What is malware?

Malware is any software written to cause harm: viruses, worms, trojans, spyware, and ransomware. It usually arrives through a phishing attachment, a malicious download, or an unpatched internet-facing system. Ransomware is the most disruptive variant, encrypting your data and demanding payment, and modern operators steal a copy first to add extortion. The defenses are patching, endpoint detection, least privilege, and tested backups.

HOW IT WORKS

01 The main types of malware

Malware is a family, not a single thing:

- Viruses attach to files and spread when those files run.
- Worms spread on their own across a network, with no user action.
- Trojans disguise themselves as something useful to get you to run them.
- Ransomware encrypts your data and demands payment.
- Spyware and infostealers quietly harvest passwords, cookies, and data.
- Rootkits hide deep in the system to evade detection.
- Loaders and botnets turn an infected machine into a foothold or a resource the attacker rents out.

02 Ransomware and double extortion

Ransomware encrypts your files and demands payment for the key. Modern operators go further with double extortion: they steal a copy of the data first, so even if you restore from backup, they can threaten to publish it.

For most organisations, a ransomware incident is not an exotic exploit. It is the basics failing in sequence: a phished credential or unpatched service to get in, no multi-factor authentication to slow them, over-broad access to spread, and backups that were never tested to recover. Fix those and ransomware becomes a bad day rather than a business-ending one.

HOW TO DEFEND

- Patch operating systems, software, and internet-facing services promptly.
- Run endpoint protection (EDR) that detects malicious behaviour, not just known signatures.
- Enforce least privilege so one infected machine cannot reach everything.
- Filter email and block risky macros and attachments at the gateway.
- Keep tested, offline-capable backups as your ransomware safety net.
- Segment your network so malware cannot spread freely.

SOURCES

[1] StopRansomware

[2] Malware, Phishing, and Ransomware

[3] MITRE ATT&CK

> PAYING RARELY ENDS IT
>
> *Authorities advise against paying: there is no guarantee you get your data back, it funds more attacks, and you may be hit again. Tested backups and an incident plan are the real leverage.*

03 Signs of a malware infection

Malware is not always obvious, but common signs include machines running slow or behaving oddly, unexpected outbound network traffic, security tools being disabled, new accounts or scheduled tasks you did not create, and, in the case of ransomware, files renamed or encrypted with a ransom note. The reliable way to catch what these miss is endpoint detection and response feeding alerts to someone who acts on them.

Find out whether one infected machine could take down the rest.

securelayer7.net/learn/threats/malware

Open online