DFS Security Recommendations for Regulators and Providers

Arnold Kibuuka, Project Officer, ITU

http://www.itu.int/go/dfssl

June 2025

DFS Security Recommendations

1. Security recommendations to protect against DFS SIM related risks
2. Recommendations to mitigate SS7 vulnerabilities
3. DFS Mobile application security Best practices (From ITU-T X.1150)
4. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
5. DFS consumer competency framework

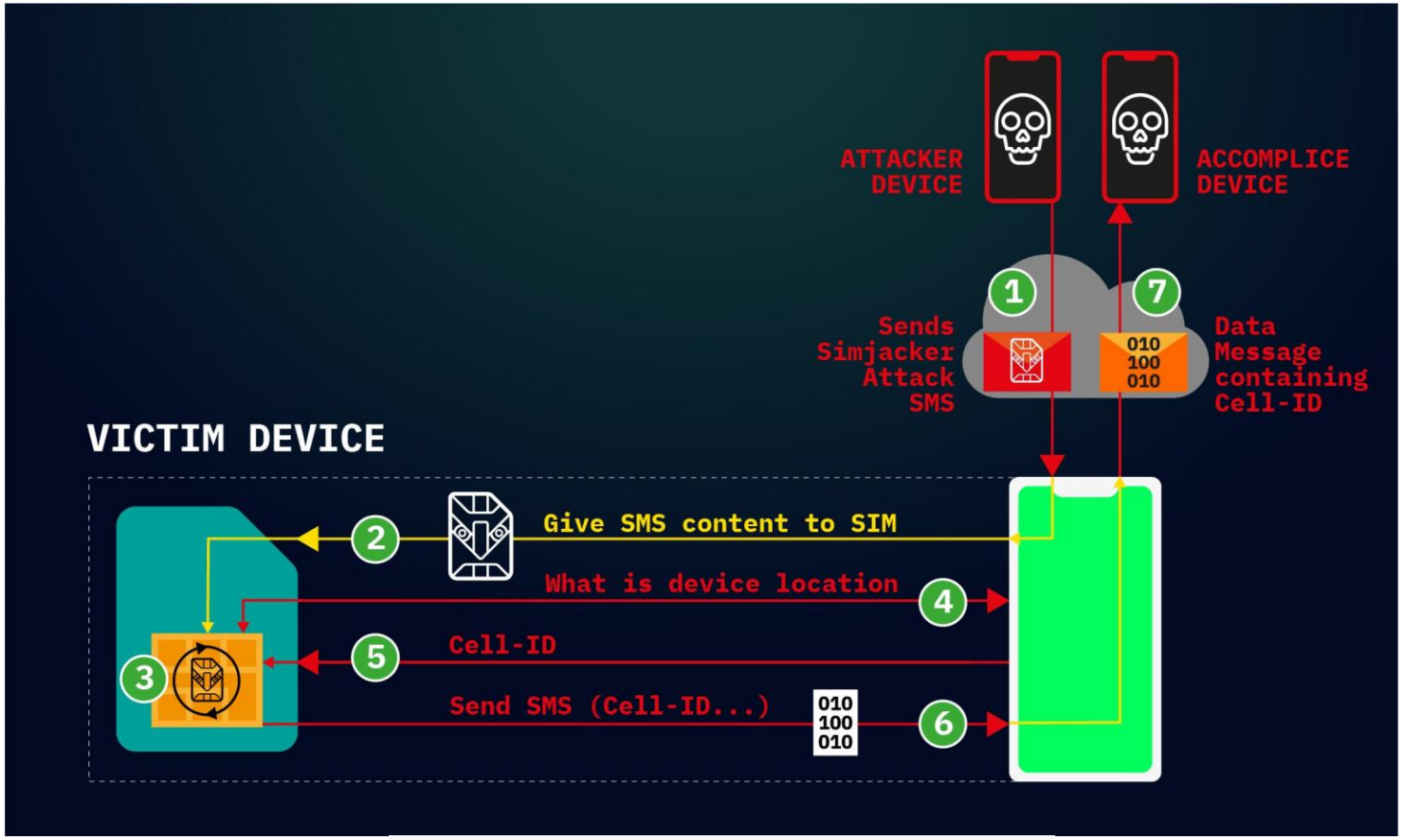
Regulatory Guidance to Mitigate SIM Risks

