Jon France
Head of Industry Security
GSMA
In The News

**NEWS**

*Fraud epidemic 'is now national security threat'*

By Gordon Corera
Security correspondent

© 25 January

**EUROPOL**

**TEN HACKERS ARRESTED FOR STRING OF SIM-SWAPPING ATTACKS AGAINST CELEBRITIES**

15 February 2021
*Press Release*

**CULTURE**

*Hackers keep stealing highly coveted Instagram usernames*

At the core of this issue is economic misery, and Instagram is part of the problem.
The Dilemma

SMS / USSD is ....

- Ubiquitous – available in all markets
- Simple to engineer for – well understood and many ways to use
- Inexpensive - Low overhead
- Well adopted

But ...

- Was engineering of its age and not designed with high security in mind
- Can be compromised through signaling attacks etc.
- Does not contain sender verification
- Well adopted
SMS / USSD – OTP – Challenges

Procedural
- Account Takeover (ATO)
- Fraudulent Sim Swap
- Social Engineering

Technology
- Interception / Re-route
- Older Signaling (SS7)
- Complex phishing

Regulatory / Advisory
- Draft NIST Deprecation
- EU Payment Services Directive 2

Market
- Consumer Confidence
- Feature rich apps
- Security experts warning
- User Experience
SMS / USSD – OTP – Challenges

Procedural
- Sim Swap Process Improvements
- Social hardening
- Consumer education

Technical
- Sim Swap API’s
- MSISDN Verify
- RCS
- SS7 Firewalling / Fraud Detection

Market
Regulatory / Advisory
Key Messages

Any second factor is better than no second factor

The majority of compromises are NOT due to technology means but are procedural / social in nature – focus on fixing these

Technical

Look at confidence factors – multi signal intelligence
Build defense in depth.

Procedural