SYC Handbook: Secure Your World – Bridging the Gap

I. Executive Summary: The SYC Program Framework

1.1 Strategic Overview: The Train-the-Trainer Model for Digital Resilience

The "Secure Your World" (SYC) program is implemented through a decentralized Train-the-Trainer (TTT) approach, designed to cultivate a sustainable, community-led culture of digital safety. Digital adoption across Nigeria, largely propelled by mobile financial technologies and social platforms, has rapidly increased the digital exposure of citizens, outpacing the establishment of foundational security knowledge.[1] The SYC framework addresses this gap by positioning trusted community leaders—such as market association heads, religious figures, and local government representatives—as indispensable channels for knowledge transmission.

The primary guiding principle underpinning the program's structure is **localization**. The efficacy of digital literacy training, particularly when addressing adult populations who may possess low technical or formal literacy skills, is intrinsically linked to the trainer's capacity to communicate effectively using local languages, familiar analogies, and context-specific examples.[3] Community leaders are uniquely positioned to meet this requirement, as they possess established trust within their networks and a deep understanding of local context and prevailing risk factors.

To maintain the high quality and practical depth of instruction, the TTT sessions must adhere to stringent structural guidelines. The ideal capacity for these intensive sessions is limited, generally **not exceeding 15 participants**, ensuring that trainers receive personalized attention and sufficient opportunity for practical engagement.[3] The curriculum is structured to be modular and highly adaptable, serving the certified trainers as a comprehensive guide that can be customized to align with the specific knowledge levels and immediate concerns of their respective community audiences.[3] The overarching workshop spans one full day, encompassing a comprehensive theoretical foundation and intensive practical skills training, culminating in the provision of standardized, ready-to-use curriculum materials.

1.2 Community Leader Profile: Understanding the Target Trainer

The designated TTT audience consists of individuals characterized by established community influence and leadership roles. This demographic often exhibits varying levels of technical proficiency. Their typical digital engagement centers heavily on mobile commerce, peer-to-peer communication via platforms such as WhatsApp and SMS, and increasingly, interactions involving national identification processes, notably the Bank Verification Number (BVN) and National Identity Number (NIN) registration.[4]

Crucially, the motivation for these leaders to participate and subsequently teach is driven less by personal technological interest and more by a compelling need to ensure community stability and protect their members from financial and identity hardship. The curriculum is thus designed not just to convey technical information, but to deliver actionable solutions tailored to mitigating the highest-impact local threats, thereby empowering leaders to become true **champions of digital resilience**.

II. Foundation and Context: The Nigerian Digital Landscape (Part 1 Deep Dive)

The morning session (9:00 AM – 11:00 AM) focuses on establishing the urgent relevance of digital security and clarifying the instructional mandate entrusted to the community leaders.

2.1 Welcome and Introduction: Setting the Stage (15 Minutes)

The session commences with an **Icebreaker activity: "My Digital Life Snapshot."** This exercise strategically asks participants to share one positive and one challenging digital experience they or someone they know has encountered. The purpose of beginning with positive experiences (e.g., social connection, ease of mobile money transactions) is to establish an environment of empowerment and utility, rather than one driven solely by fear of threats. This approach immediately validates the workshop's relevance by confirming existing digital pain points and successes among the participants.

The initial talking points introduce the "Secure Your World" program's mission, which is centered on proactive empowerment. The discussion highlights the massive scale of digital adoption in Nigeria and underscores the resulting urgency for foundational digital safety knowledge.[1] The core message emphasizes the community leaders' pivotal role: they are not merely workshop attendees, but certified **champions** who possess the necessary trust and local context to serve as the critical infrastructure for disseminating life-saving knowledge throughout their networks. The day's agenda is then briefly outlined to set clear expectations for the intensive training ahead.

2.2 The Digital World & Local Risks (45 Minutes)

The training utilizes the "Secure Your World - Core Concepts" presentation (Slides 1-5) to provide a deep analysis of Nigeria's current mobile threat landscape. The discussion moves swiftly from general internet usage to specific, locally prevalent dangers.

