Cybersecurity Management: Social Engineering as Top Threat

University of Namibia (UNAM) Security Briefing

PRESENTER

Dr. Carlson Eyongabi

POSITION

President, SwissLink Professional University, Cameroon

DATE

May 20, 2026

Presentation Agenda

01 Introduction & Why It Matters

02 Cybersecurity Foundations

03 Attack Types & Techniques

04 Psychology of Deception

05 African & Global Case Studies

06 Defence & Best Practices

07 Interactive Activity & Q&A

1

Introduction & Why It Matters

Understanding the 2024–2026 threat landscape in Africa and globally

Africa's Digital Landscape: Opportunity and Risk

646M+
Internet users in Africa (2025 est.)

38%
Africa internet penetration rate (2024)

74%
African web traffic via mobile devices (2024)

$1.1T
Africa's mobile money transactions (2024)

Why This Matters for Namibia and SADC

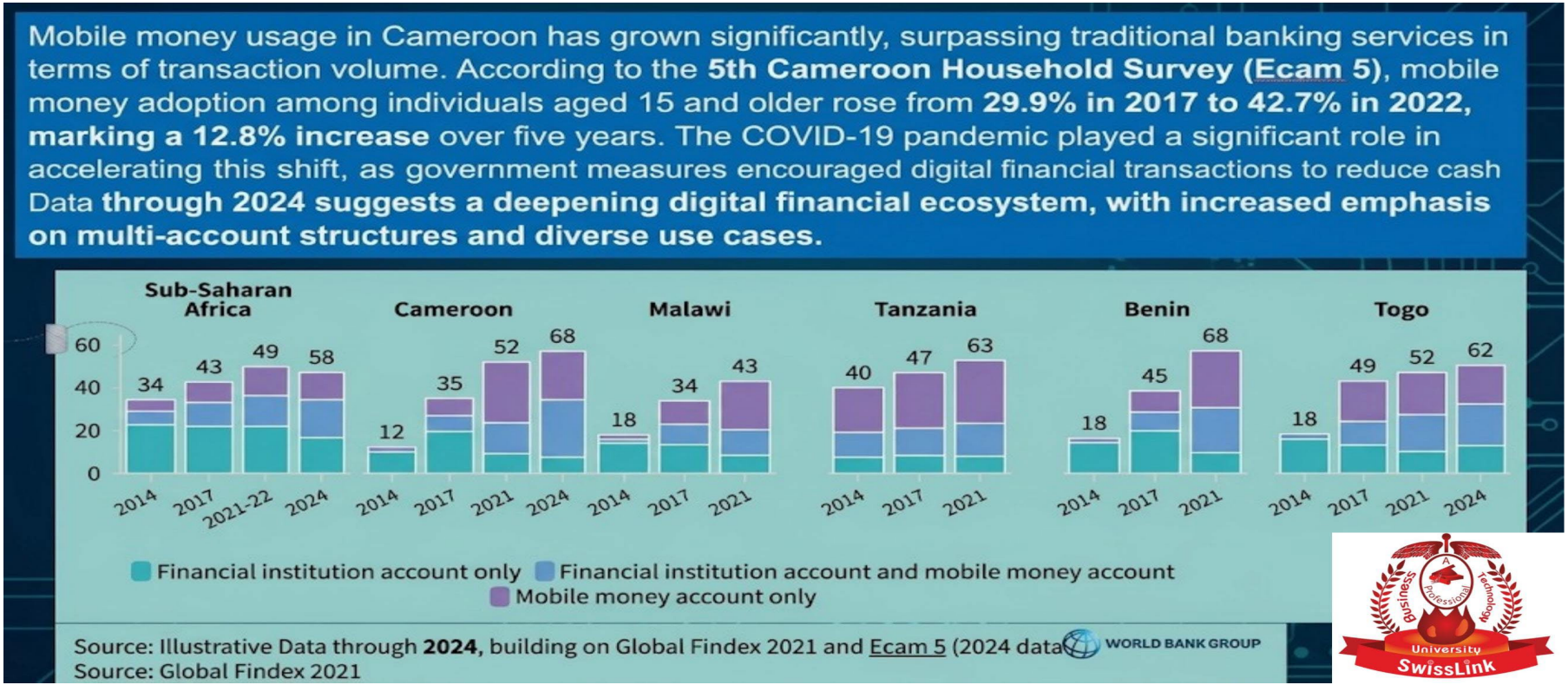
Sub-Saharan Africa is the world's fastest-growing mobile money region (GSMA, 2025). Rapid digitalisation increases the attack surface available to social engineers. With 74% of web traffic via mobile phones (Statista, 2024), mobile-first attacks — SMS fraud, fake apps, WhatsApp scams — are the dominant threat vector across the continent.

Key insight: Mobile money fraud in Africa increased 15% year-on-year in 2024. Social engineering is the primary delivery mechanism.

GSMA. (2025). State of the Industry Report on Mobile Money 2025. GSMA Intelligence. | ITU. (2024). Measuring digital development: Facts and figures 2024. ITU Publications. | Statista. (2024). Share of web traffic from mobile devices in Africa.

Mobile Money Adoption Growth Across Sub-Saharan Africa (2014–2024)

World Bank Global Findex data — financial account ownership as % of population aged 15+



World Bank. (2024). Global Findex Database 2024: Measuring financial inclusion and the fintech revolution. World Bank Group. https://globalfindex.worldbank.org | Ecam5 (5th Cameroon Household Survey). (2022). National Institute of Statistics of Cameroon.

What Is Social Engineering?

> *"Social engineering can be defined as the act of manipulating human beings, most often through psychological persuasion, to gain access to systems, data, or information the social engineer should not have."*

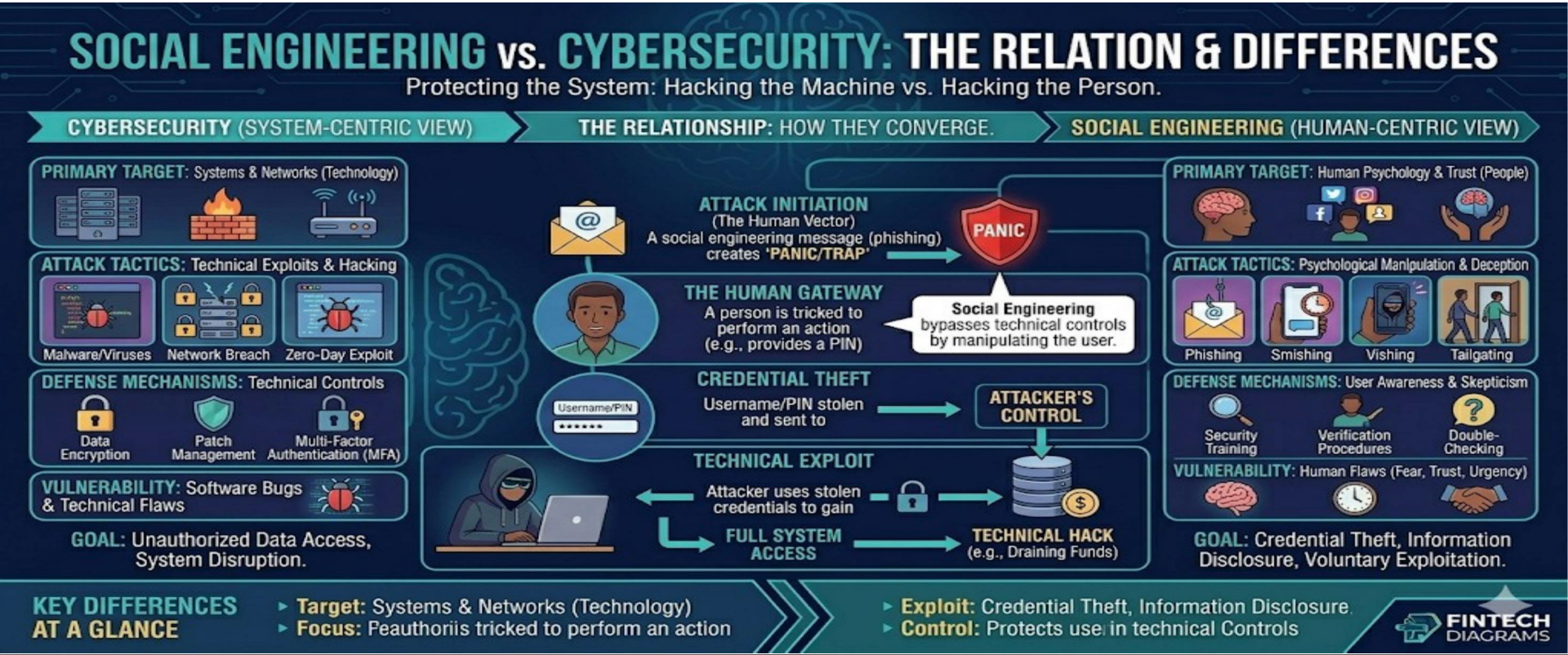
Attackers manipulate people into:

- Sharing passwords, PINs, or OTPs
- Sending money via mobile money or wire transfer
- Clicking dangerous links or opening infected attachments
- Granting remote access to devices or systems
- Trusting fake identities (impersonation)

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons. | Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. Behaviour & Information Technology, 32(10), 1014–1023. https://doi.org/10.1080/0144929X.2013.763860

Social Engineering vs. Cybersecurity: How They Converge

Social engineering bypasses technical controls by targeting the human gateway



Fintech Diagrams. (2026). Social engineering vs. cybersecurity: The relation and differences [Infographic]. | Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons.

