

Case Study:

Vodafone UK Scam Signal – Phone Upgrade Scam

Case Study: Vodafone Scam Signal

APP fraud is surging, accounting for nearly 40% of all authorised fraud losses and costing UK consumers over £450 million in 2024. With mandatory reimbursement rules now in force, banks face greater liability - making real-time scam detection critical. As a result, banks have incorporated the Scam Signal API into their risk engine to help determine whether they allow the payment through or not.

The UK telecoms industry is losing over £200 million annually to mobile phone fraud orchestrated by criminal gangs, primarily through phone upgrade scams. A phone upgrade scam is where criminals impersonate legitimate mobile network operators or retailers to steal high-value devices.

- Fraud incidents rose 650% in the first half of 2025; criminals use stolen credentials to impersonate staff, order devices on customer accounts, and intercept deliveries.
- Account takeovers reached 26,000 in early 2025, with fraudsters also using false identities to secure devices on credit.
- Stolen devices are frequently trafficked to South-East Asia for resale on the black market.

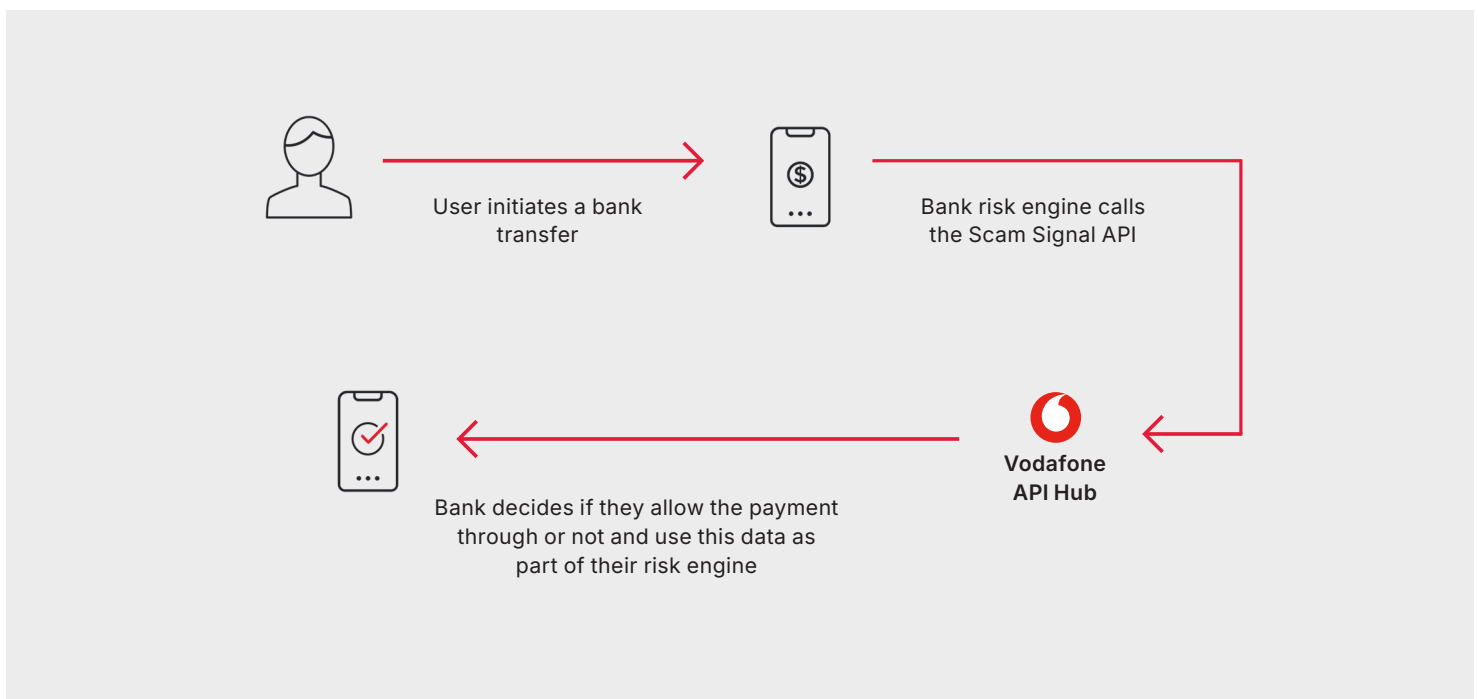
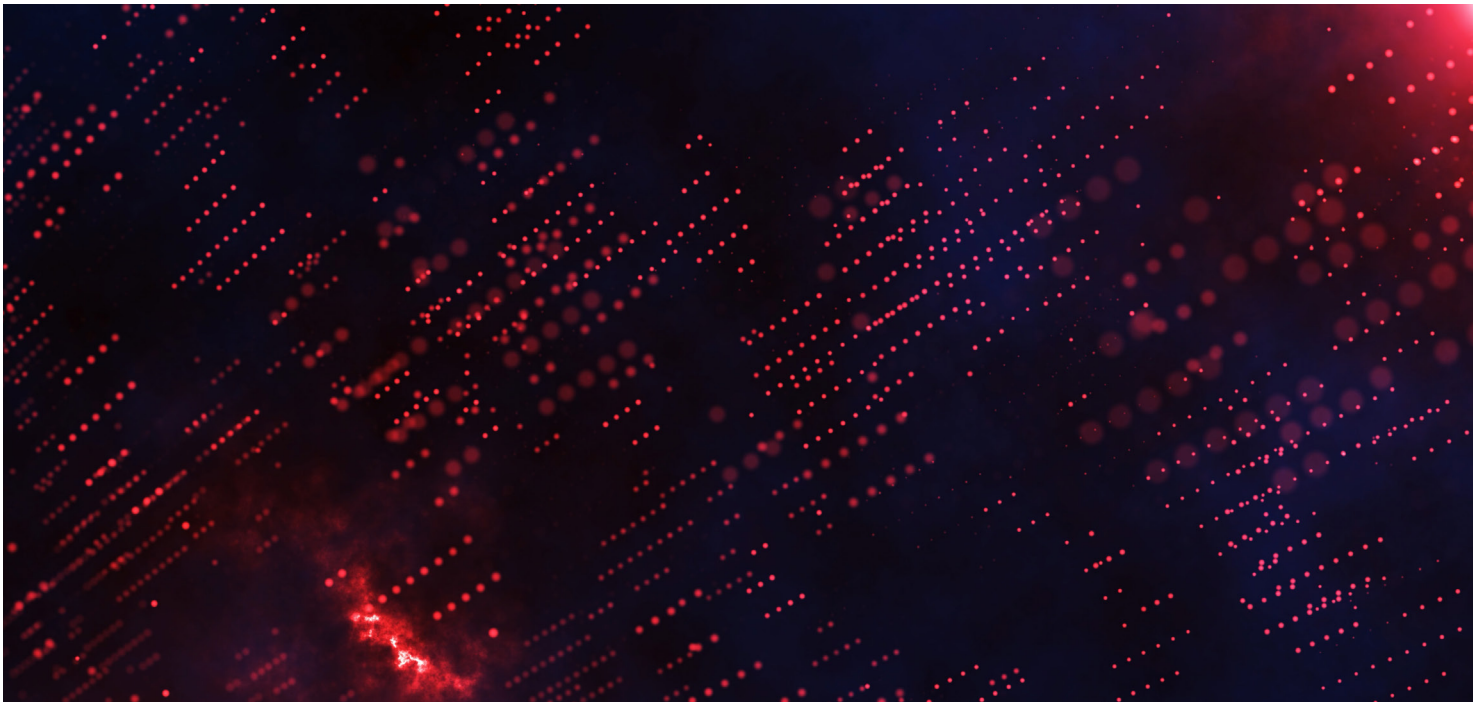


Figure 1



With phone upgrade scams, Scammers will call victims about an upgrade, requesting the victim to share their SMS OTP details as part of the 2FA. Scammers will then log into a customer’s account to order a new phone and when the victim mistakenly receives the phone to their

address, they are asked to return it to a ‘new’ address – directly to the scammer, who is now in possession of the phone.

