ScamDetect™

Africa's Trusted Anti-Fraud & Risk Intelligence Network

Botswana Scam, Fraud & Digital Risk –

Public Intelligence Report

Reporting Period (1ST November 2025 – January 10 2026)

16th January 2026

Prepared by ScamDetect™ – An E-Detectives Platform

Table of Contents

BOTSWANA NATIONAL RISK CONTEXT

Why Scam & Fraud Intelligence Is Now a National Priority ?

Botswana's Digital Trust Moment

Botswana's rapid digitalization across banking, mobile money, e-government services, social media adoption, and online commerce has delivered clear economic and social benefits. However, the same digital infrastructure is now being actively exploited by organised scam and fraud networks.

Scam, fraud and malware threats are no longer peripheral consumer issues. They now intersect directly with:

- Financial system integrity
- Public confidence in digital services
- Institutional credibility
- National cybersecurity and economic resilience

Scam & Frauds pose a particular Economic Risk

The intelligence presented in this report demonstrates that active scams and fraud:

- Drain household savings and small-business capital
- Undermine confidence in investment and digital finance
- Create hidden economic losses that are rarely captured in official statistics
- Shift costs onto financial institutions, insurers, and the state

While individual losses may appear small in isolation, **their cumulative impact is economically material**, particularly when under-reporting is considered.

Institutional and Systemic Exposure: Fragmented Visibility Enables Scalable Fraud

Scam and fraud activity in Botswana now operates **across interconnected national systems**, while detection and response remain institutionally siloed.

Exposure spans:

- **Financial institutions :**
  Payment abuse, mule account activity, reimbursement pressure, and post-transaction detection
- **Telecommunications providers :**
  SIM misuse, bulk messaging abuse, caller ID spoofing, and impersonation vectors
- **Digital platforms :**
  Identity exploitation, fake authority signalling, and rapid campaign propagation
- **Public institutions :**
  Reputational impersonation, delayed cyber disclosure, and fragmented incident awareness

No single institution has end-to-end visibility of the scam lifecycle. from initial contact to financial extraction and downstream impact. This fragmentation allows scam networks to exploit handoff points

between systems, scale activity faster than detection mechanisms, and repeat successful models with minimal resistance.

Why Traditional Approaches Are Insufficient

Historically, scam and fraud response has relied on:

- Post-loss reporting
- Individual case investigation
- Institution-specific controls

These approaches are **necessary but no longer sufficient**.

Modern scam networks operate:

- Faster than reporting cycles
- Across platforms and borders
- With adaptive narratives rather than static methods

Without early-stage intelligence and cross-sector coordination, prevention efforts will always lag behind threat evolution.

The Strategic Gap This Report Highlights

This report highlights a **national coordination gap**, not a failure of any single institution.

What has been missing is:

- A neutral, trusted intelligence layer
- Early aggregation of victim signals
- Behaviour-based pattern detection
- Responsible intelligence sharing before damage escalates

ScamDetect™ is designed to fill this gap.

National Value of an Early-Warning Intelligence Platform

A coordinated scam and fraud intelligence capability delivers national value by:

- Reducing financial harm before losses occur
- Supporting faster, evidence-based policy responses
- Improving institutional coordination without duplicating mandates
- Strengthening public trust in digital systems

In this context, ScamDetect™ should be understood as **risk infrastructure**, not a consumer product.

Strategic Framing Statement

Scam and fraud risk is not a future problem. This is a current, measurable, and preventable national exposure.

The intelligence in this report demonstrates that:

- Early signals exist
- Patterns are detectable
- Intervention is possible

Failure to act upstream will not result in stability. It will result in **compounding financial loss and erosion of digital trust**.

*What is required now is **coordination, trust, and timely action**.*

1. EXECUTIVE SUMMARY

Purpose of This Report

This report marks the **first public intelligence release by ScamDetect™**, Botswana's emerging scam, fraud, and cyber-risk intelligence platform. It consolidates verified scam, fraud, and malware reports captured during the soft-launch phase of the platform and converts them into actionable intelligence insights for the public, private sector, regulators, and law-enforcement stakeholders.

The objective of this report is not to present final prevalence statistics, but to demonstrate early warning signals, dominant fraud typologies, victim exposure patterns, and systemic weaknesses that scammers are actively exploiting. As such, this report should be read as a national risk snapshot, not an exhaustive crime ledger.