The Human Factor: Why People, Not Technology, Are the Target

TECHNOLOGY ✓	HUMANS ✗
Can be patched with updates	Cannot be "patched"
Firewalls and encryption	Susceptible to emotions and pressure
Antivirus and EDR software	Extend trust to apparent authority
Multi-factor authentication	Respond to urgency without reflection
Intrusion detection systems	Fear consequences and retaliation
Network monitoring tools	Motivated by curiosity and reward

68% of all data breaches involved a non-malicious human element — social engineering or human error (Verizon, 2024)

Verizon. (2024). 2024 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/ | Workman, M. (2008). Wisecrackers. Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779

The Financial Cost of Social Engineering Attacks

$4.88M

Global avg. cost of a data breach (IBM, 2024)

68%

Breaches involving a human element (Verizon, 2024)

$46K

Median loss per ransomware breach (Verizon, 2024)

204

Average days to identify a breach (IBM, 2024)

Key findings from the leading annual breach reports:

Phishing is the #1 initial attack vector: present in 16% of all breaches analysed globally (IBM, 2024).

Social engineering via pretexting: remains the top social engineering incident pattern — used in Business Email Compromise (Verizon, 2024).

Median click time on phishing emails: is under 60 seconds — urgency bypasses critical thinking (Verizon, 2024).

Healthcare and financial sectors: face the highest breach costs globally, averaging $9.77M and $6.08M per incident (IBM, 2024).

IBM. (2024). Cost of a data breach report 2024. IBM Security. https://www.ibm.com/reports/data-breach | Verizon. (2024). 2024 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/

2

Cybersecurity Foundations

CIA Triad, threat landscape, and core concepts

The CIA Triad: Core Principles of Information Security

C

Confidentiality

Only authorised individuals may access information. Social engineering breaches confidentiality by tricking people into revealing passwords, PINs, or access credentials.

I

Integrity

Information must remain accurate and unaltered. Social engineers may modify data or intercept communications to corrupt records or misdirect transactions.

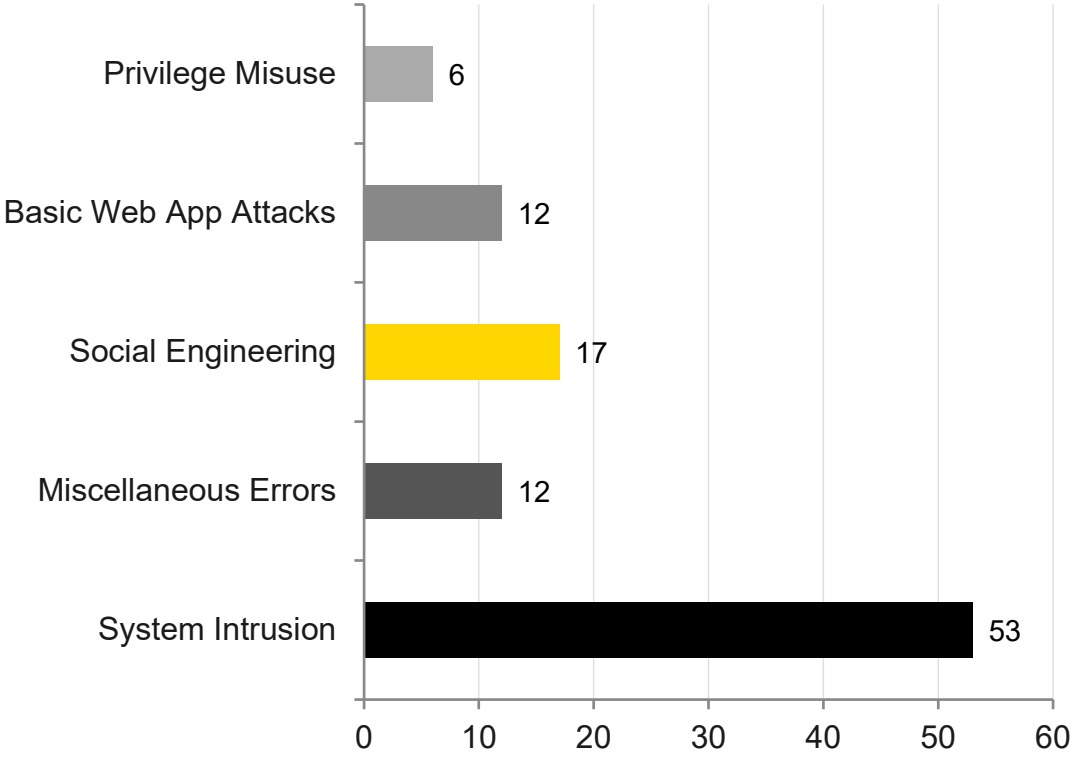
A

Availability

Systems and data must be accessible when legitimately needed. Ransomware delivered via social engineering disrupts availability, crippling operations.

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson. | NIST. (2024). Cybersecurity Framework v2.0. https://doi.org/10.6028/NIST.CSWP.29

Cybersecurity Threat Landscape: Top Patterns (Verizon DBIR, 2025)



Key Observations

- Social Engineering accounts for 17% of all confirmed breaches in 2025
- System Intrusion (53%) often begins with a social engineering initial access
- Phishing and pretexting remain the primary social engineering techniques
- Human error (Misc. Errors) contributes 12% of breaches independently
- Financial motivation drives the majority of social engineering attacks

Verizon. (2025). 2025 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

3

Attack Types & Techniques

Phishing, pretexting, baiting, mobile money fraud, and AI-powered attacks

Attack Type 1: Phishing and Its Variants

Phishing involves sending deceptive messages that appear to come from legitimate sources to harvest credentials, install malware, or initiate fraudulent transactions (Workman, 2008).

Spear Phishing	Targeted phishing using personal information about the victim (name, employer, role) to appear more credible
Whaling	Spear phishing directed specifically at senior executives or high-value targets (C-suite, government officials)
Smishing	Phishing delivered via SMS — 'Your account is suspended, click here to verify' — dominant vector in Africa
Vishing	Voice phishing via telephone — impersonating banks, MTC, government, or IT support departments
Clone Phishing	A legitimate email is copied and re-sent with malicious links or attachments substituted

Workman, M. (2008). Wisecrackers. Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779 | Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Attack Type 2: Pretexting — The Fabricated Scenario

Pretexting involves creating a fabricated scenario to manipulate a target. The attacker impersonates a trusted figure — IT support, a bank official, a government officer, or a colleague.

1	2	3	4	5
Research Target	**Build Pretext**	**Establish Trust**	**Extract Value**	**Exit & Exploit**
Collect info from LinkedIn, Facebook, company website (OSINT)	Craft believable scenario: 'I'm calling from your bank's fraud department'	Use specific personal details to appear legitimate and credible	Request passwords, OTPs, wire transfers, or remote access	Use obtained access, cover tracks — victim may not know for weeks

Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons. | Bullée, J. H., et al. (2018). Telematics and Informatics, 35(4), 1060–1079. https://doi.org/10.1016/j.tele.2017.09.012

Attack Types 3 & 4: Baiting and Quid Pro Quo

BAITING

Offers something enticing to lure victims into a trap. Exploits human curiosity and desire for reward.

- Free USB drive left in a car park or lobby
- 'You have won a prize!' pop-ups or SMS
- Free movie/software download links
- Fake job offer portals ('click to apply')
- Free public Wi-Fi hotspots used as traps

QUID PRO QUO

Offers a service in exchange for information. Exploits the principle of reciprocity.