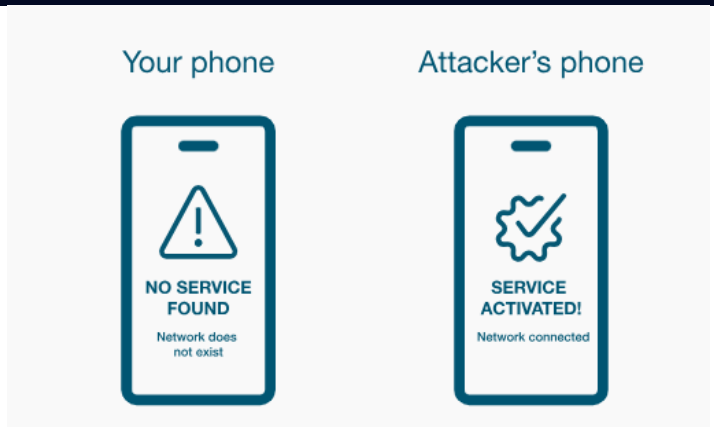
Poll Question

Which of these SIM card-related security risks are you familiar with?

SIM Risks

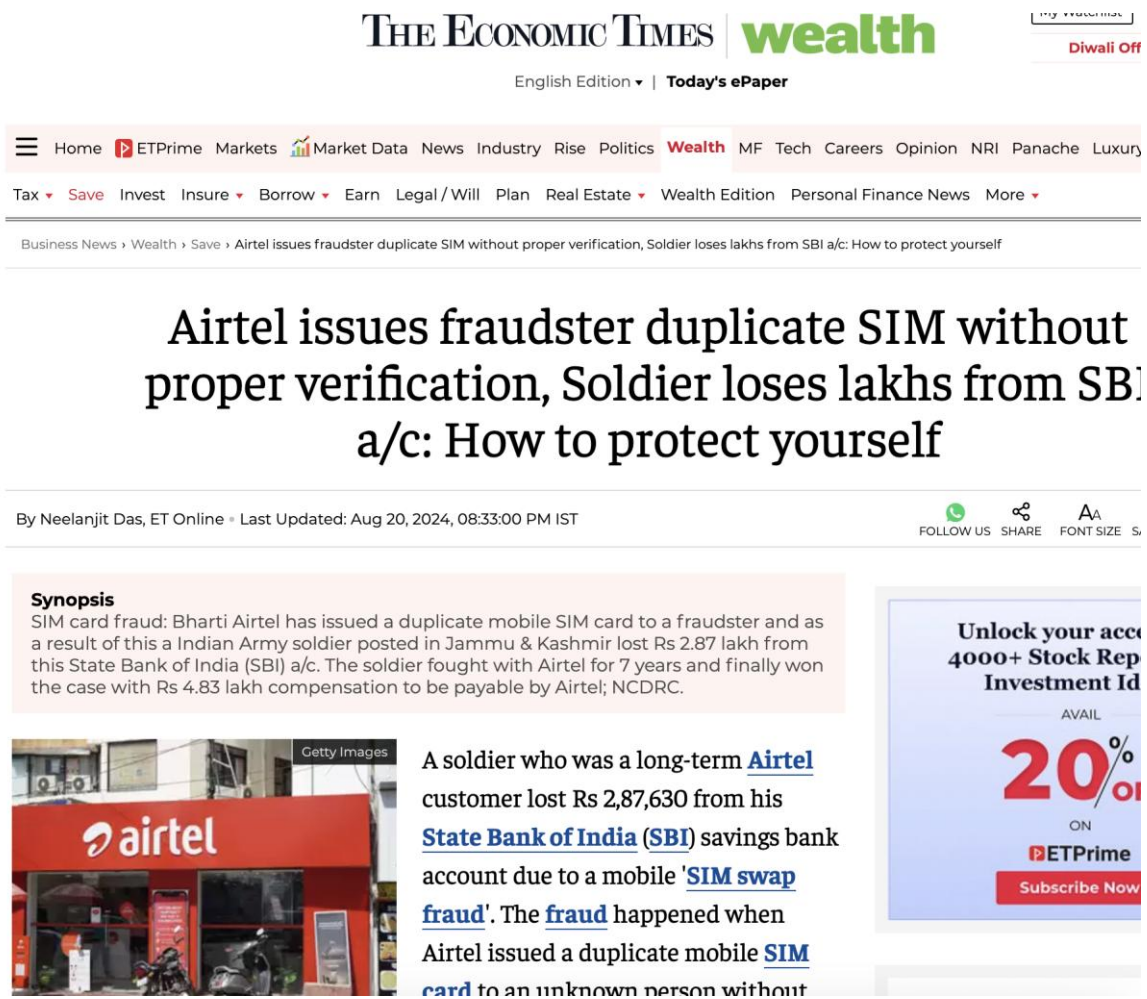
- SIM cloning
- SIM swaps
- SIM Recycling
- Binary over the air attacks (Sim jacker and WIB browser attacks)





