

2025 - Threat Landscape Snapshot

- **What we've observed across the fraud and security threat landscape. Which tactics have threat actors leveraged?**



Phishing Emails continue to circulate impersonating service providers, parcel delivery companies, streaming services, email providers and so on.



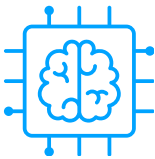
Smishing Messages are being sent to compel consumers and employees to part with valuable information - parcel delivery companies, local authorities, mobile network operators (MNOs) and governmental agencies being impersonated.



Cybersquatting is a growing trend with threat actors leveraging and registering similar domain names to legitimate businesses, services and organisations to make attacks more believable.



Social Media Security is a key issue with businesses and organisations that are active on social media exposed to risks of impersonation with cloned pages, channels or cybercriminals creating similar profiles to the genuine page. While social media marketplaces have strong links to fraud.



AI-Powered Scams are trending with AI being used to generate believable content and deepfakes to trick employees, consumers and customers or impersonate celebrities and public figures.



Vishing Phone calls impersonating banks, regulators, law enforcement, courts and so on are being used to convey a sense of urgency to compel targets to part with sensitive information.



QR Code Scams redirecting motorists, visitors and car park users and so on to phishing domains, later resulting in **APP Fraud** as part of complex impersonation attacks.

While recruitment scams, fake work-from-home offers, cloned firms, financial abuse, money mules, cryptocurrency fraud, and so on poses ongoing risks to vulnerable customers