In-Depth Analysis: Nigeria's Top Mobile Threats

The presentation dissects the evolution of **Scams and Fraud**. The foundational challenge, historically known as Advanced Fee Fraud (419), has migrated from traditional methods (postal letters, faxes, and emails) to mobile platforms.[6] The underlying psychological principles remain constant: the scammer leverages urgency, demands confidentiality, promises impossibly huge returns (e.g., millions of dollars from an international transfer or inheritance), and crucially, requests repeated "advance fees" to cover supposed transaction or government costs.[6] These schemes are now pervasive across mobile money applications, WhatsApp, and SMS, demonstrating the critical need for vigilance on handheld devices.[5]

A particularly critical local threat demanding focused attention is **BVN and Identity Fraud**. The Bank Verification Number (BVN) was introduced by the Central Bank of Nigeria (CBN) as a centralized biometric identifier intended to strengthen the banking system and enhance Know Your Customer (KYC) effectiveness.[4] However, this unique, 11-digit number linking all a customer's bank accounts has become a prime target for fraudsters. Scammers now move beyond simple cash theft; they engage in *identity compromise*. Evidence shows that fraudsters have successfully used fraudulent BVN enrollments (e.g., using static images instead of live biometric data) or leveraged stolen BVN details alongside other personal information (NIN, phone number) to open illicit loan accounts in the victim's name.[8] The implication is that financial loss is no longer the worst-case scenario. Instead, victims face long-term **credit damage and blacklisting**, crippling their future access to legitimate financial instruments, such as mortgages or credit.[9] The curriculum must therefore frame device and account security as essential protection for *future economic opportunity* and personal identity, not just current funds.

Privacy Threats are often precursors to these identity scams. The unwarranted sharing of personal identifying information—such as dates of birth, marital status, or specific family details—provides the social engineers with the necessary data points to execute believable impersonation scams and successfully compromise BVN records.

Finally, the threat of **Misinformation and Disinformation** is addressed. While often viewed as a political or social issue, the spread of unchecked rumors and false claims via platforms like WhatsApp can have tangible, real-world consequences, leading to economic panic or community discord. Device security is intrinsically linked to this, as compromised accounts can be weaponized to spread harmful content.

Following the presentation, participants engage in a **Group Discussion: "What are the biggest digital worries in your community right now?"** This mandatory activity requires the use of flip charts to visually document common concerns, which serves to validate the participants' real-world experiences and confirms that the curriculum directly addresses their needs. Active participation in this exercise aligns with proven TTT methods for adult learning.[3]

The identified threats necessitate a tailored approach to mitigation, summarized in the matrix below:

Table 1: Localized Digital Threat Matrix for Nigerian Communities (For Section 2.2)

Threat Type	**Common Community Examples (Localized)**	**Primary Impact**	**Core Mitigation Focus**
Advanced Fee Fraud (419)	Fake inheritance letters, "urgent" fees for international transfer promises, fake government procurement deals [6]	Immediate Financial Loss; Psychological distress	Skepticism, Verification, Never pay upfront fees
Identity & Financial Fraud	Obtaining BVN/NIN via impersonation; using static images for fraudulent bank/mobile money accounts [8]	Credit Damage, Identity Theft, Account Drain	Strong Accounts (2FA), Protect BVN/Identity documents
Account Takeover (ATO)	WhatsApp impersonation requests ("I changed my number, send urgent money to this new account") [5]	Social Disruption, Peer-to-Peer Financial Loss	Messaging Safely (Verify before transfer)
Device Loss/Theft	Stolen phone accessing mobile money wallets, social media profiles [10]	Privacy Breach, Financial Exposure	Physical Security (Screen Locks, Remote Wipe readiness)

2.3 What is Digital Security? (30 Minutes)

The next presentation segment (Slides 6-8) is dedicated to demystifying Digital Security. The goal is to move the concept out of the realm of abstract, expert-only knowledge and position it as a basic, practical skill relevant to every citizen.

Digital Security is defined simply as the comprehensive process of protecting one's personal information and identity when engaging online. The training stresses that this protection is universally accessible and necessary for everyone, regardless of technical background. A foundational understanding of why mobile phones are central to digital security in Nigeria is essential, given that they often host both financial transactions (mobile money) and identity keys (PINs, OTPs, BVN linkages).[2]

Technical Simplification: Encryption

A key challenge in digital literacy training is making technical concepts comprehensible. Encryption is introduced using highly accessible analogies. Encryption is the process that scrambles readable data (plaintext) into a secret code (ciphertext) that can only be unlocked with a unique digital key.[11]

The most effective simple explanation for community leaders is that encryption is like using a **"secure sealed package"** or **"putting a very strong curtain on your window"**.[12] When a user sends a message via a secure application like WhatsApp or visits a banking website (indicated by the 'https'), the communication is automatically locked with a secret code, ensuring that even if an unauthorized party intercepts the message during transit, they only obtain incomprehensible data.[13]

The session reinforces this concept with an **Activity: Pair & Share – "Explain Encryption to your neighbor like you're talking to a child."** This exercise forces trainers to immediately translate technical jargon into simple, local terms, ensuring they have internalized the concept clearly enough for future dissemination.