Sources: Positive Technologies, Yubico

SIM Risks



THE ECONOMIC TIMES | wealth

English Edition | Today's ePaper

Home ETPrime Markets Market Data News Industry Rise Politics Wealth MF Tech Careers Opinion NRI Panache Luxury

Tax Save Invest Insure Borrow Earn Legal / Will Plan Real Estate Wealth Edition Personal Finance News More

Business News › Wealth › Save › Airtel issues fraudster duplicate SIM without proper verification, Soldier loses lakhs from SBI a/c: How to protect yourself

Airtel issues fraudster duplicate SIM without proper verification, Soldier loses lakhs from SBI a/c: How to protect yourself

By Neelanjit Das, ET Online • Last Updated: Aug 20, 2024, 08:33:00 PM IST

FOLLOW US SHARE FONT SIZE

Synopsis

SIM card fraud: Bharti Airtel has issued a duplicate mobile SIM card to a fraudster and as a result of this a Indian Army soldier posted in Jammu & Kashmir lost Rs 2.87 lakh from this State Bank of India (SBI) a/c. The soldier fought with Airtel for 7 years and finally won the case with Rs 4.83 lakh compensation to be payable by Airtel; NCDRC.

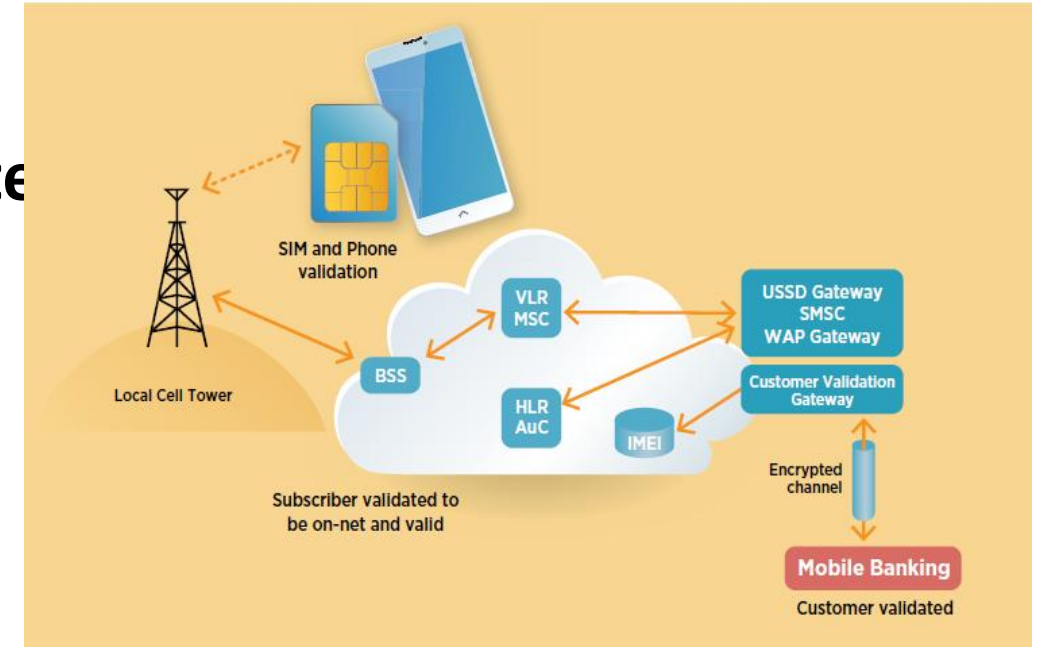
Getty Images

A soldier who was a long-term Airtel customer lost Rs 2,87,630 from his State Bank of India (SBI) savings bank account due to a mobile 'SIM swap fraud'. The fraud happened when Airtel issued a duplicate mobile SIM card to an unknown person without

Unlock your acc
4000+ Stock Rep
Investment Id
AVAIL
20%
ON
ETPrime
Subscribe Now

DFS Operators Controls to Mitigate SIM Swaps

- Real time IMSI/ICCID detection
- Real time device change detection – device to DFS account binding
- Encourage use of secure DFS access through apps.



Category: PREMIUM

API Name	API Definition
Sim Swap API	API which allows a corporate customer to check if a given MSISDN has performed a SIM swap. Returns 'MSISDN',' date of last SIM swap'
Authentication API	API which allows a corporate customer to use MTN Service to send OTPs . A customer is onboarded on the MTN instance and the OTP service is configurable to them
KYC Premium API	API allows a customer to check if the KYC info provided by its customers matches with that provided at Sim registration. Returns one or more actual customer details. This requires customer consent