- 'I'll fix your computer — just give me your password'
- Fake IT helpdesk calls offering support
- Survey 'rewards' requiring personal data
- Fake HR 'verification' calls
- Attacker helps then requests system access

Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins. | Workman, M. (2008). Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779

Attack Type 5: Mobile Money Fraud in Sub-Saharan Africa

Africa processed $1.1 trillion in mobile money transactions in 2024 (GSMA, 2025). Mobile money fraud is the fastest-growing form of social engineering in Namibia and the wider SADC region.

Fake Reversal Scam

Attacker claims to have mistakenly sent money and asks victim to reverse it. The original transaction is then cancelled, leaving the victim out of pocket.

Agent Impersonation

Caller claims to be an MTC or banking agent. States the victim's account is suspended and asks for a PIN or OTP to 'verify' identity.

Prize / Lottery SMS

Victim receives an SMS claiming they have won a prize. A link harvests personal data, or a premium-rate number is called, incurring charges.

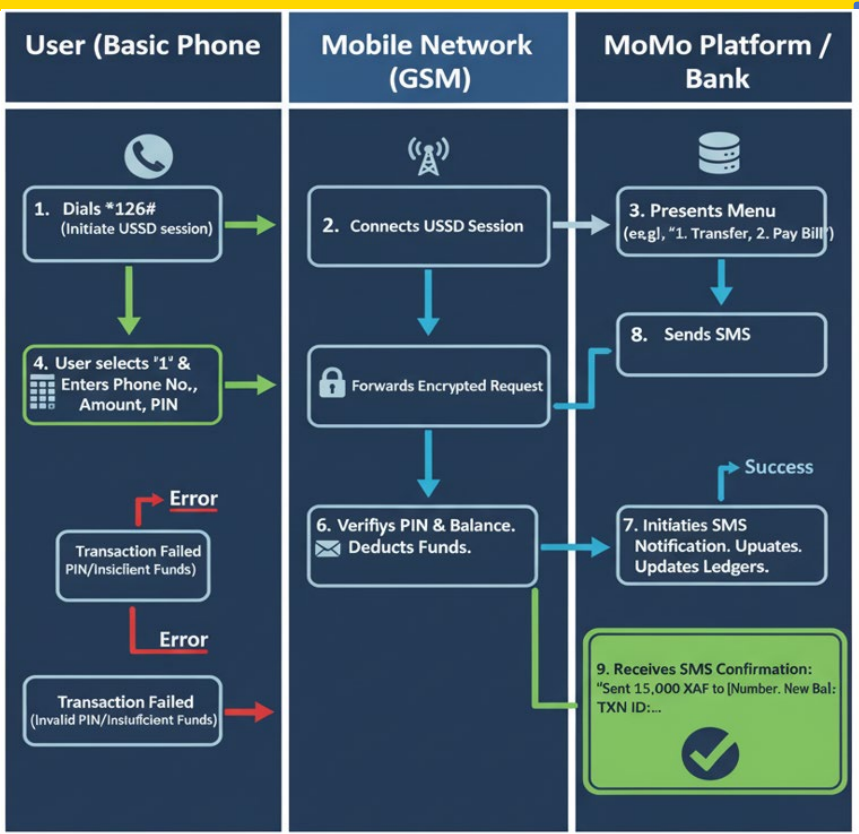
OTP Harvesting

Attacker initiates a login, then calls the victim pretending to be technical support, requesting the OTP sent to their phone.

GSMA. (2025). State of the Industry Report on Mobile Money 2025. https://www.gsma.com/sotir/ | Levi, M. (2017). Crime, Law and Social Change, 67(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

How Mobile Money Works: The USSD Transaction Flow

Understanding what attackers intercept — User → GSM Network → MoMo Platform → SMS Confirmation



The sequence of steps is as follows:

1.User (Basic Phone): Dials `*126#` (Initiate USSD session).

2.Mobile Network (GSM): Connects USSD Session.

3.MoMo Platform / Bank: Presents Menu (e.g., "1. Transfer, 2. Pay Bill").

4.User (Basic Phone): User selects "1" & Enters Phone No., Amount, PIN.

5.Mobile Network (GSM): Forwards Encrypted Request.

6.MoMo Platform / Bank: Verifys PIN & Balance. Deducts Funds.

1. If there's an error (e.g., "PIN/Insufficient Funds"), it goes back to the User with "Transaction Failed."

7.MoMo Platform / Bank: Initiates SMS Notification. Updates Ledgers.

1. If there's an error (e.g., "Invalid PIN/Insufficient Funds"), it goes back to the User with "Transaction Failed."

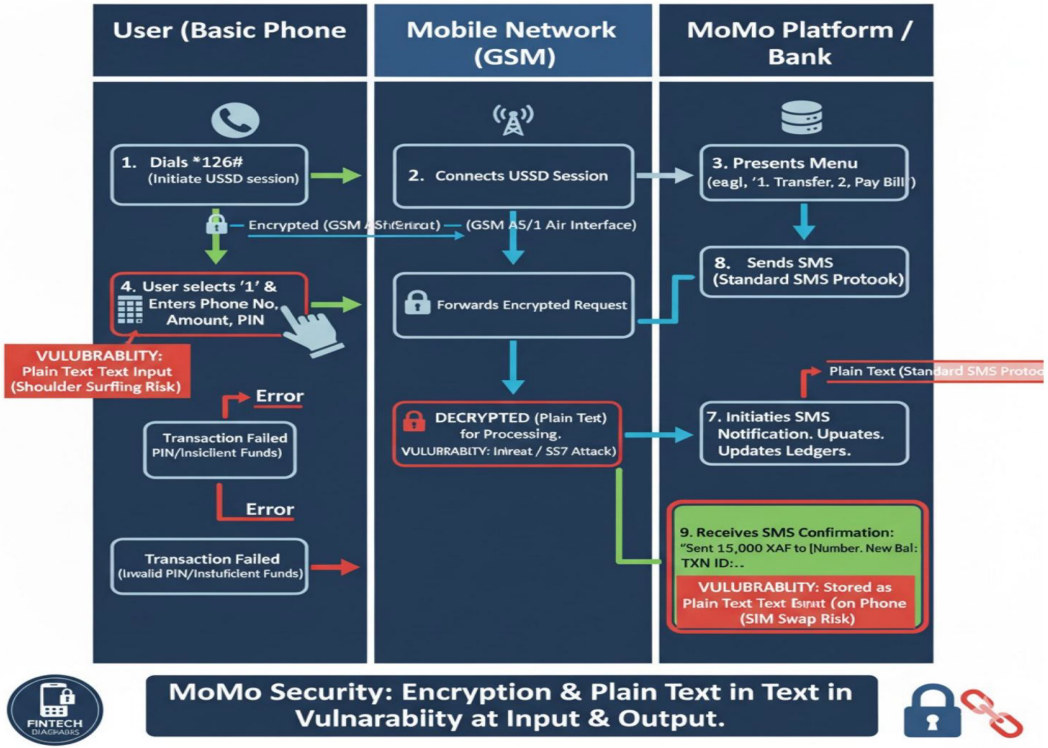
8.MoMo Platform / Bank: Sends SMS.

9.User (Basic Phone): Receives SMS Confirmation: "Sent 15,000 XAF to [Number]. New Bal: TXN ID:..."

Fintech Diagrams. (2026). MoMo transaction flow: USSD & SMS on GSM [Infographic]. | GSMA. (2025). State of the Industry Report on Mobile Money 2025. https://www.gsma.com/sotir/

Mobile Money Security: Where the Vulnerabilities Are

The same transaction flow — annotated with attack entry points used by social engineers



Breakdown of the encryption and plain text status at each stage:

1. User (Basic Phone) to Mobile Network (GSM) - USSD Session:

- **Step 1-4 (User Input):**
  - **VULNERABILITY: Plain Text Input (Shoulder Surfing Risk):** When the user dials *126# and enters their PIN/Amount, this information is **plain text on the phone screen** and visible to anyone nearby.
- **Step 4 to Mobile Network (GSM):**
  - **ENCRYPTED (GSM A5/1 Air Interface):** The USSD request (containing PIN, amount, recipient) is **encrypted** when it travels from the user's phone to the cell tower. This protects it from over-the-air eavesdropping.

2. Within Mobile Network (GSM) and MoMo Platform/Bank:

- **Step 5 (Forwards Encrypted Request):** The request remains encrypted as it's forwarded within the MNO's core network.
- **Step 6 (Processing):**
  - **DECRYPTED (Plain Text for Processing):** When the request reaches the MoMo Platform's servers for verification (PIN, balance, etc.), it must be **decrypted**. At this point, the data is **plain text** within the MNO's secure environment.
  - **VULNERABILITY: Insider Threat / SS7 Attack:** This is a point of vulnerability for sophisticated attacks or insider misconduct.