2.4 The "Train-the-Trainer" Approach (30 Minutes)

The final section of the morning (Slides 9-10) focuses on the core mandate: transforming participants into competent educators. This section lays out the pedagogical framework for sustainable knowledge transfer.

The overarching program goal is explicitly stated: participants are expected to become the teachers within their own networks. This model is based on the premise that local leaders are the most effective educators due to their inherent community trust, their ability to navigate linguistic nuances, and their contextual authority.[3] Their instruction will be more readily accepted and understood than that provided by external experts. The leaders’ role is defined as facilitating discussions, guiding practical, hands-on activities, and serving as an accessible resource for their community members.

The clear benefits for the community are articulated: empowered citizens, safer digital transactions, and stronger, more resilient local businesses.

The pedagogical blueprint relies heavily on proven methodologies for adult literacy in low-literacy settings, prioritizing **active teaching and learning** through interactive techniques such as role plays, discussion, and practical demonstrations.[3] Trainers must be reminded of the **localization imperative**: the necessity of delivering the curriculum in **local languages** to maximize comprehension and eliminate time wasted on translating complex ideas.[3]

The session concludes with a focused **Activity: Q&A – "What concerns do you have about teaching this to your community?"** This dedicated feedback loop allows facilitators to address anticipated challenges, such as the handling of complex technical troubleshooting (which is mitigated by providing Appendix E), and navigating low literacy among community members (addressed via the visual design principles in Appendix C).

III. Curriculum Mastery and Facilitation Skills (Part 2 Deep Dive)

The afternoon session (1:00 PM – 4:00 PM) transitions from theoretical context to practical curriculum delivery, focusing on mastering the instructional content and pedagogical skills required to host community sessions successfully.

3.1 Curriculum Deep Dive: Core Modules (1 Hour 30 Mins)

The curriculum is presented as a modular structure documented in the "Secure Your World - Community Session Guide" (Appendix B). This flexibility allows champions to deploy modules based on the most pressing needs of their audience.

Module 1: Protecting Your Phone's Door (Screen Locks, Updates)

This module emphasizes the critical link between physical device security and financial integrity. Mobile phones are the primary access points for mobile money wallets, and therefore, physical device protection serves as the first essential layer of defense against financial access following theft or loss.[10]

Talking Points focus on the importance of strong screen locks (PINs, complex patterns, or biometric authentication).[14] Trainers must understand and convey the necessity of software updates, explaining them simply as regular security **"patches"** that close vulnerabilities exploited by criminals.[14]

The core learning method is the **Activity: Hands-on Practice**. Participants are required to locate and demonstrate the process of setting up a secure screen lock on their own devices or on provided sample models. Trainers are instructed to advocate for fingerprints or strong PINs over simple, guessable patterns.

Module 2: Messaging Safely (WhatsApp, SMS)

Secure communication is covered, with a focus on End-to-End Encryption (E2E), simplified as a mechanism that allows only the two participants in a chat to read the sealed messages. The primary focus, however, is the identification of **social engineering scams** delivered via messaging platforms.

Talking Points highlight common red flags in suspicious messages [5]:

- **Urgency:** Messages demanding immediate action ("Act now or lose your account").
- **Too Good to be True:** Fake lotteries, prize money, or massive, unexpected inheritance promises.[6]
- **Unsolicited Requests:** Asking for confidential personal or financial details (like BVN or PINs).
- **Poor Language:** Obvious grammatical errors, typos, or strangely worded requests.[5]

The practical training culminates in the **Activity: Role Play – "Spot the SMS Scam."** Using localized scam scripts (Appendix D), pairs simulate receiving and analyzing suspicious messages, actively practicing the identification and articulation of the key red flags.[5]

Module 3: Strong Passwords & Accounts (Email, Social Media)

This module transitions from device security to account security, emphasizing the creation of strong access controls. Trainers are taught to advocate for **passphrases** (long, complex sentences) over simple passwords.