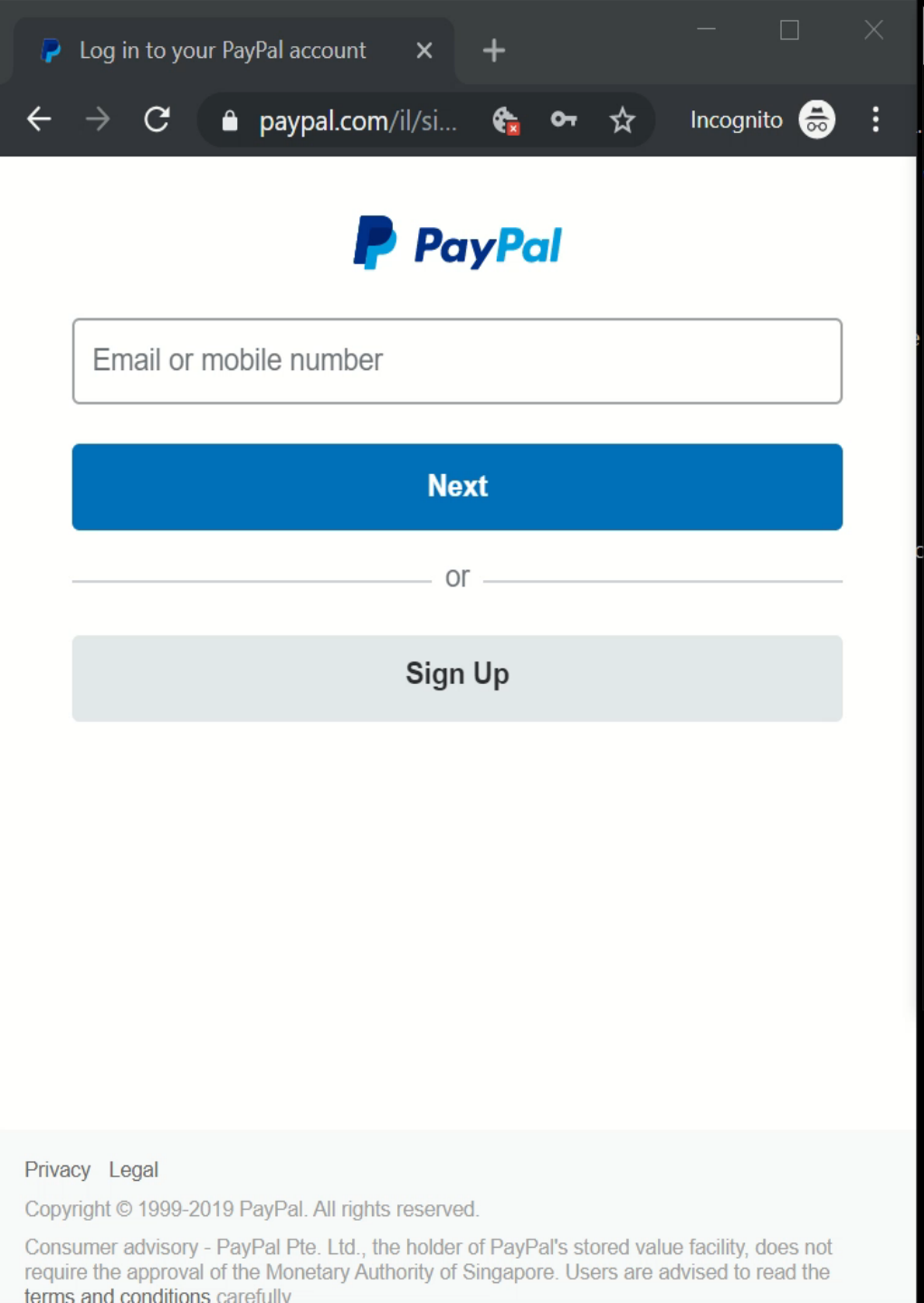
Guidance to Mitigate SS7 Threats

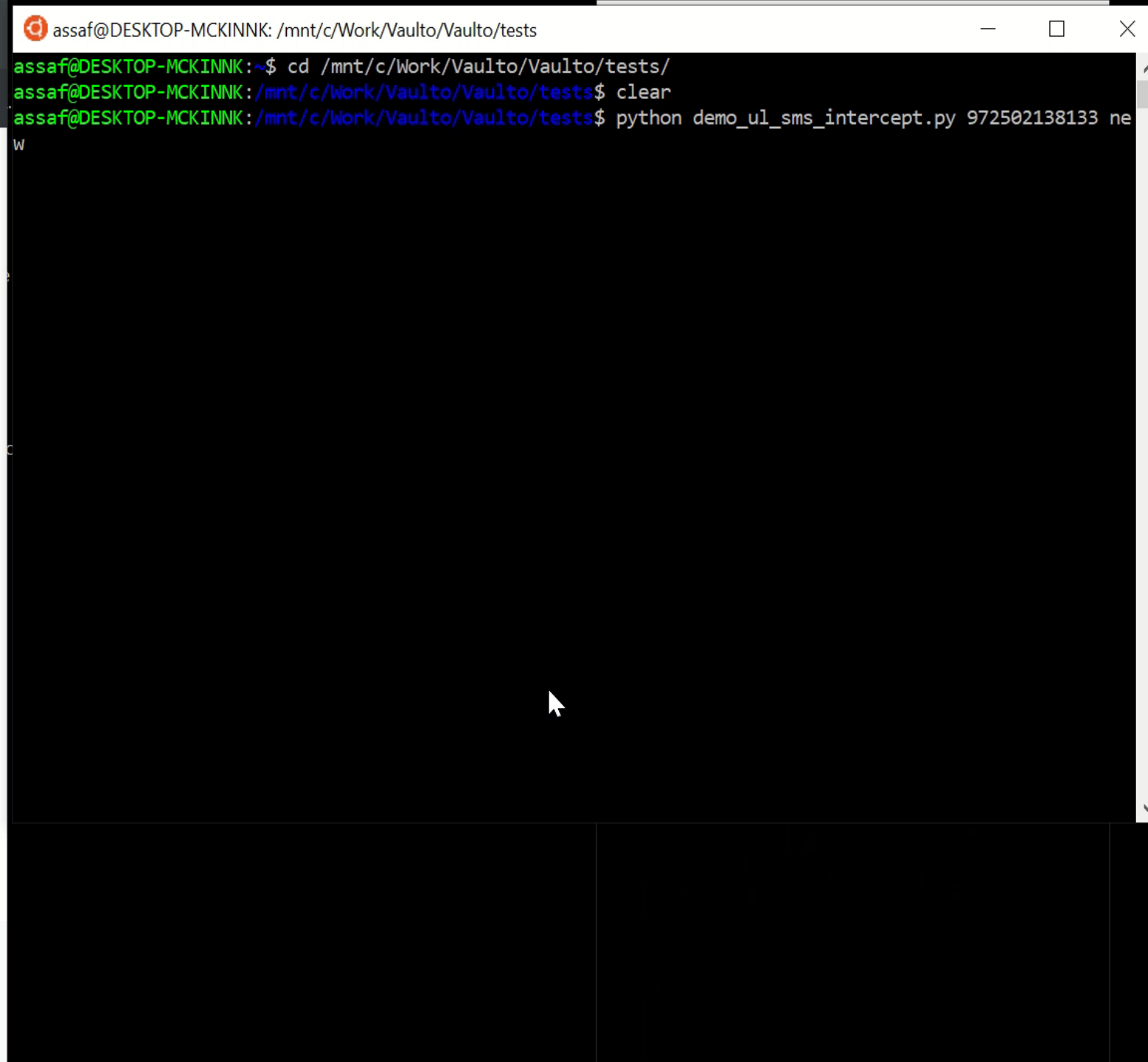
Related report: Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions

Poll Question

SS7 (Signalling System No. 7) is a network protocol used by telecom companies. Vulnerabilities in SS7 can impact the security of Digital Financial Services (DFS).

How familiar are you with SS7 and its potential impact on DFS?


Log in to your PayPal account
paypal.com/il/si...
Incognito
PayPal
Email or mobile number
Next
or
Sign Up
Privacy
Legal
Copyright © 1999-2019 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully