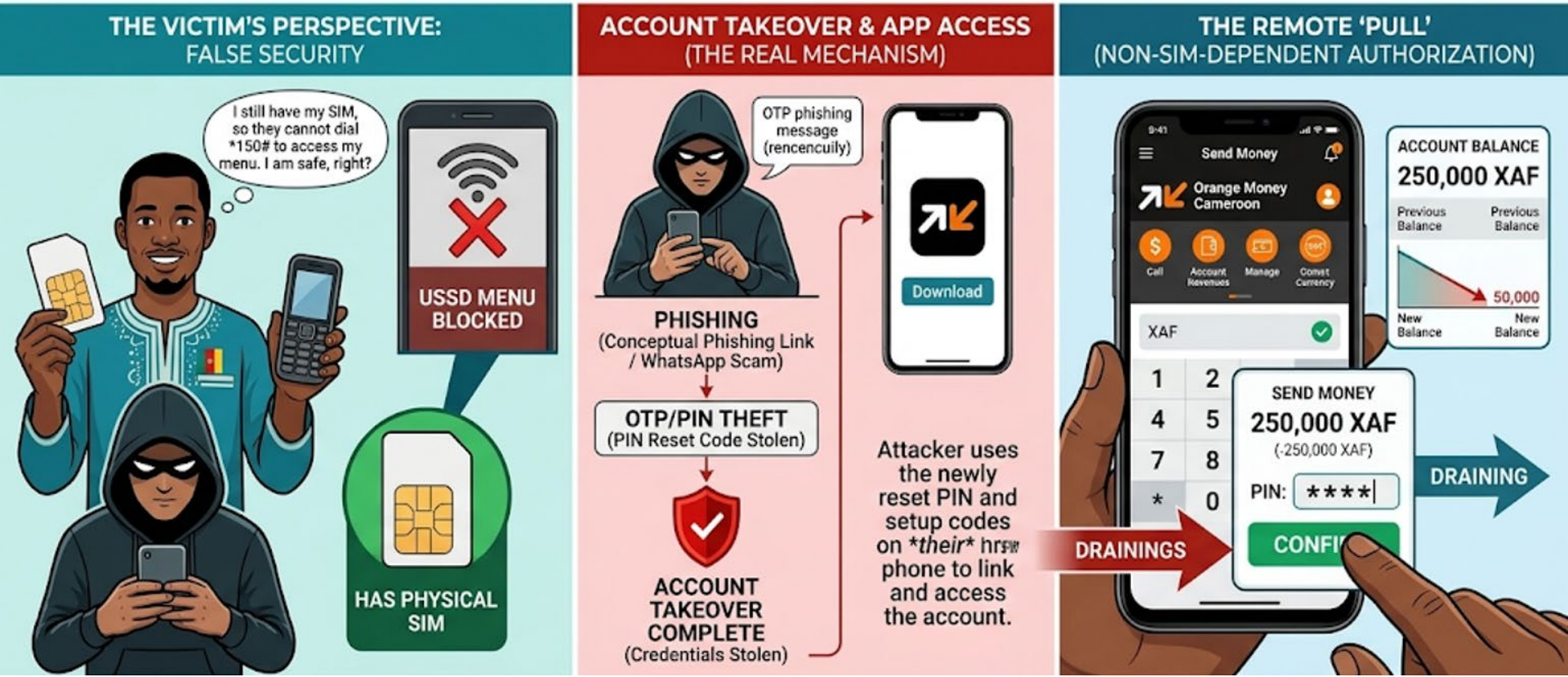
3. MoMo Platform/Bank to User (Basic Phone) - SMS Confirmation:

- **Step 7 (Initiates SMS Notification) & Step 8 (Sends SMS):**
  - **PLAIN TEXT (Standard SMS Protocol):** The SMS confirmation message generated by the MoMo Platform is sent as **plain text**. It is not encrypted end-to-end.
- **Step 9 (Receives SMS Confirmation):**
  - **PLAIN TEXT (Standard SMS Protocol):** The user receives the SMS, which is displayed as **plain text** on their phone.
  - **VULNERABILITY: Stored as Plain Text & SIM Swap Risk:** The SMS is stored as plain text on the phone and is easily readable if the phone is lost, stolen, or if a SIM swap attack occurs.

Fintech Diagrams. (2026). MoMo security: Encryption & plain text vulnerability at input & output [Infographic]. | Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons.

Account Takeover: Draining Without the SIM

The most dangerous misconception — 'I still have my SIM card, so I am safe'



Fintech Diagrams. (2026). Draining without the SIM: Attacker mechanisms [Infographic]. | GSMA. (2025). State of the Industry Report on Mobile Money 2025. https://www.gsma.com/sotir/

Attack Type 6: Physical Social Engineering

Social engineering is not exclusively digital. Physical attacks exploit human politeness, authority compliance, and environmental trust cues.

Tailgating / Piggybacking

Following an authorised person through a secured door by claiming to be a colleague, delivery person, or contractor. Exploits social obligation not to seem rude.

Shoulder Surfing

Observing someone enter a PIN, password, or sensitive data in a public space — ATMs, cyber cafés, airports. Especially relevant for mobile money users in shared spaces.

Dumpster Diving

Retrieving discarded documents containing passwords, account numbers, organisational charts, or employee details from bins or recycling.

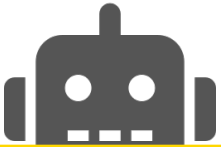
Impersonation

Posing as IT support, a delivery driver, a fire safety inspector, or a government official to gain physical access to premises or systems.

Mouton, F., et al. (2014). Computers & Security, 59, 186–209. https://doi.org/10.1016/j.cose.2016.03.004 | Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons.

Emerging Threat: AI-Powered Social Engineering (2024–2026)

Generative AI is amplifying social engineering at scale — enabling hyper-personalised phishing, synthetic voices, and real-time deepfake video. The 2025 Verizon DBIR documents a measurable rise in AI-assisted malicious emails.



Deepfake Voice (Vishing)

AI clones a known voice — a manager or CEO. Employee hears their boss authorising an urgent transfer. Used in verified fraud cases (CNN, 2024).

Deepfake Video Calls

Real-time AI face-swapping on video conferences. Arup lost US$25.6M when an employee wired funds after a fake video call with AI-generated executives (CNN, 2024).

AI-Generated Phishing

LLMs create grammatically perfect, culturally contextualised phishing emails at mass scale — removing the telltale signs of earlier attacks (Verizon, 2025).

Chatbot Impersonation

Fake customer-service chatbots harvest credentials when 'helping' users resolve account issues on fraudulent websites.

OSINT Automation

AI scrapes social media and public records to build detailed victim profiles used for targeted spear-phishing and pretexting.

AI Fraud Detection Bypass

Adversarial AI mimics legitimate transaction patterns, evading bank fraud-detection systems during mobile money attacks.

Verizon. (2025). 2025 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/ | CNN. (2024, May 16). Arup revealed as victim of $25 million deepfake scam. CNN Business. https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk

The Social Engineering Attack Lifecycle

From research to exploitation — how attacks unfold in practice across Africa

Fintech Diagrams. (2026). Social engineering: The psychological manipulation of people [Infographic]. | Mouton, F., et al. (2014). Computers & Security, 59, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Social Media as a Social Engineering Vector in Africa

WhatsApp and Facebook are the dominant platforms for social engineering attacks across Namibia and Sub-Saharan Africa, given their near-universal adoption for personal and financial communication.