The most critical concept introduced here is **Two-Factor Authentication (2FA)**. Given its fundamental importance in mitigating identity theft and unauthorized financial access, 2FA must be explained using a clear, relatable analogy tailored to the local context.[16]

Technical Simplification: Two-Factor Authentication (2FA)

Two-Factor Authentication requires users to provide two independent pieces of evidence to prove their identity: something they *know* (the password/PIN) and something they *possess* (a temporary code sent to their trusted phone).[18]

- **Local Analogy:** Securing an important asset, like a bank safe, requires two security checks to gain entry. The first check is providing your required ID card or password (something you *know*). The second, unique check is providing a one-time pass-code delivered only to your trusted mobile number (something you *possess*). Both must align for the transaction to proceed.[2] This layered defense is essential protection against BVN fraud, where stolen identity details alone are insufficient to complete transactions if 2FA is enabled.[9]

The practical training includes the **Activity: Group Challenge – "Create the strongest, easiest-to-remember password."** Participants brainstorm and whiteboard secure passphrases, often incorporating familiar Nigerian cultural phrases or proverbs, ensuring memorability without compromising complexity.

Module 4: Spotting Online Scams (Phishing, Impersonation)

This module serves as the synthesis of all previous lessons, focusing on recognizing the deceptive tactics of fraudsters. The discussion covers the mechanics of phishing and impersonation, continually linking them back to the psychological hooks—greed, fear, and urgency—that are hallmarks of the Advanced Fee Fraud model.[6]

A central teaching point is the consistency of fraud: nearly all Nigerian fraud schemes rely on the victim providing an advance fee or confidential information *before* receiving the promised reward or service.[6] This knowledge provides community members with a reliable red flag for nearly all types of mobile solicitations.

The **Activity: "Is it Real?"** requires participants to analyze visual examples of fake emails, WhatsApp messages, and SMS texts (Appendix D). The participants use the established red flags (urgency, poor grammar, unsolicited links, fee requests) to vote on whether the communication is genuine or a scam.[5]

Table 2: Simplified Analogies for Core Digital Security Concepts

Technical Concept	Simple Definition for Community Leaders	Local Analogy (Nigerian Context)
Encryption (E2E)	Scrambling your message so only the intended recipient can read it, even if someone spies on the connection.	A secure, sealed courier package that only the person with the special key (on their phone) can open.[11]
Strong Password	A long phrase, difficult to guess, using different types of characters.	The strong lock on your market stall; weak ones break easily. Use a complex sequence, not just the name of your child.
Two-Factor Authentication (2FA)	Requiring two separate pieces of proof to access an account (e.g., password + code).	Having two security checks to enter the bank: the guard checks your ID card (password), and the teller

		asks for a unique, one-time pass-code delivered to your trusted mobile number (OTP).[16]
Software Updates	Small, regular fixes that close security holes and vulnerabilities.	Patches or repairs you put on your roof or fence after a rainstorm or intrusion attempt, ensuring the house remains secure.

3.2 Facilitation Skills for Community Leaders (45 mins)

Teaching fundamental digital safety concepts requires highly specialized communication techniques, particularly when addressing low-literacy adult audiences.

Talking Points emphasize the necessity of **Simple Language**, specifically instructing trainers to avoid technical jargon entirely and instead use the local analogies detailed in Table 2. Trainers are positioned as **facilitators, not lecturers**, meaning their primary task is to encourage participation, ask open-ended questions, and actively listen, ensuring that community members guide the learning process.[3] The training stresses the pedagogical effectiveness of **Demonstration** (showing, not just telling), and highlights the importance of **Creating a Safe Space** where participants feel comfortable admitting ignorance or reporting past victimization without fear of judgment.

The ability of a facilitator to simplify complex concepts and maintain conversational confidence directly influences the retention and application of knowledge by the end-user. Therefore, the **Activity: "Practice Teaching"** is the most critical quality gate in the TTT session. Participants, working in small groups, must select one core module concept (e.g., 2FA or Screen Locks) and practice explaining it to their peers for five minutes, using only simple language and local context. This activity acts as a direct, short-term assessment of learning outcomes (Kirkpatrick Level 2) [19], ensuring that the certified champions are competent in simplification and contextual accuracy before they deploy the curriculum in their communities.

3.3 Resources, Incident Response, and Next Steps (45 mins)

This section ensures operational readiness and provides clear pathways for support and action following an incident.