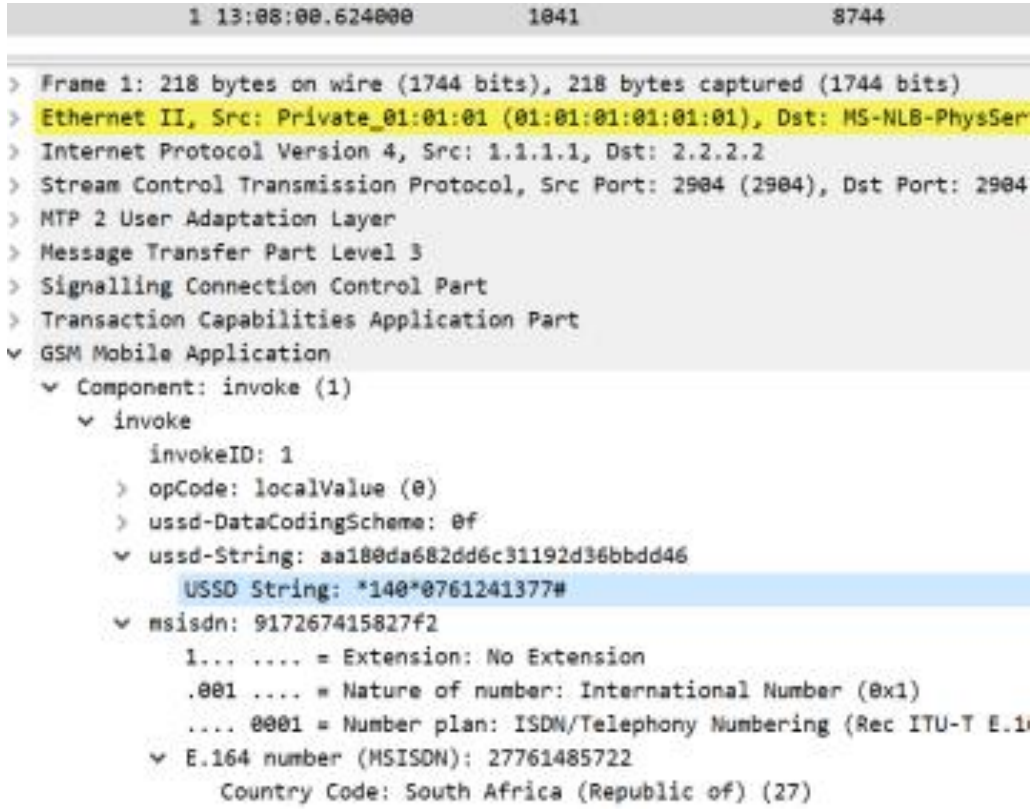

assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 ne
w

Regulatory Guidance to Mitigate SS7 Risks

- Regulatory coordination between telco and DFS regulator on SS7 vulnerabilities.
- Incentivize the industry
- Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS
- Telecom regulators to establish baseline security measures for each SS7 risk category
- IMSI validation gateway: An API that provides status of a number and real time country where client is located.

