04 Most Common Cyberthreats

Threat actors “fish” for someone who will make a mistake... and they often get a bite.

Did you know...

85%

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

The Big 4 Threats

1 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

2 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

3 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

4 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

Nearly

80%

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

-IDG Research Services

560,000

new pieces of malware are detected everyday.

AV-TEST

We understand technology can be overwhelming.

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

Contact us today

Security@trustsystems.co.uk