Immediate Incident Response Protocols

The community leaders must be trained on a clear, memorizable sequence of immediate actions to take if a mobile money or bank account is suspected of being compromised or hacked:

1. **Stop the Bleeding:** The paramount first step is to immediately contact the victim's bank or Mobile Network Operator (MNO) fraud department to freeze the account, cancel cards, and prevent further financial drain.[21]
2. **Containment:** If login access remains, the victim must urgently change all associated passwords and PINs immediately.[23]
3. **Audit:** The victim must review all recent transactions, payees, and direct debits for unfamiliar activity.[21] Given the risk of BVN fraud, victims must be advised to monitor their credit report for fraudulently acquired loans.[9]

Formal Reporting Mechanisms

Champions must be equipped with verified routes for escalating serious cybercrime. The program directs users to the official state mechanism: the **Nigeria Police Force National Cybercrime Centre (NPF-NCCC)**. The specific, actionable details provided in Appendix F include:

- **Reporting Portal:** Accessible via https://nccc.npf.gov.ng/ereport/signin.[24]
- **Support Channels:** Direct contacts including phone (+2347078489293), email (support@nccc.npf.gov.ng), and WhatsApp (+2347078489293).[24] These mechanisms cover reporting banking fraud, identity theft, phishing, and other cybercrime-related offenses.

Certification and Sustainability

The sustainability of the SYC program relies on consistent tracking and reward. Participants are informed that to receive the official "Digital Champion" certificate, they must report their community sessions back to DNS Africa using the standardized form provided in Appendix G. This process links action directly to recognition and establishes an auditable metric for program reach.

The final **Activity: "My First Session Plan,"** requires participants to briefly outline their implementation strategy, committing to an initial session date, location, and target audience. This commitment serves as an initial accountability measure and provides DNS Africa with essential short-term output data for program monitoring.[20]

IV. Sustainability, Impact, and Evaluation Framework

The SYC program is built on the principle that impact must be tracked far beyond the initial training day. A multi-level, multi-method monitoring and evaluation (M&E) framework is necessary to assess program success, tracking short-term outputs, medium-term behavioral changes, and long-term societal resilience.[20]

4.1 Measuring Success in the Community

The success metrics are categorized according to the expected time horizon for results:

Short-Term Indicators (Outputs, 1-2 Years): These metrics quantify immediate deliverables and knowledge acquisition.

- **Trainer Activity:** The total number of community sessions hosted by certified champions, reported quarterly using Appendix G.
- **Reach:** The total number of unique community members trained, with demographic data collected to track inclusivity.[20]
- **Knowledge Gain:** Assessed via mandatory post-session surveys distributed by the champion, measuring self-reported change in knowledge and digital skills among community participants.[19]

Medium-Term Indicators (Behavioral Change, 3-5 Years): These metrics assess the practical application of learned security principles.

- **Application Rate:** Observed adoption of core practices, such as the mandatory use of Two-Factor Authentication (2FA) for mobile money accounts and adherence to strict BVN sharing protocols. This requires qualitative tracking through key informant interviews with champions and community members.[20]
- **Risk Reduction:** Tracking changes in the nature of reported incidents. A successful program should result in a measurable decline in reports of *successful* fraud and an increase in reports of *identified and prevented* fraud attempts, indicating improved community vigilance.

Long-Term Indicators (Societal/Organizational Impact, 5+ Years): These indicators assess the creation of a self-sustaining security culture.

- **Cultural Shift:** Tracking institutional and organizational changes within the community, such as market associations mandating 2FA use for all digital transactions among members, or religious groups incorporating digital safety tips into public announcements.
- **Sustainability Assessment:** Evaluation of the continued operation of local digital security training sessions without the necessity of direct intervention or funding from DNS Africa, indicating that the knowledge transfer model has become self-sustaining.[20]

The most effective measure of success is the verifiable reduction in successful local cybercrime. By requiring champions to meticulously log incidents of fraud prevention or successful reporting to the NPF-NCCC through Appendix G, the program creates a crucial link between localized training activities and quantifiable improvements in community resilience.

4.2 Long-Term Support Infrastructure

To ensure the sustained impact of the TTT model, a robust support infrastructure is provided. DNS Africa commits to providing ongoing support and curricular resources through centralized contact channels listed in Appendix F. The "Digital Champion" certification process provides a verifiable credential and establishes a formal, managed network of committed trainers.

