Fraud and Scams: Staying Safe in the Mobile World

21 May 2025

Rita de Castro

Global nature of fraud

By the end of 2024, 58% of the world’s population used mobile internet, equating to 4.7 billion users.

As digital communication grows, so does the threat of fraud, impacting individuals, businesses, and governments globally.

The global financial cost of cybercrime is projected to be USD 15.63 trillion by 2029 (Statista).

Fraud is a global issue and a huge area of concern for mobile operators!

Types of Fraud

Fraud and scams can be described using a variety of terms, sometimes overlapping, but each emphasizing different aspects of deceptive practices employed by criminals to exploit victims.

Among the most prevalent and damaging are impersonation fraud and spoofing leveraging the telecommunication channels.

An alarming trend in social engineering fraud is the increasing sophistication of attacks.

Countermeasures

To address the issue, mobile operators invest significant resources in identifying, filtering, and blocking fraudulent traffic on their networks. However, the mobile industry cannot solve the issue alone.

Facilitators for communication: telecom companies provide the infrastructure/ media that scammers exploit for attacks.

Enhanced Cooperation with Banks

Collaborating with Authorities

Educating Customers

Sharing Key (Anonymized) Data

Promoting Strong Security Measures

Blocking Fraudulent Communications

Fraud Detection Technologies

Countermeasures

GSMA

- The GSMA represents mobile operators globally and helps combat fraud through awareness, guidelines, and innovations.
- The GSMA and its members have been at the forefront of developing best practices and technologies to safeguard against various types of fraud, including impersonation.
- The GSMA's Fraud and Security Group (FASG) drives the industry's direction on fraud and security matters related to mobile technology, networks and services.

Voluntary initiatives / Best Practices

In the pursuit of our customers' interests, operators cooperate with payment services providers to minimise payments fraud!

Many different approaches are followed by GSMA members to fight 'spoofing' fraud and other scam calls.

These include number registries with block lists that operators may use to validate the Calling Line Identity (CLI) during call setup as well as technical signalling controls to authenticate, secure and validate the CLI from caller to called.

In parallel, various processes are used, sometimes based on regulatory enforcement, for traceback, reconciliation, and fault investigation, to identity and eliminate sources of abusive traffic.

Recommendations

Governments and regulators

- Fostering collaboration & removing red tape and barriers to cooperation
- Empowering consumers with knowledge and tools to protect themselves
- Establishing frameworks to facilitate cross-sector and cross-border data sharing
- Introducing regulatory sandboxes to pilot new fraud prevention technologies and services
- Participating in established frameworks and conventions, e.g. ASEAN, Malabo, Budapest

Mobile operators

- Swiftly acting on fraud threats and sharing intelligence with industry and other sectors
- Providing regular employee training on security, fraud and scams
- Encouraging employees to report suspicious behaviour
- Publishing simple helpful information for consumers

Consumers

- Being vigilant and recognising warning signs
- Ensuring device software is kept regularly updated
- Learning about the common impersonation types and methods used
- Implementing two-factor authentication and employing strong, unique passwords

GSMA

Fraud and Scams:

Staying Safe in the Mobile World

February 2025

Thank You!