Reporting Period and Data Scope

- **Period covered** : 1 November 2025 – 10 January 2026
- **Total public engagements received** **:** 980 (WhatsApp, Messenger, phone calls)
- **Total reports received** : 476
- **Verified reports captured on ScamDetect™** : 94
- **Total confirmed financial loss (verified cases only)** : **BWP 720,645.85**

While only verified cases are included in statistical breakdowns, all unverified reports remain valuable intelligence signals and are retained for trend analysis, scam typology refinement, and public education planning.

Key Intelligence Findings (High-Level)

1. Scam activity is widespread, persistent, and multi-channel

Scam activity observed during the reporting period is not episodic. It is continuous, adaptive, and platform-driven, with scammers exploiting social media, messaging platforms, and digital payments as primary attack vectors. The sustained inflow of reports after initial spikes indicates ongoing organised operations rather than isolated incidents.

2. Investment scams dominate both volume and sophistication

Investment-related scams are the single largest category reported. These scams rely heavily on:

- Impersonation of trusted or prominent individuals
- Social media and messaging platforms as first-contact channels
- Rapid escalation to payment requests via mobile money or banking platforms

This confirms a shift away from crude scams toward identity-based trust exploitation, where perceived legitimacy replaces technical sophistication.

3. Financial fraud spans multiple payment ecosystems

Financial fraud cases show scammers deliberately spreading activity across banks, mobile money platforms, and remittance services, reducing traceability and complicating recovery. This fragmentation suggests operational maturity and coordination, not opportunistic fraud.

4. Malware and ransomware reporting signals long-term exposure

All malware reports captured in this period relate to ransomware incidents affecting parastatals and large enterprises. Notably, some attacks occurred as far back as 2021, but were only reported during this window. This highlights:

- Delayed disclosure
- Limited historical intelligence consolidation
- The absence of a centralised national reporting and analysis mechanism prior to ScamDetect™

Verified Case Breakdown (Snapshot)

- **Scam cases:** 60
    - Dominated by investment scams, online shopping scams, impersonation, and employment-related scams.
- **Fraud cases:** 21
    - Predominantly financial fraud, fake invoices, business impersonation, and loan-related fraud
- **Malware cases:** 13
    - All ransomware incidents affecting large organisations

This distribution confirms that scams targeting individuals and fraud affecting institutions are converging into a single risk ecosystem, rather than remaining separate problem domains.

Public Awareness and Outreach Impact

During the soft-launch phase, ScamDetect™ relied primarily on organic public engagement and media outreach, with Facebook as the primary amplification channel:

- **649,300+ people reached on Facebook**
- **4,200+ followers gained in under 3 months**
- National media engagements including:
    - BTV In-Focus
    - RB1 and RB2 radio interviews
    - Multiple podcasts and expert interviews

The volume of inbound reports relative to the platform's age indicates latent demand for a trusted reporting and intelligence channel, even before official launch or nationwide campaigns.

Strategic Intelligence Conclusion

The evidence from this first reporting cycle is clear:

Scam and fraud activity in Botswana is not declining, not random, and not purely technical in nature. It is trust-driven, socially engineered, and digitally amplified, exploiting gaps between public awareness, institutional coordination, and real-time intelligence sharing.

ScamDetect's early data demonstrates that intervention must shift upstream, from post-loss response to early detection, rapid intelligence sharing, and coordinated prevention. Without such a shift, financial losses will continue to escalate, while confidence in digital platforms, financial systems, and public trust will erode.

This first public report establishes the foundation for ScamDetect's role as a national and regional fraud intelligence capability, with future reports expected to increase in depth, accuracy, and predictive value as reporting volumes grow and institutional integrations mature.

Botswana Scam, Fraud & Digital Risk – First Public Intelligence Report

1 Nov 2025 – 10 Jan 2026 | Released 16 Jan 2026

TOTAL CASES

94

TOTAL LOST MONEY

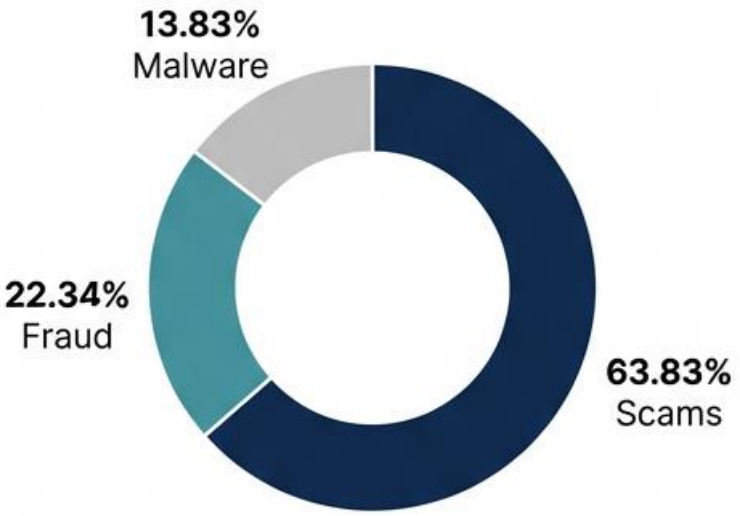
₱ 720,645.85

SCAMS

60

MALWARE

13



Key Pattern: Investment scams dominate scam cases (23; >40% of scams).