Clear escalation protocols are essential:

- **Level 1 Support:** Basic technical and troubleshooting queries (e.g., slow phone, battery drain) are first addressed by the Digital Champion using Appendix E (Troubleshooting FAQ).
- **Level 2 Support (Programmatic):** Questions regarding curriculum content, pedagogy, or resource replenishment are directed to DNS Africa Support via email or dedicated WhatsApp channels (Appendix F).
- **Level 3 Support (Criminal):** Reporting of serious cybercrime, banking fraud, identity theft, or active threats is immediately escalated to the NPF National Cybercrime Centre (NPF-NCCC) via the provided reporting methods.[24]

V. Appendices: Community Leader Resource Package (TTT Deliverables)

The appendices form the standardized, replicable kit necessary for scaling the "Secure Your World" program and ensuring content fidelity across all deployments.

Appendix A: "Secure Your World - Core Concepts" Presentation Slides

This resource contains the necessary visual aids (Slides 1-10) for community champions. The design emphasizes minimal text, high-contrast visuals, and heavy reliance on simple, memorable icons. Crucially, the accompanying trainer notes include the exact, simplified scripts and local analogies (as detailed in Table 2) to standardize the delivery of complex concepts and guarantee clear communication.

Appendix B: "Secure Your World - Community Session Guide"

This guide is the instructional script for the champions. It translates the TTT content into four streamlined, 30-minute modules designed for rapid deployment and maximum impact within community settings. The format uses clear, step-by-step instructions, including mandatory warm-up discussions and concluding, action-oriented activities suitable for low-literacy adult environments.[3]

Appendix C: Handout Templates for Community Participants (Visual Takeaways)

These handouts are designed specifically for audiences with potentially low digital or formal literacy, ensuring the message is retained visually.

Design Imperatives for Low-Literacy Audiences:

1. **Icon Reliance:** Security messages are conveyed primarily through universal, repeatable icons (e.g., locks, shields, traffic lights) to minimize dependence on reading skills.[27]
2. **Font and Layout:** A large, clean font (minimum 16px effective size) is mandated. The layout employs generous white space, clear grouping of related content (e.g., "Account Security" section), and reading lines maintained at an optimal length (45-75 characters) to promote comfortable reading.[28]
3. **Jargon Avoidance:** All technical terms are strictly prohibited. Substitutes such as "Secret Code" (for Encryption) or "Extra Check" (for 2FA) are used.[27]
4. **Action Orientation:** Content focuses exclusively on prescriptive instructions ("What to DO"), such as the immediate steps after spotting a scam, rather than theoretical explanations ("What it IS").

Appendix D: Sample SMS/Email Scams for "Is it Real?" Activity

This appendix provides necessary, localized content for simulation and role-playing activities, enabling community members to practice identifying fraud in a safe environment. Examples include:

- A classic 419 scheme, such as a message promising a large international fund transfer requiring an upfront "transfer tax" or "clearance fee".[6]
- An urgency-based BVN scam, such as a text claiming the recipient's bank account has been suspended due to an expired BVN, demanding they call an untrusted number or click an unauthorized link immediately.[9]
- A social engineering attempt via WhatsApp from an impersonated contact asking for urgent mobile money transfers due to an unforeseen emergency.

Appendix E: Troubleshooting FAQ for Common Mobile Security Issues

This document is essential for providing Level 1 technical support, empowering champions to address basic, common concerns without escalating to DNS Africa.

- **Symptom 1: Slow performance, rapid battery drain, or unexpected high data usage.**
  - **Solution:** Advise users to check for newly installed, untrusted applications and uninstall them.[30] Instruct Android users to run Google Play Protect and check for pre-installed anti-malware protection (e.g., Samsung Knox/Device Care).[32]
- **Symptom 2: Excessive pop-up advertisements.**
  - **Solution:** Instruct users to review app permissions, specifically revoking permissions for apps that "draw over other apps," which often allows malicious overlays.
- **Symptom 3: Account locked or inaccessible (suspected Account Takeover).**
  - **Solution:** Champion guides the victim through the immediate Incident Response Protocol (Section 3.3).

Appendix F: Contact Information for DNS Africa Support & Reporting

Digital Crime

This appendix centralizes all necessary contact information for support and crime reporting:

- DNS Africa Support Channels (dedicated contact methods for certified trainers).
- Official National Cybercrime Reporting (NPF-NCCC) details, including the direct reporting portal URL (https://nccc.npf.gov.ng/ereport/signin), phone numbers, and the official WhatsApp support line.[24]
- A template for listing local bank fraud hotlines and emergency numbers.

