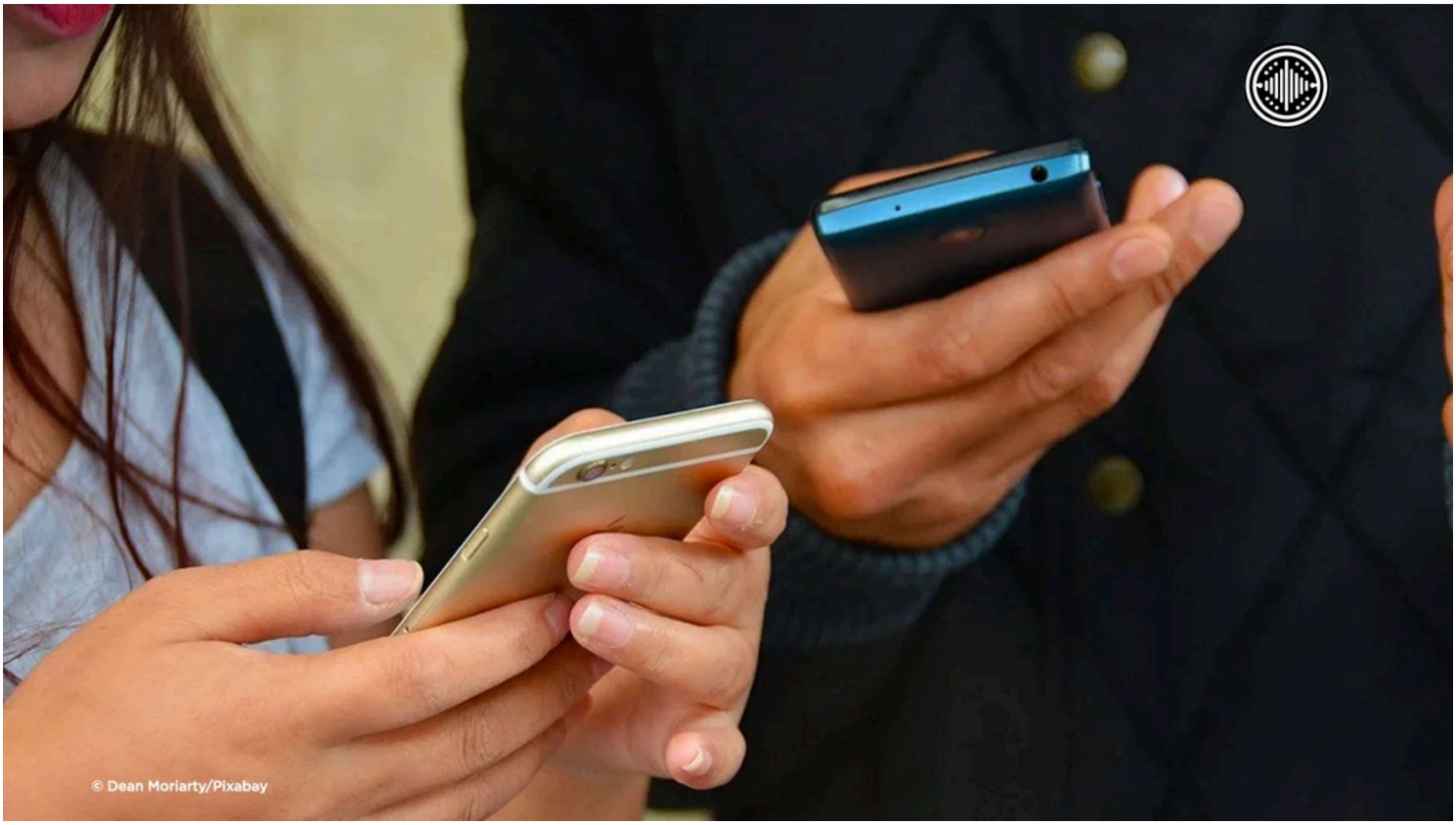
OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

Malicious Apps on the Rise as Criminals Exploit Mobile Users

July 29, 2025
— Categories: Crime



Mobile phone users are urged to exercise extreme caution when downloading apps, following a surge in sophisticated cyberattacks targeting banking details and personal data through seemingly innocent downloads, cybersecurity experts warn.

A growing wave of malicious Android apps is putting UK users at serious risk. Cybercriminals use deception to mimic everyday tools like file managers, phone cleaners, PDF readers, or even browsers like Google Chrome. Once downloaded, these rogue applications activate hidden malware to steal sensitive banking information.

Several leading organisations in the field of cybersecurity and financial fraud prevention, including the Cyber Defence Alliance (CDA), UK Finance, Cifas (Credit Industry Fraud Avoidance System), and ThreatFabric, have come together to raise public awareness. Their message is clear: think before you tap.

These malicious apps are not always obvious. In many cases, they appear to function normally at first. However, they may later prompt the user to grant excessive permissions, including access to the phone's accessibility settings, a red flag for potential malware. Users might also experience fake update requests, unresponsive banking apps, and fake overlays designed to mimic login screens of legitimate banking services.

The apps often deploy "busy" or "waiting" screens to obscure their true intent, while some even block attempts to exit the app or reboot the device. Experts warn that this level of manipulation shows how far cybercriminals have advanced in bypassing traditional security systems.

Han Sahin, Chief Executive Officer of ThreatFabric, said, "Just as we've learned to be cautious with links, we now need the same vigilance when installing apps. This is the logical next step in staying safe, and public awareness is crucial."

Garry Lilburn, Operations Director at the CDA, echoed that sentiment: "This crime highlights the growing prevalence and sophistication of mobile malware. As we work to better understand and disrupt this evolving threat, it's crucial that financial consumers stay vigilant, follow recommended security tips, and take a moment to verify what's in front of them, before becoming the next victim of this highly targeted fraud."

UK Finance is also warning that public complacency could lead to severe consequences. Dianne Doodnath, Principal of Economic Crime at UK Finance, said: "We encourage customers to stay alert to all threats of fraud, including the potential for criminals to trick people into downloading malware onto phones, which could put your personal and finance information at risk of theft. It's important that you keep your phone security system up-to-date and always download from trusted sources to ensure you're protected from the risk of fraud and data harvesting."

Mike Haley, Chief Executive Officer of Cifas, added: "The surge in Android malware is not just a tech issue, it's a growing threat to consumers and to banking services we all rely on. Criminals are evolving their tactics faster than ever, using deception and stealth to bypass

traditional security measures. The best defence is awareness. If something feels off, an unexpected update, or a strange app request, stop before you tap and always seek a second opinion. Education and vigilance are our frontline tools in the fight against fraud."

To minimise the risks, the organisations recommend only downloading apps from verified platforms such as the Google Play Store, checking developer credentials, keeping devices updated, and being cautious of any apps that request unusual permissions.

Anyone who suspects suspicious activity is advised to contact their bank immediately. The public is reminded that well-organised international criminal groups often orchestrate cybercrime, and that no user is immune from being targeted.

As digital crime evolves, so must public awareness. Taking a moment to double-check before downloading could mean the difference between security and vulnerability.