PRESS RELEASE

Stockholm, Sweden
February 25, 2024

Enea Study: Almost Two-Thirds of Enterprises Suffer Significant Losses to Mobile Fraud

Research from Enea reveals 76% of enterprises lack sufficient voice and messaging fraud protection as AI-powered vishing and smishing skyrocket following the launch of ChatGPT.

Around two-thirds (61%) of enterprises still suffer significant losses to mobile fraud, with smishing (SMS phishing) and vishing (voice phishing) being the most prevalent and costly. That's according to a new global survey undertaken by Enea which gathered insights from more than 400 telecom operator and enterprise respondents about the state of mobile fraud and network security.

The report, titled "Mobile Network Security: Bridging the Gap Between Enterprise Needs and CSP Capabilities" sheds light on the extent of fraud perpetrated through vital telecom channels used by enterprises worldwide. Enterprises account for a significant share of Communication Service Provider (CSP) subscribers and an even greater share of their revenues. They Depend on their CSP to protect them from telecom-related fraud, with the absolute majority (85%) saying security is important or extremely important for their telecoms buying decisions.

Publication of the report comes as the democratization of AI-based deepfake technology and easy access to number spoofing apps is lowering the barrier to entry for cybercriminals and increasing the sophistication of fraud-based attacks. **Since the launch of ChatGPT in November 2022, vishing, smishing, and phishing attacks have increased by a staggering 1,265%.**

The key takeaway from the survey was the discovery of a significant gap between the security needs and expectations of enterprises and the level of network security being offered by CSPs. This is a gap criminals are keen to exploit, evidenced by the soaring rate of fraud.

A summary of the report's key findings is outlined below.

Enterprises are being hit hard by voice and messaging fraud and expect their CSPs to take the lead in protecting them.

· 61% of enterprise respondents said their mobile messaging fraud costs were significant, yet more than three-quarters don't invest in SMS spam or voice scam/fraud protection.

Enea AB, P.O. Box 1033
164 21 Kista
Phone: +46 8 507 140 00
Fax: +46 8 507 140 40
E-mail: info@enea.com
Website:
www.enea.com

· Slightly more than half (51%) said they expect their telecom operator to protect them from voice and mobile messaging fraud, citing their role as more important than that of cloud providers, managed IT providers, systems integrators or direct software vendors.

· 85% of enterprises say that security is important or extremely important for their telecoms purchasing decisions.

CSPs lack sufficient capabilities to meet enterprise expectations for security.

· Only 59% of CSPs say they have implemented a messaging firewall, and just 51% said they have implemented a signaling firewall.

· Less than half (46%) report adopting some threat intelligence service, essentially leaving a majority blind to new or morphing threats.

CSPs that prioritize security are better positioned to win enterprise business.

· Security leaders, characterized by better capabilities, better funding, and a higher prioritization of security, are less than half as likely as the followers to have a security breach go undetected or unmitigated (12% vs 25%).

· CSP security leaders are more likely to see security as an opportunity to generate revenues (31% vs 19%).

"We've observed the rapidly evolving threat landscape with growing concern, particularly as AI-powered techniques become more accessible to cybercriminals," commented John Hughes, Senior Vice President and Head of Network Security at Enea. "The stark increase in mobile fraud, particularly following the advent of advanced technologies like ChatGPT, underscores a critical need for enhanced network security measures. This survey highlights a significant disconnect between enterprise expectations and the current capabilities of many CSPs, and our ongoing mission is to help the sector bridge that gap and safeguard networks and users."

In November, Enea evolved its mobile network security portfolio to help operators and CPaaS (Communication Platform-as-a-Service) providers increase their resilience amid growing threats. The portfolio includes the intelligence-driven Enea Adaptive Signaling and Messaging Firewalls, which leverages innovative and AI-enhanced capabilities to accurately guard against sophisticated smishing and vishing attacks.

To download the full report and learn more, please visit https://www.enea.com/insights/mobile-network-security-bridging-the-gap-between-enterprise-needs-and-csp-capabilities-2/.

Enea AB, P.O. Box 1033
164 21 Kista

Phone: +46 8 507 140 00
Fax: +46 8 507 140 40

E-mail: info@enea.com
Website:
www.enea.com

Survey methodology:

The report is based on responses from an online survey of 416 participants conducted by Mobile World Live on behalf of Enea. The survey participants included CSPs, enterprises, and technology vendors. To present the most relevant results, replies from technology vendors have been filtered out, and all data presented in this report is based on the responses from CSPs and enterprises. CSPs account for just over 70% of the responses, and enterprises account for the remaining 30%. Geographically, the majority (45%) of CSP respondents' company headquarters are in Europe, 21% in North America, 13% in Africa, and 9% in South America or the Middle East. The majority (54%) of enterprise respondents' company headquarters are in Europe, 20% in North America, and 13% in Africa. The remaining 13% said their company is based in Southeast Asia, Oceania, and South America.

Contact

Stephanie Huf, Chief Marketing Officer
E-mail: stephanie.huf@enea.com

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for fixed and mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day.
Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security.

Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

For more information: www.enea.com