Appendix G: Digital Champion Reporting Form

This form is the mandatory mechanism for accountability and sustainability tracking. It requires fields necessary for M&E:

- Session metrics (Date, Location, Modules Covered, Number of Attendees/Demographics).
- Qualitative Feedback (e.g., What was the most common community concern raised?).
- **Impact Log:** Crucially, this section requires the champion to document specific instances where a participant reported a recent scam, successfully prevented a fraud attempt, or formally reported a crime to the NPF-NCCC after receiving the training. This information directly measures the medium-term behavioral change and the program's success in building community resilience.[20]

VI. Conclusion and Strategic Recommendations

The "Secure Your World" TTT Handbook provides a foundational, highly contextualized curriculum designed to meet the immediate security needs of Nigerian communities by leveraging existing social trust structures. The strategic choice to focus on community leaders as champions guarantees maximum reach and adaptation potential, vital for effective digital literacy delivery to diverse audiences.[3]

The analysis confirms that contemporary digital threats in Nigeria have escalated beyond simple financial loss to critical issues of **identity compromise and long-term economic exclusion** due to pervasive BVN-related fraud.[8] Consequently, the curriculum prioritizes identity-based mitigation strategies, specifically emphasizing the necessity of strong authentication (2FA) and detailed incident response protocols.

Strategic Recommendations:

1. **Mandate Analogical Mastery:** Ensure rigorous adherence to the "Practice Teaching" activity (Section 3.2), confirming that all champions can translate technical concepts (Encryption, 2FA) into simple, locally understood analogies (Table 2). This is the highest leverage point for ensuring knowledge retention among community participants.
2. **Sustain Accountability through Reporting:** Treat Appendix G not merely as an administrative task, but as the central tool for program management. Continuous

monitoring of the "Impact Log" within Appendix G will allow DNS Africa to track the quantifiable reduction in *successful* fraud events across the network, confirming the efficacy of the TTT investment.

3. **Continuous Resource Review:** Given the rapid evolution of mobile fraud tactics (e.g., WhatsApp scams, new BVN exploits), the content of Appendix D (Scam Examples) and Appendix E (Troubleshooting) must be reviewed and updated semi-annually. This maintains the program's relevance and supports the champions as they encounter emerging threats.

Works cited

1. Nigeria's Cybersecurity Outlook 2025 - Deloitte, accessed on October 7, 2025, https://www.deloitte.com/ng/en/services/consulting-risk/perspectives/Nigerias-cybersecurity-landscape-in-2025.html
2. (PDF) Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures - ResearchGate, accessed on October 7, 2025, https://www.researchgate.net/publication/344366463_Two-Factor_Authentication_Scheme_for_Mobile_Money_A_Review_of_Threat_Models_and_Countermeasures
3. TRAINER'S MANUAL DIGITAL LITERACY TRAINING TOOLKIT - NET, accessed on October 7, 2025, https://www.uncdf.org/Download/AdminFileWithFilename?id=19307&cultureId=127&filename=digital-litracy-trainers-implementation-guide---final-pdfpdf
4. BVN | Central Bank of Nigeria, accessed on October 7, 2025, https://www.cbn.gov.ng/PaymentsSystem/BVN.html
5. About suspicious messages and scams | WhatsApp Help Center, accessed on October 7, 2025, https://faq.whatsapp.com/2286952358121083
6. Nigerian Money Transfer Scams Prevention at NC DOJ, accessed on October 7, 2025, https://ncdoj.gov/protecting-consumers/sweepstakes-and-prizes/nigerian-money-transfer-scams/
7. Nigerian Fraud Scams | Georgia Attorney General's Consumer Protection Division, accessed on October 7, 2025, https://consumer.georgia.gov/consumer-topics/nigerian-fraud-scams
8. Lack of liveness detection costs Nigeria's financial institutions millions of Naira in fraud, accessed on October 7, 2025, https://www.biometricupdate.com/202503/lack-of-liveness-detection-costs-nigerias-financial-institutions-millions-of-naira-in-fraud
9. I was scammed with my BVN. Will it affect my credit report? - Tendar, accessed on October 7, 2025, https://www.tendar.co/blog/i-was-scammed-with-my-bvn-will-it-affect-my-credit-report
10. What Is Mobile Security? Threats and Prevention | Fortinet, accessed on October 7, 2025, https://www.fortinet.com/resources/cyberglossary/mobile-security
11. What is encryption and how does it work? - Google Cloud, accessed on October

