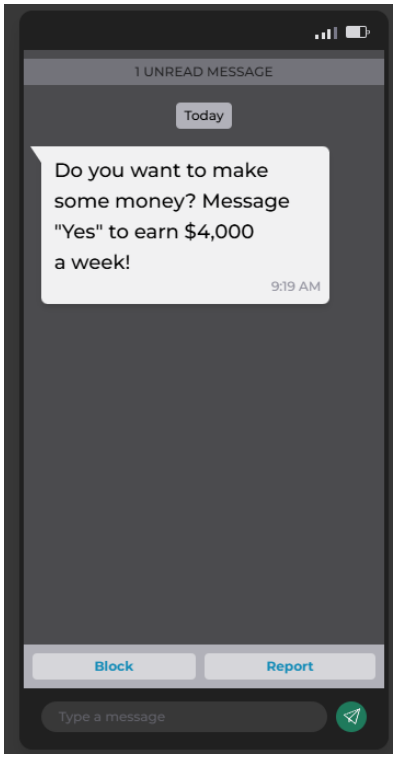
Scam messages and how to deal with them

By early 2025, approximately 95% of UK residents aged 16 and over owned a smartphone. That is around 53 million people in the UK. Presently, some 67.8 million individuals in the UK are using the internet, which accounts for 97.8% of the population. This translates to about 54.8 million social media users, indicating a strong digital presence in the country.

Inevitably the access the internet and telecommunications has drawn the interest of criminals who seek to exploit the unwary users of the media. The Global Anti-Scam Alliance's latest report, *The State of Scams in the UK* – conducted in association with UK's leading fraud prevention service, Cifas (Credit Industry Fraud Avoidance System) – has revealed UK people lost £11.4 billion to scams in the last 12 months, up £4 billion on last year. (Datareportal)

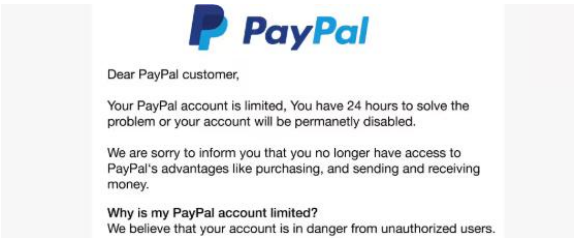


Nearly three-quarters of respondents to Cifas said they could confidently recognise if an offer seemed too good to be true. These approaches are often called "phishing". Despite the increased awareness, 61% of people revealed they encounter scams at least once a month – in particular, through rogue delivery text/SMS messages, and shopping and investment scams via online platforms such as Gmail, WhatsApp, and Facebook.

In addition to the financial harm caused by a scam, over half of the victims felt a strong emotional response. However, the majority (71%) still did not report the crime – suggesting they may have been ashamed to do so, blamed themselves, or lacked the confidence that their complaint would be dealt with. In total, 3 in 5 respondents (60%), said their trust online had declined because of scams.

The research at Ofcom also revealed that almost eight in every ten mobile phone users are not aware of the 7726 number used to report a suspected text or call – although a similar figure number agreed that reporting messages is helpful in preventing people being scammed in the future.

A typical scam email - right


PayPal

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

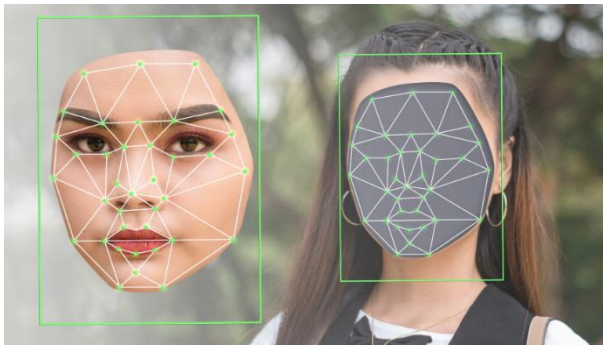
We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?
We believe that your account is in danger from unauthorized users.

Despite increasing awareness, the criminal industry continues to grow. It not only affects the people who are the targets of the attempts to manipulate and extort money but also the unwitting citizens of poor counties, who are lured into working for the scammers with false promises of other employment opportunities. Many scammers from mainland China are what Chinese authorities refer to as "san di" ("three lows"), meaning they have low income, education and age. Victims often begin their new "jobs" with a massive debt for flights, visas, permits and broker or trafficker fees.

Once trapped in their web on deceit they may face physical restraint and coercion to work for many hours a day in secret call centres, trying to earn enough money to escape or simply survive. In many compounds, the scammers work long shifts, sometimes as many as 17 hours a day. Any refusal to cooperate can result in severe treatment by the criminal gangs, including assaults and sexual trafficking. Experts estimate there are hundreds of thousands of scammers in the industry across Southeast Asia. Some of the gang leaders are unrepentant criminals, ruthlessly exploiting victims across the world.

If the human misery around text and email scams was not enough, The rise of generative artificial intelligence has significantly increased the scale and sophistication of cybercrime, particularly identity theft and fraud. Global cybercrime is expected to cost $10.5 trillion annually by 2025, up from $3 trillion in 2015, according to Cybersecurity Ventures. To put it in perspective, if annual cybercrime were a country, it would have the third-largest gross domestic product (GDP) worldwide.



AI-driven deepfake technology allows criminals to impersonate individuals' appearances with deceptive accuracy, potentially bypassing verification systems and gaining access to sensitive resources. Gone are the days of the “Nigerian Prince” email scams. Generative AI has enabled scammers to create more convincing phishing communications.

The Online Safety Act, which was passed in October 2023 by the UK government, requires service providers, including social media firms, search engines, messaging, gaming and dating apps and pornography and file-sharing sites, to remove any harmful content deemed illegal from their platforms. However, the Act does not explicitly mention phishing as a target for prevention.

Taking down illegal and fraudulent websites is a time consuming task for legitimate companies. Our law enforcement agencies are far less effective at takedown than commercial firms, who get an awful lot more practice. However, firms with a poorer understanding of computer security and technical matters are more likely to have their websites compromised in the first place, and less likely to be able to rectify the problems quickly.

For the present, we can only help to protect ourselves by being cautious when providing our information online and double-checking websites to ensure they are secure and reputable before entering any sensitive information.

Limit the information we share on social media. Scammers need to build a false identities and anything that supports their creation, is a boon to them. Although it may seem tedious, review the privacy policies of websites and applications before using them, to understand how your data is being collected, stored, and used. Use strong, unique passwords for each online account to make it harder for hackers to access your information.

Ultimately the degree of online fraud will only decrease if there is growing awareness and activity to defend ourselves. The scammers attempt to contact millions of people very hour of the day and it only needs a small number to respond positively to make it worth their effort.

New figures shared by Action Fraud have revealed an increase in the number of scams being reported. The Suspicious Email Reporting Service, which is when you forward scam emails to report@phishing.gov.uk, reached its highest level of reporting in May since its launch in 2020. Reports have led to the removal of 329,000 scam websites by the National Cyber Security Centre.

The reporting of scam text messages to 7726, the free service offered by mobile network providers, has also increased and led to more than 60,000 malicious websites being removed in March 2024.

Digital 2025: The United Kingdom — DataReportal – Global Digital Insights
Scammers stole £11.4 billion from UK people in last 12 months | Cifas
45 million people targeted by scam calls and texts this summer
AI-driven cybercrime is growing, here's how to stop it | World Economic Forum