



What is a Cyber Attack?

A cyber attack is a deliberate attempt by a criminal, organised crime group, or hostile state actor to gain unauthorised access to computers, devices, networks, or data, or to disrupt, damage, steal, manipulate, or destroy information and services.

Simple Definition

A cyber attack is like a digital break-in, theft, or act of vandalism carried out with the help of computers, mobile devices, and the internet instead of physical tools.

Common Types of Cyber Attacks:

Phishing

Criminals send fake emails, text messages, social media messages, or create fraudulent websites that appear legitimate in order to trick people into revealing passwords, bank details, personal information, or security codes.

Example: An email claiming to be from Microsoft asking you to "verify your account" by clicking a link.

Ransomware

Malicious software (malware) that locks or encrypts files and demands payment for their release.

Example: A user opens a malicious attachment and suddenly loses access to their files, with a message demanding payment.

Malware

Software specifically designed to damage systems, steal information, spy on users, or gain unauthorised access to devices.

Examples include:

- Viruses
- Worms
- Trojans
- Spyware
- Keyloggers

Password Attacks

Criminals attempt to guess, steal, buy, or crack passwords in order to gain access to accounts and systems.

Denial-of-Service (DoS/DDoS)

Attackers overwhelm a website or online service with huge volumes of traffic, causing it to become slow or unavailable to legitimate users.

Social Engineering

The manipulation of people into carrying out actions or revealing confidential information.

Example: A caller claiming to be from IT support, a bank, the police, or another trusted organisation asking for passwords, security codes, or payment.

Typical Cyber Attack Objectives

Cyber criminals may seek to:

- Steal money
- Steal personal or business data
- Commit identity theft
- Disrupt services or operations
- Spy on organisations or governments
- Damage reputations

- Gain a competitive or political advantage
- Extort money from victims

Signs of a Cyber Attack:

Warning signs can include:

- Unexpected password reset notifications
- Unusual account activity or login alerts
- Slow, unstable, or unresponsive devices
- Pop-up messages demanding payment
- Antivirus or security alerts
- New or unknown software appearing on devices
- Suspicious emails, text messages, or links
- Friends or colleagues receiving unexpected messages from your account

How to Protect Yourself:

- ✓ Use strong, unique passwords for every account
- ✓ Enable Multi-Factor Authentication (MFA) wherever possible
- ✓ Keep devices, apps, and software updated
- ✓ Be cautious of unexpected emails, text messages, links, and attachments
- ✓ Regularly back up important data
- ✓ Use reputable antivirus and security software
- ✓ Never share passwords or security codes
- ✓ Verify payment requests and changes to bank details using a trusted contact method
- ✓ Stop, think, and check before taking action on unexpected requests

Example

An employee receives an email that appears to come from their manager requesting an urgent payment to a supplier. The email is actually from a criminal impersonating the manager.

This is a cyber attack involving both **phishing** and **social engineering**.

In Summary

A cyber attack is any deliberate attempt to compromise the **confidentiality, integrity, or availability** of digital systems, networks, or data. Cyber attacks can target individuals, businesses, charities, schools, and governments, and they represent one of the most significant security threats in today's digital world.

What to do if you are the victim of a Cyber Attack

Report it immediately: Visit - [UK's Home for Reporting Cyber Crime & Fraud - Report Fraud](#) or call **0300 123 2040**

If you have shared financial details, or lost money also contact your bank's fraud team by calling **159**

Please help protect others

If you found this information useful, please share it with your family, friends, neighbours, colleagues, and community groups. Greater awareness helps prevent people from becoming victims of cyber crime and fraud.

Remember: Stop • Think • Check before you click, call, or pay.