Facebook / Instagram

- Fake profiles to build romantic relationships
- Cloned accounts to defraud contacts
- Fake marketplace buy/sell scams
- Phishing links via Messenger or DMs

WhatsApp

- 'Wrong number' romance and investment scams
- Group admin impersonation attacks
- Fake investment/crypto opportunity forwards
- Malware-laden forwarded files or links

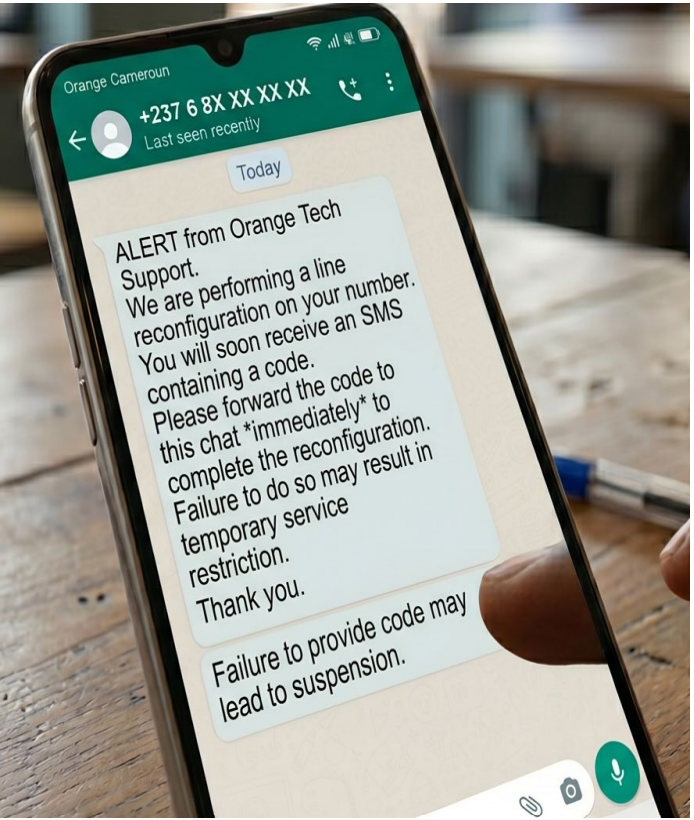
LinkedIn

- Fake recruiters extracting company information
- Spear phishing with professional context
- Credential harvesting via fake job portals
- Corporate intelligence gathering (OSINT)

Airehrour, D., et al. (2018). Information, 9(2), 37. https://doi.org/10.3390/info9020037 | DataReportal. (2025). Digital 2025: Global overview report. We Are Social & Kepios. https://datareportal.com

WhatsApp Impersonation: A Real OTP Harvesting Attack

Real screenshot — attacker impersonates 'Orange Cameroun' tech support via WhatsApp to steal OTP



1. **Platform:** Real telecom support will never use a personal WhatsApp chat with standard privacy settings
2. **The Request Itself:** Legitimate services will *never* ask you to read or forward an SMS verification code back to them via chat or over the phone. The standard security warning included in almost all OTP messages is "Do not share this code with anyone.“
3. **Threats:** Official customer support generally does not threaten immediate service suspension for refusing to manually provide security data over a chat application.

Fintech Diagrams. (2026). Draining without the SIM: WhatsApp OTP scam scenario [Infographic]. | Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins.

4

Psychology of Deception

Why intelligent people fall for social engineering attacks

Cialdini's Six Principles of Persuasion in Social Engineering

Authority

We comply with people who appear to be in charge. 'This is your bank manager calling to verify your account...'

Urgency/Scarcity

Panic reduces critical thinking. 'Your account will be suspended in 10 minutes if you do not act now!'

Social Proof

'Everyone in your department has already verified their credentials.' Exploits conformity bias.

Liking

We comply with people who flatter or befriend us. Attackers build rapport before striking.

Scarcity

'Only 3 spots remain — act now before the offer expires!' Creates artificial urgency.

Reciprocity

If someone does us a favour, we feel obligated to return it — exploited in quid pro quo attacks.

Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins. | Abroshan, H., et al. (2021). IEEE Access, 9, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Cognitive Biases That Increase Social Engineering Vulnerability

Optimism Bias	"It won't happen to me." Research shows individuals systematically underestimate their personal susceptibility to social engineering attacks relative to others.
Confirmation Bias	We seek and believe information that confirms existing beliefs. Attackers craft messages consistent with our expectations — an expected bank call, a familiar contact.
Automation Bias	We over-trust professional-looking technology and communications. Polished HTML emails or official-looking websites bypass critical scrutiny.
Familiarity Effect	Repeated exposure increases trust. Attackers contact targets multiple times before executing the attack, building familiarity progressively.
Status Quo Bias	We prefer to avoid action. When attackers create urgency ('act now or lose access'), victims make hasty decisions to restore the status quo.

Vishwanath, A., et al. (2018). Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483 | Workman, M. (2007). Information Systems Security, 16(6), 315–331. https://doi.org/10.1080/10658980701788165

Cultural and Contextual Factors in Namibia and Southern Africa

Social engineers adapt their attacks to exploit specific cultural norms and social dynamics. The following factors are documented as increasing susceptibility in sub-Saharan African contexts:

Deference to Authority

Strong cultural respect for elders, officials, and managers creates reluctance to question requests — even those that raise suspicion (Abroshan et al., 2021).

Community Trust (Ubuntu)

High communal trust reduces suspicion when attackers claim to be connected to one's community or family network.

Fear of Government

Messages purportedly from NAMRA, NamPol, or MTC generate compliance through fear rather than trust, bypassing critical assessment.

Digital Literacy Gaps

Newer internet and mobile money users may not recognise spoofed URLs, fraudulent app interfaces, or suspicious OTP requests.

Shared Device Usage

Use of shared smartphones or cyber cafés means that logged-in accounts may be accessible to multiple people and their attackers.

Financial Aspiration

Investment scams exploiting the genuine desire for economic advancement are highly effective across the region (Levi, 2017).

Abroshan, H., et al. (2021). IEEE Access, 9, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383 | Levi, M. (2017). Crime, Law and Social Change, 67(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

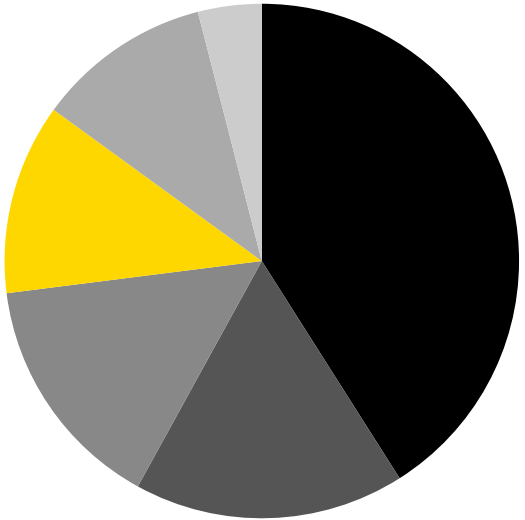
5

Case Studies

Verified attacks from Africa and globally — lessons learned

African Context: Cybercrime Statistics from Cameroon (ANTIC, 2023)

Cameroon's cybersecurity incident data is one of the most comprehensively published in francophone Africa and provides a relevant baseline for understanding the threat landscape across the SADC region.

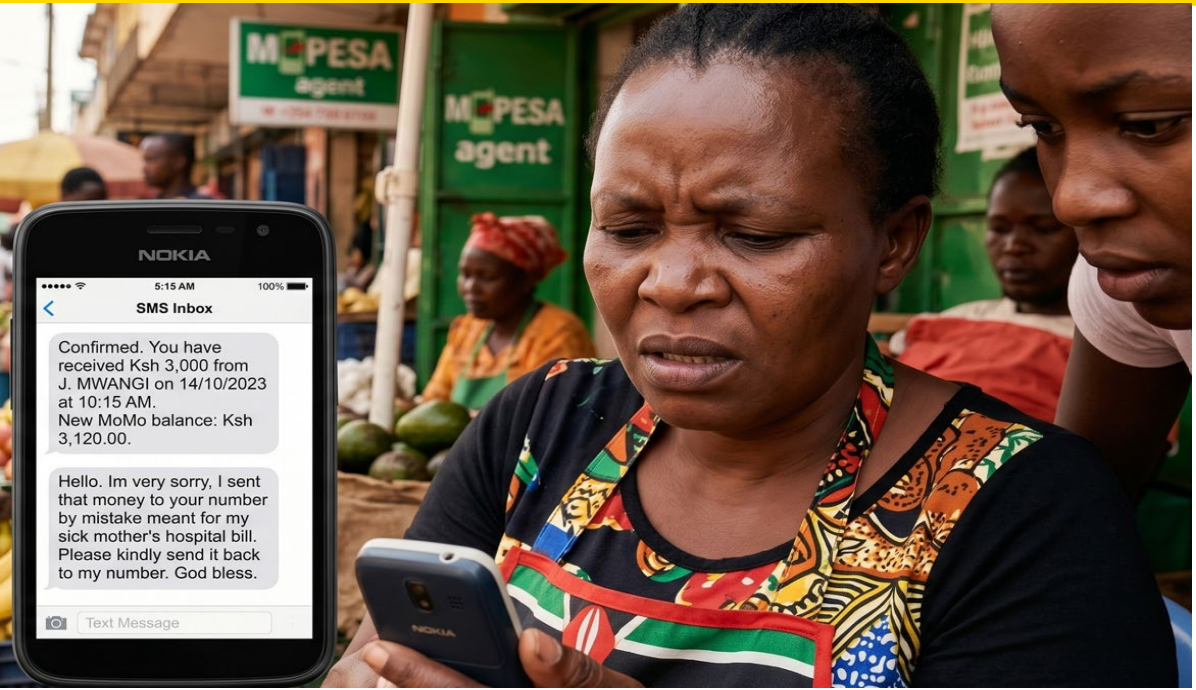


Key findings

- Scamming (41%) is the dominant cybercrime — driven by social engineering
- Social engineering underlies 4 of the 6 top incident categories
- Similar patterns are documented across Namibia, Botswana, and Zimbabwe
- Mobile money fraud is the primary financial attack channel in SADC countries
- WhatsApp-based scams grew significantly between 2021 and 2023 across the region

Agence Nationale des Technologies de l'Information et de la Communication (ANTIC). (2023). Rapport annuel sur la cybercriminalité au Cameroun 2023. Government of Cameroon. | ITU. (2024). Global cybersecurity index 2024. ITU Publications.