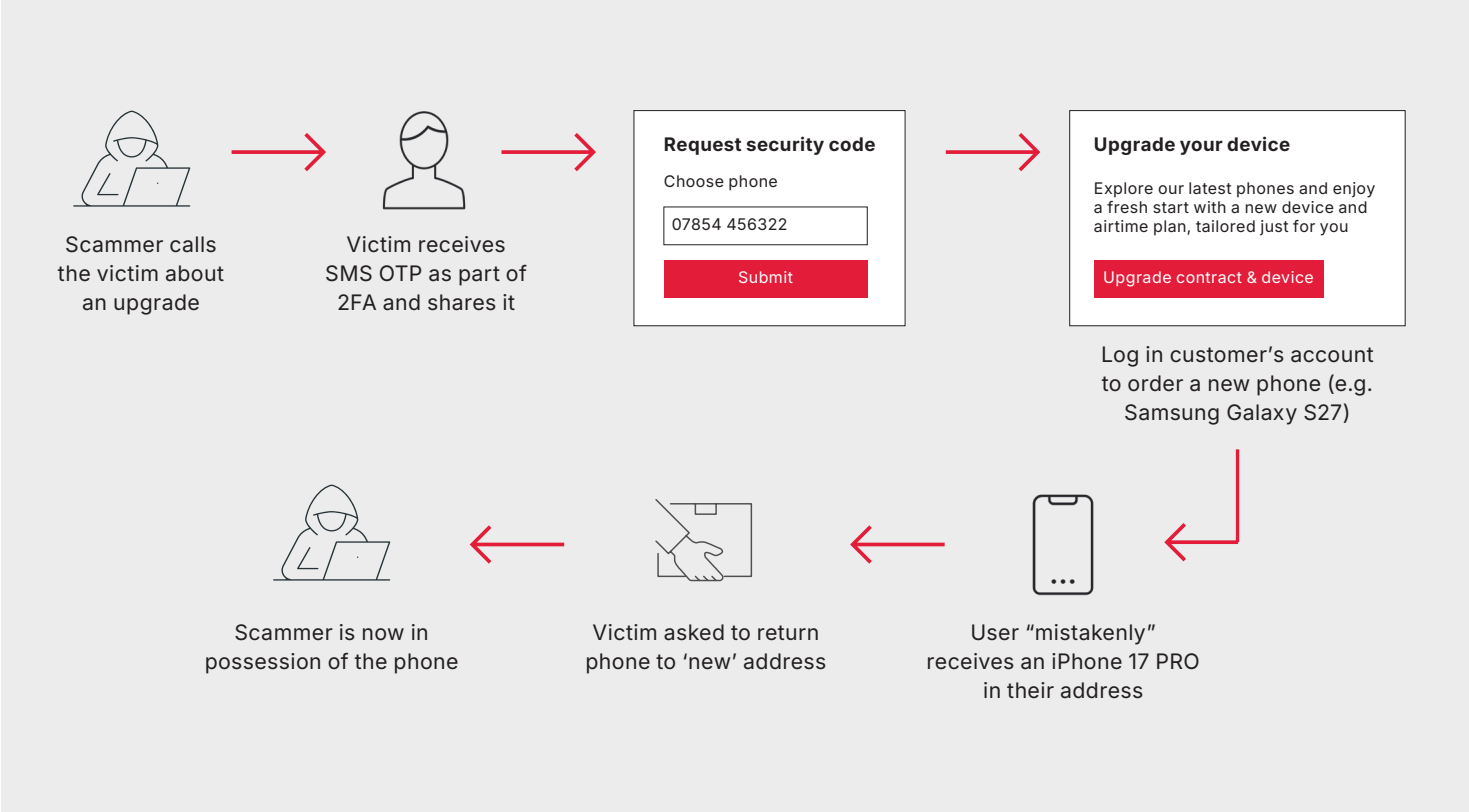


Figure 2

Actions:

To mitigate phone upgrade scams, Vodafone has applied the same logic as banks who embedded the Scam Signal API into their risk engines by incorporating

it into their phone upgrade journey. Now, when the scammer calls the victim about an upgrade and asks the victim to share the SMS OTP, the Scam Signal API is triggered and the phone order upgrade that the scammer requests is subsequently rejected, with Vodafone’s customer service team contacting the customer instead.

