OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

Online Scammers Target Londoners More Than Any Other Region, Research Shows

July 31, 2025

- Categories: Crime



Tech giants Meta and Microsoft join forces in a major international anti-fraud effort as London residents are now the most targeted group in the UK when it comes to online and text-based scams, according to new figures from the Global Signal Exchange (GSE), an international fraud prevention alliance.

The research found that 78% of people living in the capital have received scam-related emails or text messages, compared with a national average of 71%. Nearly a quarter of

those surveyed said the fraudulent messages they received included a brand name they already knew, increasing the chances they would trust and interact with the scam.

The GSE, which describes itself as a cross-sector platform for sharing threat signals, released the data alongside news that Meta and Microsoft are officially joining its growing list of partners. The two tech firms join over 30 other major players in the global battle against digital fraud and cybercrime.

Rising Scam Tactics

The research highlighted several types of scams that are particularly prevalent among Londoners. These include delivery-related fraud (21%), online payment issues (19%), banking scams (18%), fake prize or lottery wins (18%), job offer scams (18%), bogus fines (18%), HM Revenue and Customs (HMRC) payment fraud (17%), romance scams (15%), cryptocurrency cons (15%), fake charity appeals (15%), investment scams (14%), and ancestry frauds (11%).

These scam types often rely on impersonating well-known companies or institutions to convince recipients to hand over personal or financial information. The GSE noted that many individuals are more likely to believe a message is real if it appears to come from a brand they trust.

Founded in 2024 by Oxford Information Labs Research (OXIL), Google, and the Global Anti-Scam Alliance (GASA), the GSE serves as a central hub for data-sharing and collaboration across different sectors. Its goal is to quickly identify and block online scams before they spread and cause financial harm.

The alliance now holds over 320 million threat signals from 32 different data providers, including Google, Spamhaus, and Abusix. This expanded pool of information allows partners to act faster and more effectively when dealing with malicious actors.

Microsoft's Director of Outreach and Governance for Central Fraud and Abuse Risk Chris Compton, said the company is "proud to join the Global Signal Exchange, a network we see as pivotal in the global effort to combat online scams and abuse." He added, "We believe that collaboration across sectors and borders is critical to disrupting malicious activity. GSE will enhance our ability to work together with our fellow members to stop bad actors

worldwide. Joining the Exchange marks an important step in Microsoft's continued commitment to the safety of users everywhere."

Meta's Global Head of Counter Fraud, Nathaniel Gleicher, echoed that view, warning of the growing sophistication of online crime. "Online scams are driven by ruthless cross-border criminal networks that use sophisticated schemes to abuse a wide range of platforms and target people across society," he said. "We need platforms, banks, governments, law enforcement, domain name systems, and telecoms to work together to stop these actors, and we're committed to doing our part."

Gleicher added that Meta is testing new technologies, including facial recognition tools, to strengthen its anti-scam defences, and is also providing users with warnings and educational material to help them recognise and avoid common fraud tactics.

Emily Taylor, co-founder of the Global Signal Exchange, said younger people are being hit particularly hard by scam attempts, with one reporting as many as 240 scam messages in a single day. She said the GSE's next step is to build stronger ties with law enforcement and government bodies to take the initiative further.

"We warmly welcome Microsoft and Meta to the Global Signal Exchange, and we are excited by the significant contribution they will make in helping us all to change the narrative on crime, fraud, and abuse," she said. "The level of global support for the Global Signal Exchange signifies a step-change in the fight against online crime, as we facilitate a new culture of co-operation and data sharing."

Taylor stressed that online criminals often coordinate and share information at speed, meaning isolated efforts by individual companies are no longer enough. "Scammers work together, they share, and they move quickly, which means the days are long-gone when individual brands can tackle online crime alone. The Global Signal Exchange marks a new chapter in the collective fight-back against online crime."

Figures from the Global Anti-Scam Alliance's 2024 Global State of Scams Report place the annual cost of online scams at over \$1 trillion globally. Yet despite the rising toll, the World Economic Forum estimates that only 0.05% of cybercrime cases worldwide ever lead to prosecution.