7, 2025, https://cloud.google.com/learn/what-is-encryption

12. How can I explain to non-techie friends that "cryptography is good"?, accessed on October 7, 2025, https://security.stackexchange.com/questions/123234/how-can-i-explain-to-non-techie-friends-that-cryptography-is-good
13. How African Governments Undermine the Use of Encryption - CIPESA, accessed on October 7, 2025, https://cipesa.org/download/briefs/How_Africa_Government_Undermine_the_Use_of_Encryption_2021.pdf
14. Ten Steps to Smartphone Security, accessed on October 7, 2025, https://www.fcc.gov/sites/default/files/smartphone_master_document.pdf
15. Top 6 Mobile Security Threats and How to Prevent Them - Check Point Software, accessed on October 7, 2025, https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/top-6-mobile-security-threats-and-how-to-prevent-them/
16. A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications, accessed on October 7, 2025, https://www.mdpi.com/1999-5903/13/12/299
17. A Two Factor Authentication Security Architecture Using Biometrics for E-Banking Fraud Mitigation in Nigeria | Nigerian Journal of Engineering, accessed on October 7, 2025, https://www.njeabu.com.ng/index.php?mno=120674
18. Two Factor Authentication Solutions (2FA) - Thales, accessed on October 7, 2025, https://cpl.thalesgroup.com/access-management/two-factor-authentication-2fa
19. What metrics should be used to evaluate the effectiveness of training programs?, accessed on October 7, 2025, https://sbnsoftware.com/blog/what-metrics-should-be-used-to-evaluate-the-effectiveness-of-training-programs/
20. Measuring for Success: Evaluating Leadership Training Programs for Sustainable Impact, accessed on October 7, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC8284530/
21. Hacked online bank account recovery guide - The Cyber Helpline, accessed on October 7, 2025, https://www.thecyberhelpline.com/guides/hacked-online-bank-account
22. How to regain control of your hacked account - Punch Newspapers, accessed on October 7, 2025, https://punchng.com/how-to-regain-control-of-your-hacked-account/
23. 5 Steps to Take if Your Online Account Has Been Hacked - A Guide for Overseas Filipino Workers (OFW) - ACE Money Transfer, accessed on October 7, 2025, https://acemoneytransfer.com/blog/5-steps-to-take-if-your-online-account-has-been-hacked-a-guide-for-overseas-filipino-workers-ofw
24. NPF launches new cybercrime reporting platform - Enhancing Service Delivery - govserv.ng, accessed on October 7, 2025, https://govserv.ng/npf-launches-new-cybercrime-reporting-platform/
25. Welcome to Nigeria Police Force - National Cybercrime Center!!! - NPF-NCCC, accessed on October 7, 2025,

https://nccc.npf.gov.ng/news/nigeria-police-force-national-

26. Measuring for Success: Evaluating Leadership Training Programs for Sustainable Impact, accessed on October 7, 2025, https://pubmed.ncbi.nlm.nih.gov/34307066/
27. Low Digital Literacy Design Do's and Dont's, accessed on October 7, 2025, https://www.digital.gov.au/sites/default/files/documents/2024-07/Low%20digital%20literacy%20poster%20FINAL%20accessible.pdf
28. Accessibility for visual designers - Digital.gov, accessed on October 7, 2025, https://digital.gov/guides/accessibility-for-teams/visual-design
29. Research-based Web Design and Usability Guidelines - HHS.gov, accessed on October 7, 2025, https://www.hhs.gov/sites/default/files/research-based-web-design-and-usability-guidelines_book.pdf
30. How to Know If Your Phone Has a Virus + How to Remove It - TCL, accessed on October 7, 2025, https://www.tcl.com/global/en/blog/tips/how-to-know-if-your-phone-has-a-virus-how-to-remove-it
31. Common Android Phone Problems and Their Solutions - Carlcare, accessed on October 7, 2025, https://www.carlcare.com/ng/tips-detail/common-android-phone-problems/
32. Remove malware or unsafe software - Android - Google Account Help, accessed on October 7, 2025, https://support.google.com/accounts/answer/9924802?hl=en&co=GENIE.Platform%3DAndroid
33. How do I use the Smart Manager application to check for malware or viruses? | Samsung UK, accessed on October 7, 2025, https://www.samsung.com/uk/support/mobile-devices/how-do-i-use-the-smart-manager-application-to-check-for-malware-or-viruses/
34. How to measure the impact of Employee Sustainability Training - Mammoth Climate, accessed on October 7, 2025, https://www.mammothclimate.io/en/blog/corporate-sustainability-training/how-to-measure-employee-sustainability-training-impact