What is Cybercrime and Cyber-Enabled Crime?

Cybercrime is an illegal act that is committed on the internet or using a digital device such as a computer or smartphone.

The internet or these devices can be used as a tool to commit the crime, be the target of the crime, or the place where the crime occurs. Common examples are **hacking** and **ransomware attacks.**

IN ENGLAND AND WALES

58%

OF ALL CRIME IS CYBER-ENABLED CRIME.

*The Cyber Helpline report 2024

Cyber-enabled crime refers to crimes that are made easier or more widespread through the use of the internet or digital devices.

These can include digital frauds such as **investment scams** and **identity theft**, as well as online harms such as **online harassment** and **cyberstalking**.

Where to get help if you are a victim of cybercrime

The Cyber Helpline

The Cyber Helpline offers free, expert support for victims of cybercrime, digital fraud and online harm. They can provide guidance on securing your accounts and devices, and preventing it from happening again.

www.thecyberhelpline.com

Citizens Advice

Citizens Advice Consumer Service can offer support if you or someone you know has been scammed. They will give you advice on what to do next.

www.citizensadvice.org.uk

Age UK

Age UK provides free tailored support to scam victims over 50 including one-on-one advice, a national advice line, specialised casework to help with recovery, and prevention education including free guides.

www.ageuk.org.uk

Friends Against Scams

Scam awareness and prevention for individuals, communities and professionals.

www.friendsagainstscams.org.uk

Friends Against SCAMS

Cybercrime Guide



The Cyber Helpline
Supporting victims of cybercrime

Friends Against SCAMS

NATIONAL TRADING STANDARDS
Scams Team

What are the different types of cybercrime?

Fraud & Scams

Criminals use scam emails (phishing), texts (smishing), and calls (vishing) that impersonate trusted organisations to steal money or personal information.

Other common scams include romance fraud (catfishing), sextortion, investment and cryptocurrency fraud, online shopping and card fraud, loan, or recruitment schemes.

Malware & Device-Based Attacks

Malware is designed to damage devices, steal data, or gain unauthorised access. This includes ransomware, which locks files or devices and demands payment, and the covert use of bugs, cameras, or trackers to monitor a person's activities, communications, or location without consent.

Data & Privacy Violations

Data and privacy violations occur when personal or sensitive information is exposed without consent. This may result from data breaches, organisational errors, accidental sharing, or deliberate acts such as doxxing.

Online Harassment & Abuse

Online harassment and abuse involve using digital platforms to intimidate, exploit, or harm others. This includes cyberstalking, cyberbullying, intimate image abuse, fake profiles, exposure to harmful content, and online grooming of children.

Account & Identity-Based Crimes

These crimes involve unauthorised access (hacking) to accounts or personal information for fraudulent or malicious purposes.

Common Enablers of Cybercrime

Cybercriminals often exploit common vulnerabilities and human behaviour. Weak account security, outdated software, and clicking unverified links can provide attackers with easy access to devices and accounts.

Oversharing on social media, trusting strangers, and responding to unexpected communications can expose personal information. Urgency, fear, greed, and emotional manipulation are frequently used to pressure victims.

What to do if you have been targeted by cybercriminals



Stop: do not send further money, data, or access.



Secure: change passwords and enable 2 factor authentication (2FA) on affected accounts.



Bank: contact your bank immediately if money has been stolen or is at risk.



Report: report to Report Fraud.



Support: reach out for help; you are not alone and it is not your fault.

England & Wales
Report: contact **Report Fraud** on **0300 123 2040**
Advice: contact **Citizens Advice** on **0808 223 1133**

Scotland
Report: call **Police Scotland** on **101**
Advice: contact **Advice Direct** on **0808 164 6000**

Northern Ireland
Report: contact **Report Fraud** on **0300 123 2040**
Advice: contact **Consumerline** on **0300 123 6262**