Public Awareness

VIEWS	UNIQUE VIEWERS	LINK CLICKS	MESSAGING CONTACTS	NEW FOLLOWERS
2.0M	649.3K	38.9K	929	4.2K

2. ABOUT SCAMDETECT™

2.1 What ScamDetect™ Is

ScamDetect™ is an **intelligence-led scam, fraud, and digital risk detection platform** designed to capture, analyse, and translate real-world victim reports into early-warning intelligence.

It is not a complaints system, a consumer helpdesk, or a case-management tool.
ScamDetect™ functions as a risk intelligence layer that sits between the public, financial systems, digital platforms, and enforcement bodies transforming fragmented victim experiences into structured intelligence that can be acted upon before damage escalates.

At its core, ScamDetect™ exists to answer one question:

What scam and fraud activity is happening right now, how is it evolving, and who is at risk next?

2.2 Why ScamDetect™ Exists

ScamDetect™ was created in response to a critical gap:

While scams and fraud have become faster, digital, and socially engineered, national detection and response mechanisms remain slow, fragmented, and reactive.

Today:

- Victims report incidents after losses occur
- Reports are scattered across banks, police, telecoms, social platforms, and informal channels
- Intelligence is siloed, delayed, or never consolidated
- Patterns are discovered months or years too late

As a result, the same scam models repeatedly succeed, even when individual cases are known.

ScamDetect™ exists to collapse that delay, to capture signals early, connect patterns quickly, and enable preventive action rather than post-incident response.

2.3 The Problem ScamDetect™ Addresses

Modern scam and fraud ecosystems are characterised by:

- **Trust exploitation**, not just technical compromise
- **Identity and impersonation abuse**, not only fake accounts
- **Platform convergence**, where social media, messaging apps, and payment systems are used together
- **Cross-border operations**, making attribution and takedown difficult

Traditional approaches focus on:

- Financial loss recovery
- Individual case investigation

- Institutional silos

ScamDetect™ addresses the problem at a systemic level by focusing on:

- Behavioural patterns
- Scam typologies
- Campaign indicators
- Early-stage signals

This shift from loss accounting to risk intelligence is essential if scams are to be disrupted at scale.

2.4 Who ScamDetect™ Serves

ScamDetect™ is designed as a shared intelligence platform, serving multiple stakeholder groups without privileging one at the expense of others.

The Public	• Individuals reporting scams, attempted fraud, or suspicious activity • Communities seeking early warnings and education • Victims contributing intelligence even when recovery is no longer possible
Enterprises and Institutions	• Banks and financial service providers • Insurance companies • Telecommunications operators • Large corporates exposed to impersonation and brand abuse
Government and Enforcement	• Law-enforcement agencies • Regulators and policy makers • Cybersecurity and consumer protection bodies

Each group contributes different signals. ScamDetect's role is to connect them responsibly, within clear governance and privacy boundaries.

2.5 How ScamDetect™ Is Different

ScamDetect™ differs from traditional reporting platforms in five fundamental ways:

1. **Intelligence-First Design**
   Reports are analysed for patterns, not processed as isolated complaints.
2. **Early-Stage Signal Capture**
   Attempted scams and near-misses are treated as valuable intelligence, not noise.
3. **Behaviour-Based Classification**
   Scam types are defined by how fraud is executed, not how victims describe it.
4. **Cross-Sector Relevance**
   Intelligence is designed to inform banks, telecoms, regulators, and the public simultaneously.
5. **Prevention-Focused Outcomes**
   The goal is to stop the next victim, not only document the last one.

2.6 Mission, Vision, and Operating Ethos

Mission
To detect risk early, share intelligence, and stop fraud before damage is done.

Vision
To become Africa's most trusted scam, fraud, and digital risk intelligence platform protecting people, businesses, and economies through early detection and shared intelligence.

These are not marketing statements. They define how decisions are made, how data is handled, and how trade-offs are evaluated across the platform.

2.7 Positioning Going Forward

As ScamDetect™ transitions from soft launch to official national rollout, its role will expand from signal collection to risk coordination, supporting faster warnings, better-informed decisions, and more effective intervention across Botswana and, eventually, the region.