Case Study 1: The Mobile Money Reversal Scam — Africa



The Social Engineering Hook

1. Exploiting Urgency
2. Relying on Credential Trust
3. The Actual Theft

What Happened:
Victim receives a genuine-looking MoMo deposit. A follow-up message claims it was sent by mistake and requests a refund. Victim sends money back — the original deposit is reversed. Total loss = victim's own funds. Exploits reciprocity (Cialdini, 2007).

Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins. | GSMA. (2025). State of the Industry Report on Mobile Money 2025. https://www.gsma.com/sotir/

Case Study 2: Fake Bank Phishing Email Analysis

From: security@bankwindh0ek.com

Subject: ⚠ URGENT – Your account has been suspended

Dear Customer,

We have detected unusual login activity on your Bank Windhoek online banking account. Your account has been temporarily suspended for security reasons.

To restore access immediately, please verify your identity:

[RESTORE MY ACCOUNT NOW]

Failure to act within 24 hours will result in permanent account closure.

Bank Windhoek Security Team
Tel: +264 000 0000

Red Flags — What Makes This Phishing?

- Sender domain: 'bankwindh0ek' — zero replaces the letter 'o'
- Generic greeting: 'Dear Customer' — your bank knows your name
- Artificial urgency: '24-hour' deadline prevents rational thought
- Vague threat: 'unusual activity' with no specific details
- Call to action button — link leads to a spoofed website
- No official Bank Windhoek contact number or address
- No personalisation or account reference number shown

Action: Call your bank directly on their official number.

Vishwanath, A., et al. (2018). Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483 | ENISA. (2023). ENISA threat landscape 2023. https://www.enisa.europa.eu

Case Study 3: The Arup Deepfake Video Fraud (Hong Kong, 2024) — US$25.6 Million

Confirmed incident reported by Hong Kong Police and verified by Arup Group (CNN, 2024) | Largest documented AI-powered social engineering fraud globally at time of incident

What Happened:

A finance employee at Arup Group's Hong Kong office received an email purportedly from the UK-based CFO requesting a 'secret transaction.' Initially suspicious, the employee's doubts were dispelled when invited to a video conference call that appeared to include the CFO and several senior colleagues. All participants, except the victim, were AI-generated deepfakes created from publicly available corporate videos. The employee made 15 transfers totalling HK$200 million (≈US$25.6M) to five bank accounts. The fraud was discovered only when the employee subsequently contacted Arup's UK head office.

Social Engineering Principles Exploited:

- Authority: Deepfake CFO and senior colleagues made request appear legitimate
- Social Proof: Multiple 'colleagues' on call endorsed the transaction
- Trust Escalation: Initial phishing email + follow-up video call overcame initial suspicion
- Urgency: Framing as a 'secret transaction' requiring immediate action

CNN. (2024, May 16). Arup revealed as victim of $25 million deepfake scam. CNN Business. https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk | CNN. (2024, February 4). Finance worker pays out $25 million after video call with deepfake 'CFO'. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

Comparative Context: Switzerland vs. Namibia/Africa

CH Switzerland

- Advanced digital banking and QR payment infrastructure
- NCSC issues public phishing and fraud alerts
- Common attacks: phishing, fake bank calls, fake parcel SMS, QR code fraud
- Elderly targeted in credit card phishing campaigns
- Fake prize competitions used to harvest credentials
- High trust in digital systems increases automation bias

🌍 Namibia / Africa

- Rapid mobile money adoption — $1.1 trillion transacted in Africa (2024)
- NACSA and NAMPOL Cybercrime Unit provide national response
- Common attacks: mobile money fraud, WhatsApp scams, fake prizes, OTP harvesting
- Romance and investment scams exploiting financial aspiration
- Shared devices create multi-person exposure vectors
- Rapid digitalisation without proportional digital literacy growth

National Cyber Security Centre Switzerland (NCSC). (2024). NCSC annual report 2023/2024. https://www.ncsc.admin.ch | GSMA. (2025). State of the Industry Report on Mobile Money 2025. https://www.gsma.com/sotir/

Case Study 4: Romance Scam (Catfishing) — SADC Region

Romance scams cause severe financial and psychological harm. The FTC reports that romance scams cost US victims alone US$1.14 billion in 2023 — and the pattern is replicated across Africa at significant scale.

Contact	Grooming	Crisis	Extraction
Fake profile (Facebook, WhatsApp) contacts target. Presents as an overseas engineer, military officer, or aid worker with a compelling narrative.	Weeks or months of daily communication — compliments, emotional investment, shared plans. Victim develops genuine feelings and deep trust.	Attacker suddenly faces an emergency — customs delay, medical bill, visa complication. Requires money urgently to resolve the situation.	Victim transfers money via mobile money or Western Union. Multiple crises extend the fraud over months, draining the victim progressively.

Federal Trade Commission (FTC). (2024). Consumer Sentinel Network data book 2023. U.S. FTC. https://www.ftc.gov/reports/consumer-sentinel-network | Whitty, M. T. (2013). British Journal of Criminology, 53(4), 665–684. https://doi.org/10.1093/bjc/azt009

Case Study 5: Investment Fraud and Ponzi Schemes in Namibia

Social engineering is central to investment fraud. Attackers use persuasion, social proof, and urgency to overcome victims' critical thinking (Cialdini, 2007).

🚩 RED FLAGS — Fraudulent Scheme	✓ Legitimate Investment — What to Expect
✗ 'Guaranteed' returns of 50–300% per month	✓ Realistic returns (5–12% per annum for equities)
✗ Requires you to recruit others to earn	✓ Registered and regulated by NAMFISA or NSX
✗ Platform not registered with NAMFISA or NSX	✓ Company is transparent, verifiable, and audited
✗ Pressure to invest immediately before 'spots fill'	✓ No obligation to recruit others to earn returns
✗ Withdrawals require an advance 'release fee'	✓ Withdraw funds at any time without advance fees
✗ Testimonials feature strangers with luxury goods	✓ Risk is clearly disclosed in writing before investment

Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins. | Namibia Financial Institutions Supervisory Authority (NAMFISA). (2024). Annual report 2023/2024. https://www.namfisa.com.na

6

Defence & Best Practices

Evidence-based strategies for individuals and organisations

Recognising Red Flags: How to Identify a Social Engineering Attack

🚩 Urgency or Pressure

'Act NOW or your account will be permanently suspended!' Legitimate organisations allow time for verification.

🚩 Request for PINs or OTPs

Your bank, MTC, or any legitimate service will NEVER ask for your PIN, OTP, or password — under any circumstances.

🚩 Too Good to Be True

Prizes you did not enter, guaranteed investment returns of 50%+, free gifts requiring personal data — classic bait.

🚩 Suspicious Links or Domains

Hover over links before clicking. One character difference (0 vs o, rn vs m) is a spoofed domain. Check the full URL.

🚩 Impersonation

Verify identity independently. If in doubt, hang up and call back on the number shown on the official website.

🚩 Unusual or Irregular Requests

A manager requesting that you bypass normal procedures — purchase gift cards, disable security — is a major red flag.

ENISA. (2023). ENISA threat landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu | Schaab, A., et al. (2017). Information Systems Frontiers. https://doi.org/10.1007/s10796-019-09925-3

Personal Defence Strategies: Evidence-Based Countermeasures

Strong, Unique Passwords

12+ characters. Use a password manager (Bitwarden, 1Password). Never reuse passwords across accounts.