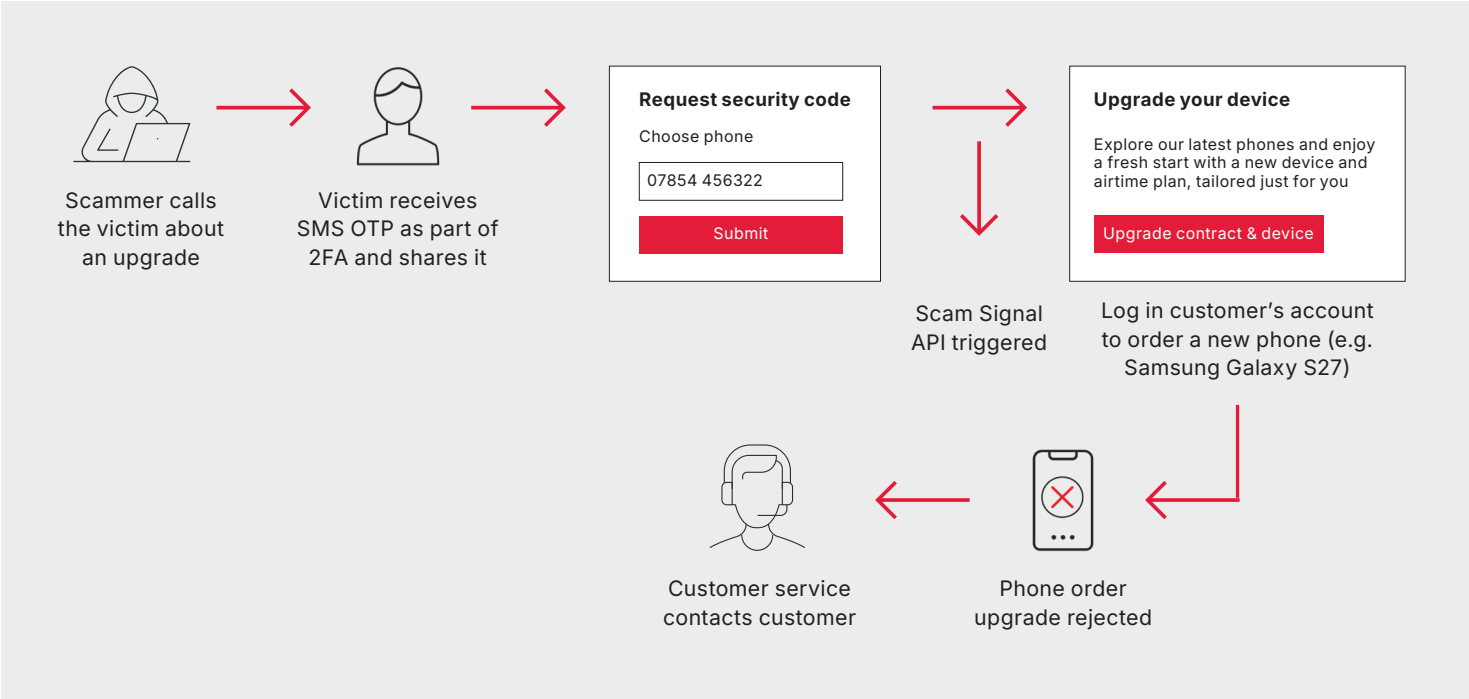


Figure 3

Impact:

With Scam Signal now embedded in the phone upgrade journey, there has been a significant reduction in fraud detection.

Additional information

	Participating organisation:	Vodafone UK
	Location:	United Kingdom

GSMA Head Office

1 Angel Lane
London
EC4R 3AB
United Kingdom
www.gsma.com