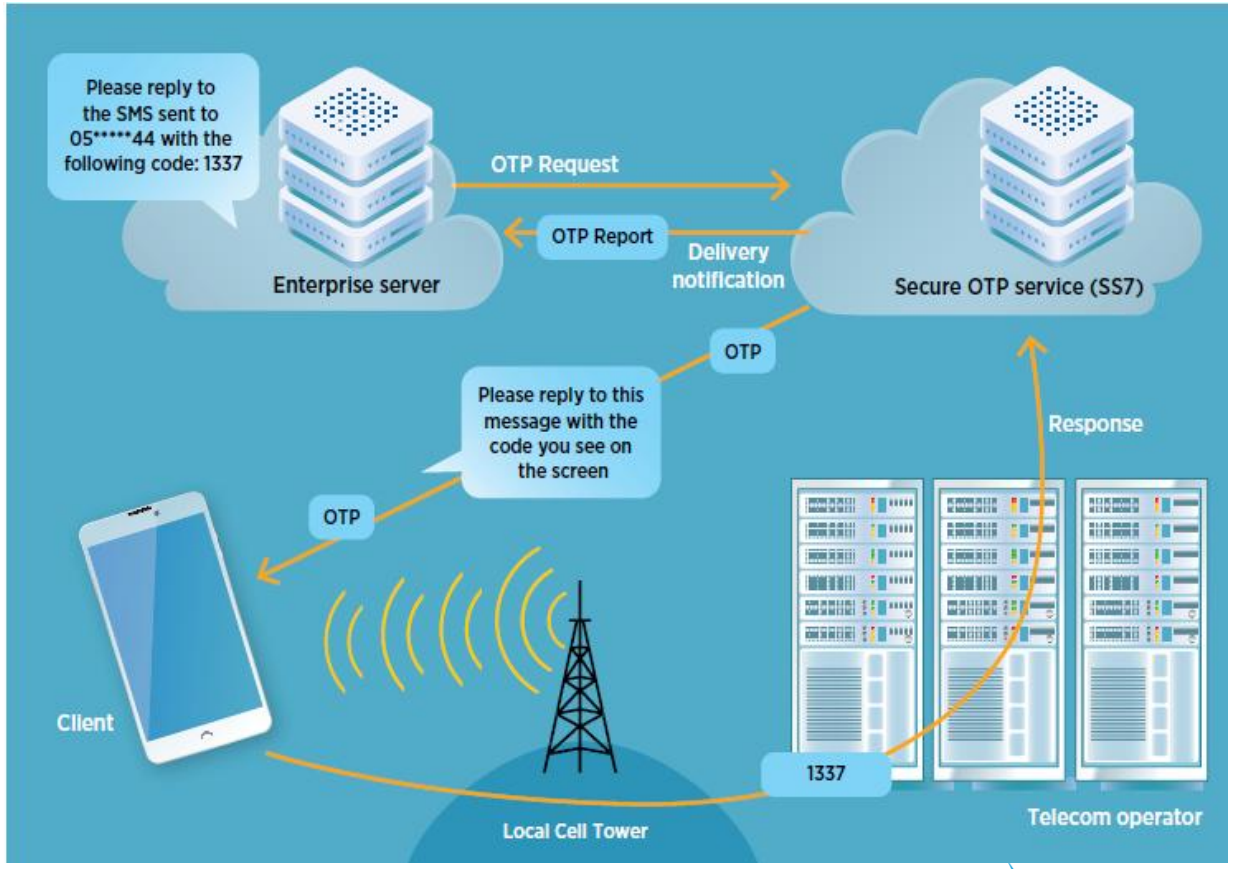
Recommendations for MNO to Mitigate SS7 Risks

- SS7 interconnect security monitoring guidelines
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing



DFS Operator Controls to Mitigate SS7 Risks

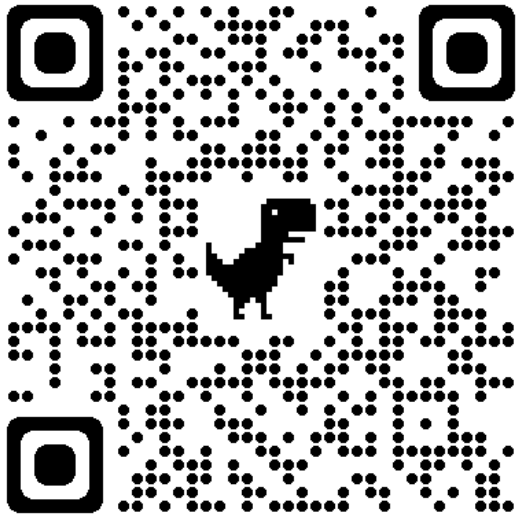
- Session time out
- Transaction limits for insecure channels
- User education
- Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD
- Bidirectional OTP SMS flow



ITU-T Study Group 11 Work on SS7

Published Recommendations and Technical Reports:

- ITU-T QSTR-SS7-DFS (2019): SS7 vulnerabilities and mitigation measures for digital financial services transactions
- ITU-T QSTR-USSD (2021) Low resource requirement, quantum resistant, encryption of USSD messages for use in financial services
- ITU-T Q.3062 (2022): Signaling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks
- ITU-T Q.3063 (2022) : Signaling procedures of calling line identification authentication
- Draft Q.TSCA: Requirements for issuing End-Entity and Certification Authority certificates for enabling trustable signaling interconnection between network entities.
- Draft Q.DMSA: Principles for detection and mitigation of signaling attacks in security signaling gateway



http://www.itu.int/go/dfssl

Contact: dfssecuritylab@itu.int

Thank you!