcement. Payment guarantees nothing.
- Do not wipe systems before preserving evidence for investigators.

THE ONE MOVE

Keep offline, tested backups, put MFA on every remote and admin login, and patch internet-facing systems fast. Those three controls stop or survive most ransomware. Report incidents to CISA and the FBI.

IF IT HAPPENS

1. Isolate affected systems: disconnect from the network, but do not power down yet.
2. Activate your incident plan and contact your IT team or a response firm.
3. Report to CISA (cisa.gov) and the FBI at ic3.gov.
4. Restore from clean, offline backups only after the cause is found and closed.

Get a briefing like this every week, free.
threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: Verizon DBIR (2026); Sophos State of Ransomware (2025); CISA. Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.