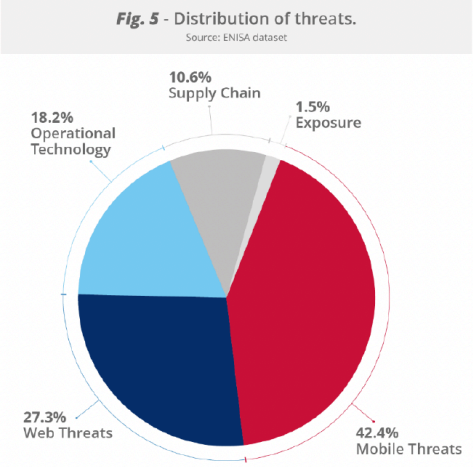
# Mobile Threat of the Month

January 2026

## 2025 European Mobile Threat Landscape Summary

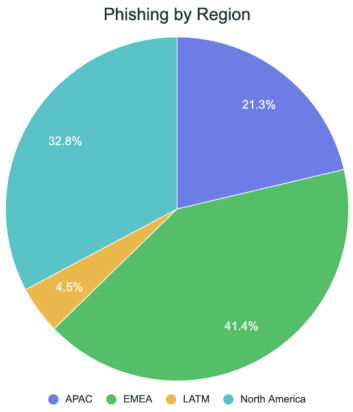
2026 marks the end of mobile security as a 'transitional' issue in the EU; it is now an urgent, active exposure. We have entered the era of the **'weaponisation of ubiquity,'** where the universal presence of mobile devices provides hackers with an unprecedented and permanent surface for attack.

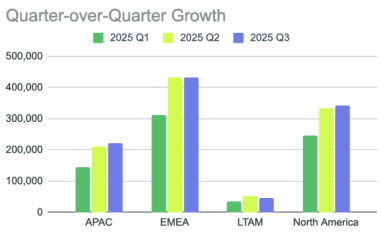
The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2025 (ETL 2025) report serves as a definitive barometer for the cybersecurity climate of the European Union.




The report confirms a historic shift in EU cybersecurity: mobile threats now represent the single largest risk category, accounting for **42.4% of all incidents.** This is no coincidence. As businesses have centralised their security—using mobile devices for Multi-Factor Authentication (MFA) and corporate access—attackers have followed suit. By targeting the mobile device, hackers are no longer just stealing a phone; they are capturing the **"keys to the kingdom"** for entire corporate networks.

This aligns with findings from Lookout's Q3 2025 Mobile Threat Landscape report, which identifies the EMEA region (Europe, the Middle East, and Africa) as a "structurally elevated" threat landscape that sustains a higher absolute volume of mobile phishing attacks compared to other global regions.




Threat actors are no longer probing whether mobile-first phishing techniques are effective across European businesses. Instead, they are executing repeatable, scalable campaigns that rely on mobile phishing, social engineering, and identity abuse as primary access vectors. In many cases, attackers no longer require malware or vulnerability exploitation at the outset; instead, they operate entirely within legitimate authentication and access workflows.

For today's Security and IT Teams, visibility into mobile risk is no longer optional—it's foundational. The European threat activity outlined in this report reflects that mobile devices have become one of the most reliable early access points for attackers seeking to compromise the enterprise through its people.

Contact your Lookout Partner to understand your organisation's exposure to mobile risk.

Sources: ENISA & Lookout