This report represents the first step in building a shared intelligence picture, one that grows stronger as participation, integration, and trust increase.

2.8 Boundary Statement

ScamDetect™ does not seek regulatory, investigative, or enforcement authority.
It operates as an independent intelligence capability that supports existing mandates through early-warning insights and coordination.

3. METHODOLOGY AND DATA GOVERNANCE

3.1 Purpose of the Methodology

The methodology applied by ScamDetect™ is designed to ensure that all intelligence outputs are:

- **Reliable** – based on structured assessment, not raw allegations
- **Consistent** – comparable across time, sectors, and scam categories
- **Ethically sound** – respectful of victims and compliant with data protection principles
- **Fit for intelligence use** – enabling early warning, pattern detection, and prevention

This methodology prioritises signal quality over volume, recognising that early-stage intelligence must balance inclusivity with analytical integrity.

3.2 Data Collection Channels

Reporting Channel	Why This Channel Matters	Intelligence Value Enabled
WhatsApp Reporting	Low-friction, familiar channel widely used by the public	Captures early scam approaches, real-time narratives, and rapid campaign spread
Facebook Messenger	Primary engagement channel for social media–driven scams	Visibility into impersonation, investment scams, and platform-based entry vectors
Direct Phone Calls	Accessible for victims uncomfortable with digital reporting	Reveals urgency tactics, authority exploitation, and high-pressure scam execution
Web-Based Submissions	Structured intake for users able to provide detailed information	Supports higher-quality verification, documentation, and trend analysis

All reports are time-stamped at the point of receipt, enabling temporal trend analysis, campaign clustering, and detection of surge and persistence patterns. Channel diversity is a deliberate design choice to reduce reporting friction and capture intelligence signals that would otherwise be lost.

3.3 Report Intake and Initial Screening

All incoming reports undergo an initial intake process focused on completeness and relevance, not proof of loss.

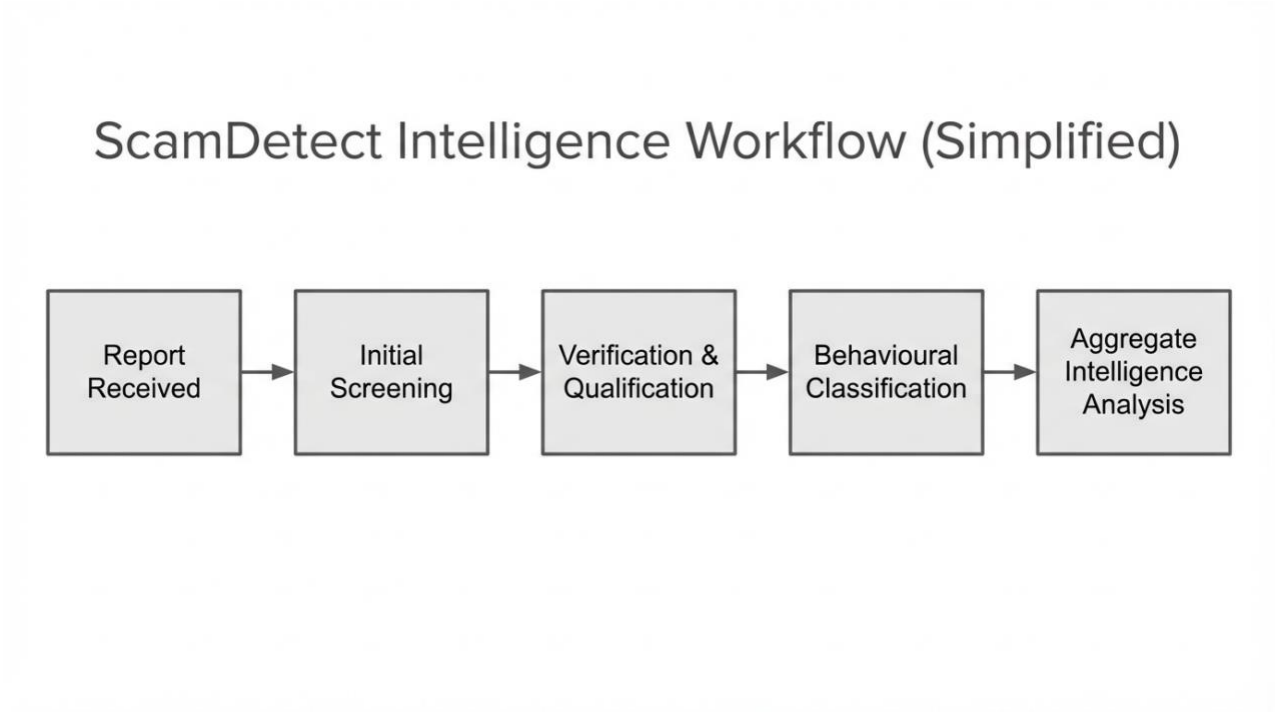
At this stage:

- Reports are accepted even where financial loss has not yet occurred
- Attempted scams and near-misses are treated as valuable early-warning signals
- Reports that are clearly unrelated to scams or fraud are excluded

This ensures ScamDetect™ captures emerging threats, not only completed crimes.

