

The 5-minute ransomware guide

What is ransomware?

Ransomware is a type of malicious software that allows a hacker to restrict access to an individual's or company's vital information and demand payment (usually cryptocurrency) to lift the restriction.



In 2016, the FBI projected ransomware could lead to **\$1B** in global losses.¹

In 2019, total ransomware damage was **\$11.5B** at an average of **\$141,000** per incident.²

By 2021, experts expect **\$20B** of total losses due to ransomware.³



Time from initial infection to ransomware demand:



Advanced persistent threat (APT) attacks have delayed timelines, with attackers attempting to infect as many systems in a network as possible.

Damages due to lost productivity are usually

5-10x

the actual ransom amount.⁴



Publishing sensitive data or "dirty secrets" online and giving away information to competitors are increasingly common tactics.

A 2019 report found that following a ransomware attack, the average organisation lost:⁴



9.6 days
of productivity



8% of data

How ransomware is affecting UK organisations

48%

of UK organisations hit by ransomware in the last year.⁵

5.9 Million

ransomware attacks recorded in the UK in the first half of 2020.⁶

\$840,000

The average remediation cost of a successful ransomware attack to UK enterprises.⁶



Today, almost anyone can contact a **Ransomware-as-a-Service (RaaS)** group to launch an attack.



\$1.14M

Amount paid by University of California San Francisco to recover research files after a ransomware infection in June 2020.⁷

The projected frequency of global ransomware attacks by 2021 is every²

11 seconds

Negotiations took place on the Dark Web, with an initial ransom request of ⁷

\$3M



Now that you understand how ransomware typically works, learn how you can defend your organisation against an attack.

[Learn more](#)