Security of Digital Financial Services (DFS)

Vijay Mauree
Programme Coordinator
Standardization Bureau
ITU
DFS Security Recommendations

The DFS Security Recommendations contain the following specific guidelines that may be adopted by regulators:

1. Model Memorandum of Understanding between a Telecommunications Regulator and a Central Bank Related to Security for Digital Financial Services

2. Recommendations to mitigate SS7 vulnerabilities

3. Recommendations for securing mobile payment apps

4. Recommendations for operators and regulators for SIM card risks such as SIM swap fraud and SIM card recycling.
Guidance to mitigate SIM fraud

1. Regulatory coordination between telco and DFS regulator on SIM vulnerabilities. - e.g. An MOU between the DFS regulator and Telecom regulator
2. Standardization by regulators of SIM swap rules amongst MNOs/MVNOs - including SIM swaps leading to porting of numbers to other MNOs/MVNOs
3. Recommending security measures for MNOs on SIM risks
DFS Security Lab - Objectives

Collaborate with regulators to adopt DFS security recommendations

Perform security audits of mobile payment apps (USSD, Android and iOS)

Encourage adoption of international standards on DFS security

Organise security clinics & Knowledge transfer for Security Lab

Assist regulators to evaluate the cyberresilience of DFS critical infrastructure

Networking platform for regulators for knowledge sharing on threats and vulnerabilities

Website: https://www.itu.int/en/ITU-T/dfs/seclab/Pages/default.aspx