UK Spam & Social Engineering Weekly Threat Briefing

Week Commencing: 04 June 2026

Prepared for: Ibby Ahmed

Intelligence Sources: OnionClaw (Dark Web) | BioCatch | Which?

This briefing combines intelligence from 10 dark web search engines (routed through Tor), clearnet threat intelligence sources, and official UK fraud data. It is intended for situational awareness and personal security purposes.

CLASSIFICATION: CONFIDENTIAL — For recipient only

1. Executive Summary

Social engineering fraud in the UK has reached record levels in 2025-2026, with a 62% year-on-year increase in attempted attacks. Fraudsters are pivoting away from technical hacking toward psychological manipulation, exploiting human behaviour rather than system vulnerabilities. The widespread adoption of generative AI has dramatically improved the quality and believability of phishing, voice cloning, and deepfake attacks, making them significantly harder for the general public to identify.

This briefing covers the most active threats affecting UK consumers this week, with actionable awareness tips and reporting guidance.

2. Key Statistics (BioCatch Report — April 2026)

Source: BioCatch 2026 Digital Banking Fraud Trends in the UK. Data from 9 UK financial institutions covering 100M+ accounts.

+62% YoY Social Engineering Scams	**+140%** Phishing Attacks
+112% Stolen Device Fraud	**+16%** Mule Accounts

Fraud Type Breakdown (2025 YoY Increases)

- Purchase scams: +63% — largest increase across all fraud categories
- Investment scams: +34% — driven by crypto and pig-butchering schemes
- Romance scams: +47% — increasingly using AI voice cloning technology
- London: 70,000+ phones stolen in 2025 — used to bypass banking authentication
- Remote-access and malware-based fraud attempts: declining

3. Top 5 Active Threats — June 2026

These are the most prevalent scams targeting the UK general public right now, ranked by frequency and impact.

3.1 Purchase Scams (Marketplace / Social Media)

Fake listings on Gumtree, Facebook Marketplace, eBay, and Vinted. Fraudsters use AI-generated product photos and legitimate-looking profiles. You pay via bank transfer, item never arrives. Increasingly sophisticated with fake tracking numbers and accidental refund phishing follow-ups.

⚠ RED FLAG

Seller insists on bank transfer, refuses PayPal/Vipps. Price is suspiciously low. Profile was created recently with very limited activity.

3.2 Task Scams (Click Work / Micro-Tasks)

Victims recruited via text/SMS or social media ads to perform simple tasks: liking videos, writing reviews, rating apps. Initial small payments build trust. Victims then asked to pay a fee to unlock higher-paying tasks or tricked into installing remote-access software. Which? reports significant rise in 2025-2026.

⚠ **RED FLAG**

Any job offering £10-£50 for simple tasks like liking posts. Requests for upfront fees or membership payments.

3.3 AI-Powered Investment Scams (Crypto / Pig Butchering)

Deepfake videos of celebrities (Martin Lewis, Elon Musk, Deborah Meaden) endorsing fake crypto investment platforms. Victims added to WhatsApp/Telegram groups where most members are bots. The platform shows fictional profits to encourage larger deposits. When withdrawal is attempted, demands for taxes or fees are made. The platform then disappears entirely.

⚠ **RED FLAG**

Unsolicited investment offers via WhatsApp/Telegram. Celebrity endorsements without verified social media links.

3.4 Romance Scams with AI Voice Cloning

Fraudsters build relationships via dating apps or social media over weeks or months. They now use AI voice cloning to call victims, sounding exactly like their established persona. Common emergencies: hospital bills, stuck abroad, legal fees. BioCatch data shows 47% increase YoY.

⚠ **RED FLAG**

Never met in person. Always an emergency needing money. Refuses video calls (camera broken excuses).

3.5 HMRC / NHS / Council Impersonation

Calls and texts claiming to be from HMRC (tax owed/refund), NHS (appointment/prescription), or local council (council tax rebate, parking fines). Number spoofing makes caller ID show genuine numbers. Demand immediate payment via gift cards, bank transfer, or cryptocurrency. 140% increase in phishing overall.

⚠ **RED FLAG**

HMRC never demands payment via gift cards or Bitcoin. NHS does not send text links for appointments you did not book.

4. Dark Web Intelligence (OnionClaw)

The following intelligence was gathered via OnionClaw, routing through the Tor network across 10 dark web search engines. Dark web search engines are ephemeral, and several were unreachable at time of scan, which is normal for this environment.

4.1 AI-Powered Phishing Kits (UK-Focused)

- Multiple mentions of AI-powered phishing kits being sold on dark web forums targeting UK banks
- UK-specific templates for HSBC, Barclays, Lloyds, and Santander login pages available for purchase
- SMS spoofing services advertised, specifically for UK mobile providers (O2, EE, Vodafone, Three)

4.2 Stolen UK Credentials & Data Trading

- UK financial credentials and personal data (names, addresses, DOBs) actively traded on forums
- Stolen device data from London phone thefts used to bypass banking MFA
- Mule account recruitment advertisements: earn £500/week for sharing your bank account

4.3 Scam-as-a-Service Offerings

- AI voice cloning services: £50-£200 per cloned voice, targeting UK victims
- Deepfake video generation for fake celebrity endorsements
- Telegram/WhatsApp bulk messaging bots pre-configured for UK phone numbers

Note: Dark web search engines are unreliable and often go offline. DuckDuckGo via Tor is the most reliable for

clearnet intelligence. The OnionClaw crawler can be pointed at specific .onion forums for deeper investigation on request.

5. Weekly Awareness Tips

Share these with family and friends. These are the most effective defences against current threats.

This Week's Top 3 Tips

- STOP — If someone calls claiming to be your bank, HMRC, or the police asking you to move money or buy gift cards, hang up. Call them back on the official number from their website. Wait 5 minutes first to clear any line-holding scams.
- VERIFY — If a friend or family member calls asking for money urgently (especially via WhatsApp), call them back on their actual phone number. AI voice cloning is now cheap and convincing.
- BLOCK — Unsolicited investment offers on WhatsApp/Telegram. If it sounds too good to be true, it is. Legitimate investments do not recruit via group chats.

Quick Reference: How to Report

- Action Fraud (national reporting centre): 0300 123 2040 / actionfraud.police.uk
- Crimestoppers: 0800 555 111 (anonymous)
- Your bank: Call the number on the back of your card, not numbers from suspicious messages
- Phone theft: Report to local police via 101 or online
- Suspicious texts: Forward to 7726 (SPAM) — free on all UK networks

6. Sources & Further Reading

- BioCatch (2026) Digital Banking Fraud Trends in the UK
- Which? (2026) Scams expert on the scams that will be big in 2026
- IBS Intelligence (April 2026) UK banks see surge in fraud as scams shift to authorised payments
- Rest Less (2026) Latest scams to watch out for in 2026
- BioCatch data on UK social engineering scams — biometricupdate.com
- OnionClaw dark web search: Ahmia, Torch, OnionLand, Phobos, Candle, DuckDuckGo (via Tor)
- Action Fraud — actionfraud.police.uk
- National Cyber Security Centre (NCSC) — ncsc.gov.uk

This briefing was generated using the OnionClaw dark web intelligence toolkit (Tor-routed), web intelligence sources, and the FPDF2 library. Generated on 04 June 2026.