Protect Your OTPs and PINs

Never share a One-Time Password with anyone — including a person claiming to be from your bank or mobile operator.

Think Before You Click

Hover over links to check the real URL. Look for misspellings. If uncertain, navigate directly via the official app.

Verify via Known Channels

If a call or message seems suspicious, end it. Call back using the number shown on the organisation's official website.

Secure Your Connection

Avoid public Wi-Fi for mobile banking or sensitive accounts. Use a VPN if connecting in a public space.

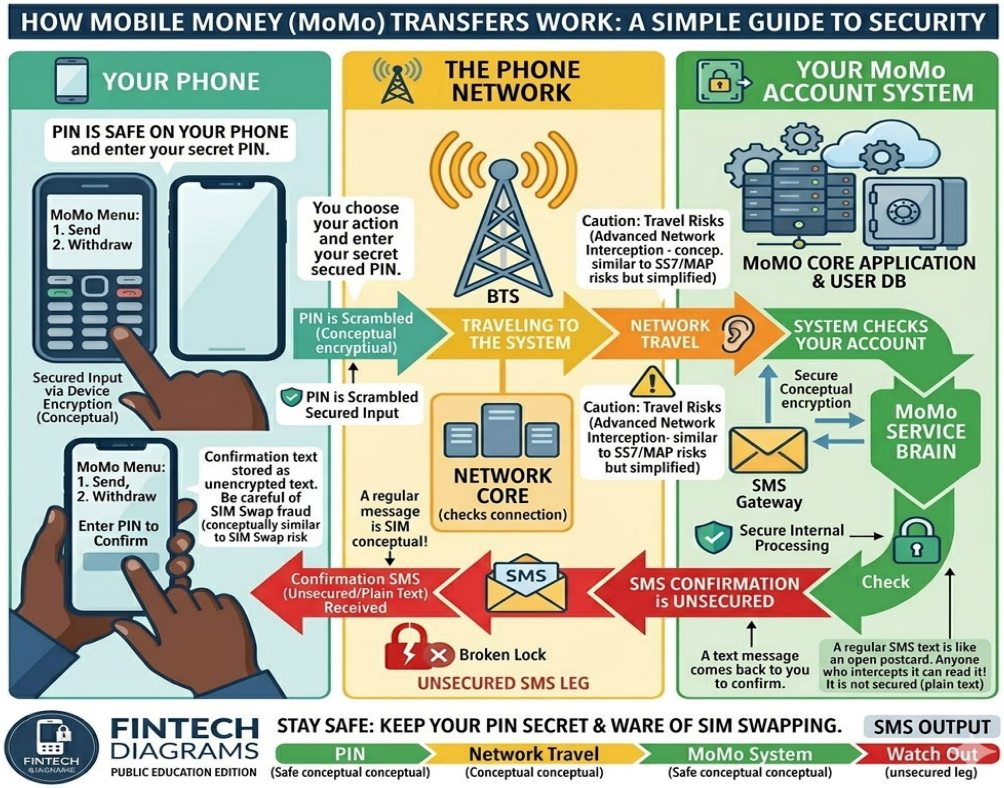
Limit Your Digital Footprint

Restrict what you share on social media — location, employer, and family details are used to craft spear-phishing attacks.

NIST. (2024). Cybersecurity Framework v2.0. https://doi.org/10.6028/NIST.CSWP.29 | Schneier, B. (2015). Secrets and lies: Digital security in a networked world (15th anniversary ed.). John Wiley & Sons.

Mobile Money Security at a Glance: Your Phone → Network → MoMo System

A simple guide — understanding where your PIN is safe and where the SMS leg is exposed



How to Stay Safe

1. KEEP YOUR PIN SECRET
2. BE AWARE OF SIM SWAP
3. Prevent SIM swapping with your carrier

Fintech Diagrams. (2026). How mobile money (MoMo) transfers work: A simple guide to security [Infographic]. | GSMA. (2025). State of the Industry Report on Mobile Money 2025. https://www.gsma.com/sotir/

Organisational Defence: A Layered Security Framework (NIST CSF v2.0)

PEOPLE

- Mandatory security awareness training (annual minimum)
- Phishing simulation exercises with feedback
- Clear incident reporting culture — blame-free environment
- Role-based access controls and least-privilege principle

PROCESS

- Two-person verification rule for financial transactions
- Documented incident response plan (tested regularly)
- Regular security risk assessments
- Clear communication and escalation protocols

TECHNOLOGY

- Email filtering and anti-phishing systems
- Multi-Factor Authentication (MFA) on all critical systems
- Endpoint detection and response (EDR) tools
- Network monitoring and Security Information and Event Management (SIEM)

NIST. (2024). Cybersecurity Framework v2.0. https://doi.org/10.6028/NIST.CSWP.29 | ISO/IEC. (2022). ISO/IEC 27001:2022. International Organisation for Standardisation.

Incident Response: What To Do If You Are Attacked

1

Stay Calm — Do Not Panic

Panic leads to further mistakes. Take a moment to assess the situation before taking any further action.

2

Stop Further Loss Immediately

Change passwords on affected accounts. Contact your bank or MTC to block or freeze suspicious transactions.

3

Preserve All Evidence

Screenshot everything — messages, emails, phone numbers, transaction IDs, and timestamps before deleting anything.

4

Report to Official Channels

Contact NAMPOL Cybercrime Unit and your bank or MTC immediately. Report to NACSA for national-level incidents.

5

Warn Your Contacts

If your account was compromised, notify your contacts — attackers frequently use hacked accounts to target the victim's network.

6

Review and Learn

Understand what happened. Identify which red flag was missed. Update your personal security practices.

NIST. (2012). Computer security incident handling guide (SP 800-61 Rev. 2). https://doi.org/10.6028/NIST.SP.800-61r2 | ISO/IEC. (2016). ISO/IEC 27035:2016 — Information security incident management. International Organisation for Standardisation.

Namibia: Official Cybercrime Reporting Channels

If you are a victim of social engineering, cybercrime, or financial fraud in Namibia, contact the following official bodies immediately:

NAMPOL Cybercrime Unit	Tel: +264 61 209 4111 | cybercrime@nampol.gov.na | Windhoek Police Headquarters
NACSA — Namibia Cybersecurity Authority	Website: nacsa.gov.na | National cyber incident reporting and coordination authority
Bank of Namibia (BoN)	Tel: +264 61 283 5111 | Report financial fraud, unlicensed investment schemes, and banking scams
NAMFISA	Tel: +264 61 290 5000 | Report pyramid schemes, fake investment platforms, and unregistered financial services
MTC Namibia Customer Care	Tel: 123 (free from MTC) | Report mobile money fraud, SIM swap fraud, and account compromise

Namibia Police Force (NAMPOL). (2024). Cybercrime unit. https://www.nampol.gov.na | NACSA. (2024). National cybersecurity strategy. https://nacsa.gov.na | NAMFISA. (2024). Consumer protection. https://www.namfisa.com.na

Building a Cybersecurity Culture: Your Role as Future Professionals

Research consistently shows that technical controls alone are insufficient. An organisation's security posture is only as strong as its least aware employee (Verizon, 2025). As UNAM graduates, you will shape this culture.

Train Consistently

Security awareness must be ongoing. Annual phishing simulations and briefings have demonstrated efficacy in reducing click-through rates (Verizon, 2024).

Build a Safe Reporting Culture

People must feel able to report mistakes without fear of punishment. A 'blame-free' reporting culture is a best-practice standard (ISO/IEC 27001, 2022).

Lead by Example

Leaders who follow the same security rules as everyone else drive compliance. Security privilege for executives creates dangerous precedents.

Update, Patch, and Review

Keep software, systems, and policies current. Social engineers exploit unpatched known vulnerabilities and outdated access controls.

Verizon. (2024). 2024 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/ | ISO/IEC. (2022). ISO/IEC 27001:2022. International Organisation for Standardisation.

7

Interactive Activities & Quiz

Test your knowledge — can you identify the attack?

🎯 Quiz: Spot the Scam — Scenario 1 (Smishing / OTP Harvesting)

📱 SMS Message Received — Read carefully and answer the questions below:

From: MTC-NAMIBIA

Dear Customer, your MTC Mobile Money wallet has been flagged for suspicious activity. To avoid permanent suspension, you must verify your account immediately by clicking the link below:

http://mtc-secure-namibia.com/verify

Your One-Time Password will be issued after verification. You have 2 hours to respond.

