CYBERCRIME FACT SHEET

Created in partnership by The Cyber Helpline & Friends Against Scams (National Trading Standards)

What is Cybercrime & 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.

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 fraud such as investment scams and identity theft, as well as online harms such as online harassment and cyberstalking.

Cybercrime and cyber-enabled crime are a widespread and growing issue, with 58% of all crime in England and Wales being online or cyber-enabled, and over 5 million victims impacted in 2025.

Who is at Risk?

- Anyone can be a victim. Cybercrime does not discriminate by age, background, or technical ability.
- Certain groups are more likely to be targeted, such as older adults and people facing emotional or financial challenges.
- Victims are often targeted because of sophisticated and convincing tactics, not because of naivety.
- Fear of stigma can heighten vulnerability, as victims may postpone seeking support or reporting incidents.

Types of Cybercrime & Subcategories

Fraud & Scams
• **Scam Emails** | Also known as *Phishing*: Fake emails designed to look like they're from a trusted organisation, such as a bank or government agency, with the goal of coercing victims into revealing personal information or clicking a malicious link. • **Scam Texts** | Also known as *Smishing*: The same as phishing, but carried out through text message (SMS) instead of email. • **Scam Calls** | Also known as *Vishing*: Voice calls impersonating trusted organisations, such as banks, HMRC, police, or technical support, to manipulate victims into handing over personal details or money. • **Romance Fraud** | Also known as *Catfishing:* Fraud where an offender creates a fake identity online to build a romantic relationship and manipulate victims into sending money or gifts over time. • **Extortion or Blackmail Using Intimate Images** | Also known as *Sextortion:* A form of blackmail where offenders obtain or fabricate intimate images or videos of a victim and threaten to share them unless money or further content is provided. • **Investment and Cryptocurrency Fraud**: Fraud involving fake platforms or schemes to coerce victims into handing over money in the belief they are making an investment. • **Online Shopping Fraud:** Fake listings or websites that mislead people about a product or service. Payment and personal details are taken, but nothing is delivered. • **Online Card Fraud:** Unauthorised use of card details to make fraudulent purchases online. • **Recruitment Fraud:** Fake job adverts or opportunities used to extract money or personal data from jobseekers. • **Loan Fraud:** Fake loan offers used to extract upfront fees from victims seeking credit.
Malware & Device-Based Attacks
• **Malware:** Malicious software designed to damage devices, steal data, or gain unauthorised access to systems. • **Ransomware**: Malicious software that locks files or devices and demands payment for their release. • **Bugs, cameras, and trackers**: The covert installation of listening devices, cameras, or location trackers on someone's devices or property without their consent.

Account & Identity-Based Crimes
• **Account Takeover** | Also known as *Hacked Account*: Unauthorised access is gained to online accounts such as email, banking, social media, or gaming accounts. • **Identity Theft**: Personal information (such as names, bank details, or passwords) is stolen to open accounts or make fraudulent purchases. • **SIM Swapping**: Control of a mobile SIM account is gained and ownership (and the telephone number) is transferred to an attacker-controlled SIM. • **Fraping**: When someone's social media account is accessed without their permission and content is posted that causes them distress or reputational damage.
Online Harassment & Abuse
• **Cyberstalking:** Persistent online surveillance, monitoring, or unwanted contact intended to cause fear or distress. • **Online Harassment** | Also known as *Cyberbullying:* Repeated abusive, threatening, or intimidating behaviour directed at an individual online. • **Intimate Image Abuse** | Also known as *Revenge Porn*: Sharing or threatening to share intimate images without the victim's consent. • **Fake Profiles:** Creating false online identities to harass, impersonate, or cause distress to another person. • **Inappropriate Content:** Exposure to hate speech, extremist material, or harmful content online, including content targeting children or vulnerable users. • **Online Grooming:** An adult building a relationship of trust with a minor online for the purpose of exploitation or abuse *(if you are concerned about a child, contact the police or CEOP immediately at ceop.police.uk)*
Data & Privacy Violations
• **Data Breach:** When a company or service provider is hacked or makes a mistake that exposes users' personal data to cybercriminals or the public. • **Unauthorised exposure of personal or sensitive data:** The unauthorised disclosure of personal or sensitive information, resulting in the loss of control over private data and potential harm to the individual. This may include accidental sharing (e.g. publicly posting private content), or intentional disclosures such as outing and doxxing.

Common Enablers of Cybercrime

1	**Poor account security**: Weak or reused passwords and no two-factor authentication make it easier for attackers to gain control of accounts.
2	**Outdated software and devices:** Unpatched vulnerabilities leave systems open to exploitation.
3	**Clicking unverified links:** Primary entry point for phishing and malware**.**
4	**Oversharing on social media**: Provides attackers with personal details to target victims. Private information can be leveraged for exploitation or blackmail.
5	**Unexpected communications**: Messages that catch individuals off guard can prompt hasty decisions.
6	**Urgency and emotional manipulation**: Attackers deliberately create fear, love, or greed triggers to pressure victims into quick decisions.
7	**Trusting strangers**: Believing strangers too easily opens the door to social engineering (psychologically manipulating someone into revealing access credentials or sensitive information).
8	**Relationships**: Criminals exploit emotions and personal connections to manipulate and deceive.
9	**Investments**: The promise of quick money is used to exploit victims.
10	**Lack of awareness**: Not recognising what cybercrime looks like increases vulnerability.

What to Do If You've Been Targeted

1. **Stop** — do not send further money, data, or access.
2. **Secure** — change passwords and enable 2FA on affected accounts.
3. **Bank** — contact your bank immediately if money has been stolen or is at risk.
4. **Report** — report to Report Fraud.
5. **Support** — reach out for help; you are not alone and it is not your fault.

Please be aware: If you have been a victim of cybercrime or fraud, you may be targeted again by individuals or companies claiming they can recover your lost funds, often for an upfront fee. This is known as recovery fraud and is itself a scam. No legitimate organisation will guarantee the recovery of lost funds or charge you a fee to do so. If you are approached in this way, do not pay and report it to Report Fraud.

How to Report

1. **Report Fraud** — 0300 123 2040 | reportfraud.police.uk/reporting-a-fraud/
2. **Your bank or payment provider** — as soon as possible if money is involved.
3. **The platform** where the crime occurred (social media, marketplace, email provider).

Where to Get Help

- **The Cyber Helpline** — thecyberhelpline.com — Cybercrime, digital fraud and online harms victim support, for individuals and sole traders aged 13+.
- **Friends Against Scams** — friendsagainstscams.org.uk — Scam awareness and prevention for individuals, communities and professionals.
- **Citizens Advice** — citizensadvice.org.uk — General advice including scams and fraud, available to anyone in the UK, free and confidential.
- **Age UK** — ageuk.org.uk — Scam awareness, prevention and victim support for people aged 50+ and those who support them.

Supporting Someone Else

- Approach without blame — victims are often embarrassed or ashamed.
- Listen first; avoid saying "I told you so" or questioning their judgment.
- Help them take the practical steps listed above.
- Signpost them to The Cyber Helpline or Friends Against Scams for further support.
- Friends Against Scams runs the SCAMchampion programme, which trains individuals to help protect others in their communities. Consider joining the programme to help safeguard people in your community.