GOBHOZA LEGAL PRACTICE

GOBHOZALEGALPRACTICE.CO.BW
+267 3116371

Tech Tuesdays With Masa.

SIM CARD FRAUD: HOW CRIMINALS HIJACK YOUR NUMBER AND WHAT YOU CAN DO ABOUT IT

Published: 11th March2025

SIM swap scams have become increasingly common in Botswana, exposing individuals to financial theft and identity fraud. A recent case in Spain provides valuable lessons on why telecom companies must strengthen security measures, and how individuals can protect themselves.

The Orange España Case

A client of Orange España fell victim to SIM card fraud after criminals impersonated her and obtained a duplicate SIM card from the telecom provider without proper verification. Using the new SIM card, the fraudsters intercepted her bank authentication codes, gaining access to her accounts and stealing €9,000. She filed a complaint with the Spanish Data Protection Agency (AEPD), alleging that Orange failed to implement adequate security measures to prevent the unauthorized swap.

Orange defended itself, claiming that at the time, it followed standard procedures and only strengthened security after the incident. However, the AEPD ruled that the GDPR requires preventive measures, not reactive ones. The telecom giant was fined €1.2 million for failing to ensure the confidentiality and security of personal data, as required by Article 5(1)(f) and Article 32 of the GDPR.

Lessons for Botswana: Protecting Consumers from SIM Card Fraud

In Botswana, where SIM card fraud is on the rise, this case highlights why stronger security measures are needed from both telecom providers and individuals. Under the Botswana Data Protection Act, 2024, companies handling personal data must implement robust safeguards to prevent unauthorized access, similar to the requirements under GDPR.

How Telecom Providers Can Prevent SIM Card Fraud

1. Stronger Identity Verification – Require multi-factor authentication before issuing a replacement SIM.

2. Fraud Detection Systems – Monitor unusual SIM swap requests and alert customers immediately.

3. Regulatory Compliance – Align security measures with Botswana's Data Protection Act, 2024 to avoid liability.

Tech Tuesdays With Musa.

Published: 11th March 2025

What Individuals Can Do to Stay Safe

1. Set a PIN or Password for SIM swaps Ask your provider if you can add extra protection.

2. Use Authentication Apps Instead of SMS Codes – Banks often allow verification via authenticator apps

3. Monitor Bank and Mobile Accounts – Report any suspicious activity immediately.

4. Be Cautious with Personal Information Avoid sharing sensitive details that could be used to impersonate you.

Conclusion

The Orange España case serves as a wake-up call for Botswana's telecom providers, regulators, and consumers. SIM card fraud is not just a tech issue, it's a serious data protection risk. Stronger security protocols must be enforced to prevent fraudsters from exploiting weak systems. For individuals, awareness and proactive measures are key to keeping personal data safe.

Article by Princess Musa Motlogelwa

If you have interest in an in-depth discussion on this subject matter or any Data Protection issues, feel free to contact us at info@gobhozalegalpractice.co.bw
Tel: 3116371