Discussion Questions:

1. What specific red flags can you identify in this SMS message?
2. Which of Cialdini's (2007) psychological principles does this message exploit?
3. What should you do if you receive this message on your phone?

Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins. | Vishwanath, A., et al. (2018). Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483

✅ Quiz Answer — Scenario 1: Smishing Analysis

Spoofed Domain:	mtc-secure-namibia.com is NOT the official MTC domain (mtc.com.na). A hyphenated look-alike domain is a classic phishing indicator.
Artificial Urgency:	'2 hours to respond' is designed to prevent the recipient from thinking critically or verifying the message with MTC directly.
Vague Threat:	'Flagged for suspicious activity' offers no specific details — a scare tactic that creates anxiety without substance.
OTP Pre-emption:	Mentioning that an OTP will be issued 'after verification' is designed to prime the victim to share it — the actual goal of the attack.
Generic Greeting:	MTC knows registered customers by name. 'Dear Customer' indicates a mass-sent fraudulent message, not a personalised legitimate alert.

Workman, M. (2008). Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779

🎯 Quiz: Spot the Scam — Scenario 2 (Vishing + Remote Access)

📞 Unsolicited Phone Call — Listen carefully:

"Good afternoon. Am I speaking with [Your Name]? This is James from the IT Support department at UNAM. We have detected a serious virus on your university computer account that is actively spreading to other students' accounts. We need to remotely access your computer immediately to contain it. Could you please open your browser and go to anydesk.com and download the remote access software? I can fix everything for you right now."

Discussion Questions:

1. What social engineering technique(s) are being used in this call?
2. What would happen if you downloaded AnyDesk and allowed access?
3. What is the appropriate response to this caller?
4. How would you verify whether this caller is legitimate or not?

Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons. | Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins.

✅ Quiz Answer — Scenario 2: Vishing + Remote Access Scam

This is a Tech Support Vishing combined with a Remote Access Scam — one of the most common scam types documented by consumer protection agencies globally (FTC, 2024).

Technique:	Pretexting + Vishing: A fabricated scenario (virus outbreak) delivered by voice call impersonating a trusted institution (UNAM IT Support).
Urgency Used:	'Actively spreading to other students' accounts' prevents the victim from pausing to verify. Panic drives compliance (Cialdini, 2007).
Real Goal:	AnyDesk gives the attacker FULL remote control of the device — file access, banking app access, credential theft, and malware installation.
Correct Response:	Hang up immediately. Call the official UNAM IT Help Desk using the number published on the unam.na website — never use a number provided by an unknown caller.

FTC. (2024). Consumer Sentinel Network data book 2023. https://www.ftc.gov/reports/consumer-sentinel-network | Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins.

Future Trends in Social Engineering: 2026–2030

Generative AI Phishing

LLMs produce grammatically perfect, hyper-personalised phishing at mass scale (Verizon, 2025).

Synthetic Identity Fraud

AI combines real and fabricated personal data to create convincing new identities for account fraud.

IoT-Based Social Engineering

Smart devices become vectors — 'your device has reported a security problem, click here.'

5G Attack Surface Growth

Faster, lower-latency networks enable real-time deepfakes in calls and more sophisticated mobile attacks.

Supply Chain Manipulation

Attackers target vendors and software suppliers to gain indirect access to larger organisations (Verizon, 2025).

Quantum Cryptographic Risk

Future quantum computers may compromise current public-key encryption, requiring post-quantum migration (NIST, 2024).

Verizon. (2025). 2025 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/ | NIST. (2024). Post-quantum cryptography standards. https://www.nist.gov/pqcrypto

Stay Safe. Stay Aware.

The Human Firewall starts with YOU.

Your 4 Actions Starting Today:

- Enable 2FA on all your accounts — today.
- Never share your PIN or OTP with anyone.
- Verify before you trust. Think before you click.
- Educate your family, friends, and colleagues.

Thank You!

Visual materials courtesy of Fintech Diagrams (2026). Used for educational purposes.

Key Takeaways

01	Social engineering exploits human psychology — not technology. The human remains the primary and most vulnerable attack target (Mitnick & Simon, 2002).
02	Attackers leverage Cialdini's (2007) persuasion principles — authority, urgency, social proof, liking, scarcity, and reciprocity — to bypass critical thinking.
03	Mobile money fraud is the fastest-growing threat in Namibia and the SADC region. Africa processed $1.1 trillion in mobile transactions in 2024 (GSMA, 2025).
04	Red flags: urgency, OTP or PIN requests, too-good-to-be-true offers, suspicious domains, and requests to bypass normal procedures.
05	Defence is layered: strong passwords, MFA, verification habits, security training, and a blame-free reporting culture (NIST, 2024; ISO/IEC 27001, 2022).
06	AI is amplifying attack sophistication. Deepfakes, AI-generated phishing, and autonomous OSINT tools are documented and growing threats (Verizon, 2025).
07	As future professionals, you have a responsibility to educate colleagues, family, and communities — and to embed security into the culture of your organisations.

Mitnick & Simon (2002). | Cialdini (2007). | GSMA (2025). | NIST (2024). | Verizon (2025). | See Bibliography slides for full references.

References — Part 1 of 2

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. IEEE Access, 9, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Agence Nationale des Technologies de l'Information et de la Communication (ANTIC). (2023). Rapport annuel sur la cybercriminalité au Cameroun 2023. Government of Cameroon.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs: Pitfalls and ongoing issues. Future Internet, 11(3), 73. https://doi.org/10.3390/fi11030073

Bullée, J. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks. Telematics and Informatics, 35(4), 1060–1079. https://doi.org/10.1016/j.tele.2017.09.012

Cialdini, R. B. (2007). Influence: The psychology of persuasion (rev. ed.). HarperCollins.

CNN. (2024, February 4). Finance worker pays out $25 million after video call with deepfake 'CFO'. CNN. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

CNN. (2024, May 16). Arup revealed as victim of $25 million deepfake scam involving Hong Kong employee. CNN Business. https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk

European Union Agency for Cybersecurity (ENISA). (2023). ENISA threat landscape 2023. ENISA. https://www.enisa.europa.eu

Federal Trade Commission (FTC). (2024). Consumer Sentinel Network data book 2023. U.S. FTC. https://www.ftc.gov/reports/consumer-sentinel-network

Fintech Diagrams. (2026). Mobile money & social engineering infographics [Series]. Fintech Diagrams Publications.

Florêncio, D., Herley, C., & Van Oorschot, P. C. (2014). Password portfolios and the finite-effort user. USENIX Security Symposium.

GSMA. (2024). Mobile economy Sub-Saharan Africa 2024. GSMA Intelligence. https://www.gsma.com/sotir/

References — Part 2 of 2

Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons.

IBM. (2024). Cost of a data breach report 2024. IBM Security. https://www.ibm.com/reports/data-breach

IBM. (2025). Cost of a data breach report 2025. IBM Security. https://www.ibm.com/reports/data-breach

International Telecommunication Union (ITU). (2024). Measuring digital development: Facts and figures 2024. ITU Publications. https://www.itu.int/itu-d/reports/statistics/

ISO/IEC. (2016). ISO/IEC 27035:2016 — Information technology — Information security incident management. International Organisation for Standardisation.

ISO/IEC. (2022). ISO/IEC 27001:2022 — Information security management systems — Requirements. International Organisation for Standardisation.

Levi, M. (2017). Assessing the trends, scale, and nature of economic cybercrimes. Crime, Law and Social Change, 67(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Namibia Financial Institutions Supervisory Authority (NAMFISA). (2024). Annual report 2023/2024. https://www.namfisa.com.na

National Cyber Security Centre Switzerland (NCSC). (2024). NCSC annual report 2023/2024. https://www.ncsc.admin.ch

NIST. (2012). Computer security incident handling guide (SP 800-61 Rev. 2). https://doi.org/10.6028/NIST.SP.800-61r2

NIST. (2024). Cybersecurity Framework v2.0. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. Behaviour & Information Technology, 32(10), 1014–1023. https://doi.org/10.1080/0144929X.2013.763860

Verizon. (2024). 2024 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Verizon. (2025). 2025 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Whitty, M. T. (2013). The scammers persuasive techniques model. British Journal of Criminology, 53(4), 665–684. https://doi.org/10.1093/bjc/azt009

Workman, M. (2007). Gaining access with social engineering. Information Systems Security, 16(6), 315–331. https://doi.org/10.1080/10658980701788165

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats. Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779

World Bank. (2024). Global Findex Database 2024. World Bank Group. https://globalfindex.worldbank.org