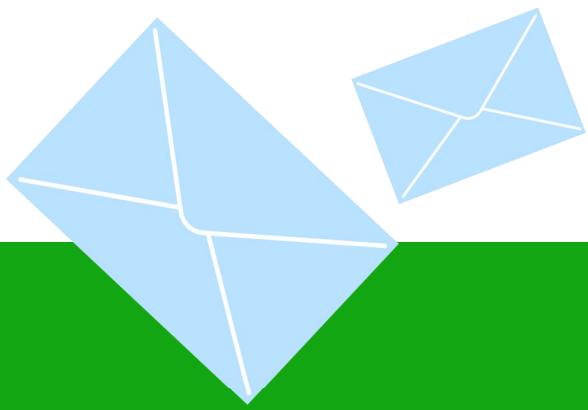


4 Most Common Cyberthreats



Threat actors *“fish”* for someone who will make a mistake ...



and they often get a bite.

Did you know...

Over
80%

of data breaches are caused by **employee mistakes**

The Big 4 Threats

MALWARE



WHAT IT IS

A broad term covering many types of malicious software installed on devices

HOW IT WORKS

Threat actors try to install malware on an endpoint (laptop, desktop, mobile phone)

END GOAL

To harm, extort, or scare



PHISHING

WHAT IT IS

A form of social engineering

HOW IT WORKS

Threat actors pose as a trusted source and trick users into compromising their account, device or network

END GOAL

To exploit information for financial gain



RANSOMWARE

WHAT IT IS

A form of malware

HOW IT WORKS

By encrypting, or otherwise locking down, the contents of a device to block access to the user

END GOAL

To harm, extort, or scare



DATA BREACH

WHAT IT IS

Digital data theft

HOW IT WORKS

Threat actors (external or internal) enter an organisation's corporate systems and remove data without permission

END GOAL

To exploit information for financial gain, enjoy recognition, damage reputation



560,000

new pieces of malware are detected every day.

– Statista



Nearly
88%

of IT leaders believe their organisations lack sufficient protection against cyberattacks.

– Foundry's 2023 Security Priorities

We understand technology can be overwhelming.

Partner with a managed service provider who specialises in cybersecurity technology.

Contact us today!