DFS Security Webinar Series

Epimack Mbeteni

Focus Areas

1. Introduction
2. Social engineering scenarios
3. Impact of social engineering
4. Preventive & Reactive measures

Social engineering scenarios

- Social engineering is a type of fraud that involves **manipulating** individuals into divulging confidential information or performing actions that compromise security. In the context of mobile money, social engineering fraud scenarios include impersonation of mobile money operators, regulatory authority impersonation, fake SIM upgrades by freelancers, and child emergency scams

social engineering scenarios

Impersonation

- Impersonation in social engineering involves fraudsters pretending to be someone they are not to manipulate individuals into divulging confidential information or performing actions that compromise security. In the context of mobile money, impersonation scenarios include:

Social engineering	Meaning
Impersonation of Mobile Money Operator	Fraudsters send fake SMS and calls pretending to be a mobile money operator representative, requesting a fund reversal and instructing the customer to send money to the fraudster
Regulatory Authority Impersonation	Fraudsters claim that the customer's SIM will be deactivated and impersonate a regulator to trick the customer into sending money
Friends/Family/promotion impersonation	Uses your relative name or social media to ask for help, common also in lost/stolen phone. Sometimes promotion or prize scam.

Impact of social engineering

- **Loss of Trust**
- **Financial loss**
- **Loss of personal data**
- **Brand & reputation damage**
- **Increase in operation cost**

Preventive & Reactive Measure

Education initiative

- Mobile Money operator led
- Industry and regulator led
- SMS, Radio, community engagements.

AI & Machine learning to used to identify and block fraudulent SMS

Promotion of 100 as customer care

Account suspension/blocking – Using short cade

Daily transaction threshold

Together we can