3.4 Verification and Qualification Criteria

Not all reports received are immediately included in ScamDetect's verified intelligence dataset.



Reports are assessed against defined qualification criteria, which may include:

- Internal consistency of the narrative
- Plausibility of the scam method described
- Presence of corroborating indicators (e.g. screenshots, message content, transaction references)
- Alignment with known or emerging scam typologies

Only reports that meet the qualification threshold are:

- Categorised as verified cases
- Included in statistical breakdowns
- Used for financial loss aggregation

During this reporting period:

- **476 reports** were received across all channels
- **94 reports** met verification criteria and were formally captured as verified cases
- Verified financial losses totalled **BWP 720,645.85**

Reports that did not meet verification criteria were not discarded. Instead, they were retained as unverified intelligence signals to inform:

- Scam trend monitoring
- Education and awareness priorities

- Future typology refinement

3.5 Categorisation and Classification

ScamDetect™ classifies reports based on **behavioural characteristics**, not solely on how victims label incidents.

Classification is anchored on four analytical dimensions	
Engagement vector	How contact is initiated (e.g. social media, messaging platforms, phone calls, email)
Persuasion mechanism	The behavioural lever used (e.g. impersonation, urgency, authority, opportunity)
Extraction method	How value is obtained (e.g. payment instructions, account takeover, data harvesting)
Target profile	Who is being targeted (individuals, businesses, institutions)

This approach deliberately abstracts away from narrative detail to reveal structural similarities across incidents that appear different on the surface**.** By classifying behaviour rather than labels, ScamDetect™ reduces misclassification, surfaces repeatable scam models, and enables comparison across time, platforms, and victim groups.

Scams rarely fail because victims misunderstand the threat; they succeed because systems fail to recognise recurring behavioural patterns early enough.

3.6 Data Analysis and Intelligence Development

Once verified, reports are analysed collectively to identify:

- Recurring scam models
- Common impersonated identities or roles
- Dominant communication and payment channels
- Indicators of organised or repeat activity
- Shifts in scam tactics and targeting

Importantly, ScamDetect™ does **not** attempt to:

- Attribute criminal responsibility
- Make legal determinations
- Replace law-enforcement investigation

The platform's role is to provide decision-grade intelligence, not prosecutorial conclusions.

3.7 Treatment of Financial Loss Data

Financial loss figures reported by ScamDetect™ reflect confirmed losses only, based on information voluntarily provided by victims and meeting verification thresholds.

As a result:

- Reported loss figures are conservative by design
- Actual economic impact is likely higher
- Absence of reported loss does not imply absence of harm or risk

This conservative approach protects credibility and avoids inflating figures for attention or advocacy purposes.

3.8 Limitations of Early-Stage Data

As a soft-launch intelligence dataset, the findings in this report are subject to known limitations, including:

Under-reporting	Many victims do not report scams due to shame, fear, or lack of awareness
Incomplete submissions	Some reports lack technical or transactional detail
Short observation window	Early reporting periods may amplify apparent spikes or lulls
Non-representative sampling	Volumes do not equate to national prevalence rates

These limitations are openly acknowledged to ensure responsible interpretation of findings.

3.9 Data Governance, Ethics, and Privacy

ScamDetect™ applies a **privacy-by-design and ethics-first** framework throughout its operations.

Key safeguards include:

1. **Data minimisation:** Only information necessary for analysis is collected.
2. **De-identification:** Personal identifiers are removed before analysis and reporting.
3. **Purpose limitation:** Data is used solely for scam detection, prevention, and intelligence.
4. **Controlled access:** Sensitive intelligence outputs are shared under governance oversight.

ScamDetect™ does **not**:

- Sell personal data
- Profile individuals for commercial purposes

- Use automated decision-making that affects individual rights

3.10 Methodological Integrity Statement

ScamDetect's methodology is continuously reviewed and refined as:

- Reporting volumes increase
- Institutional integrations expand
- Scam tactics evolve

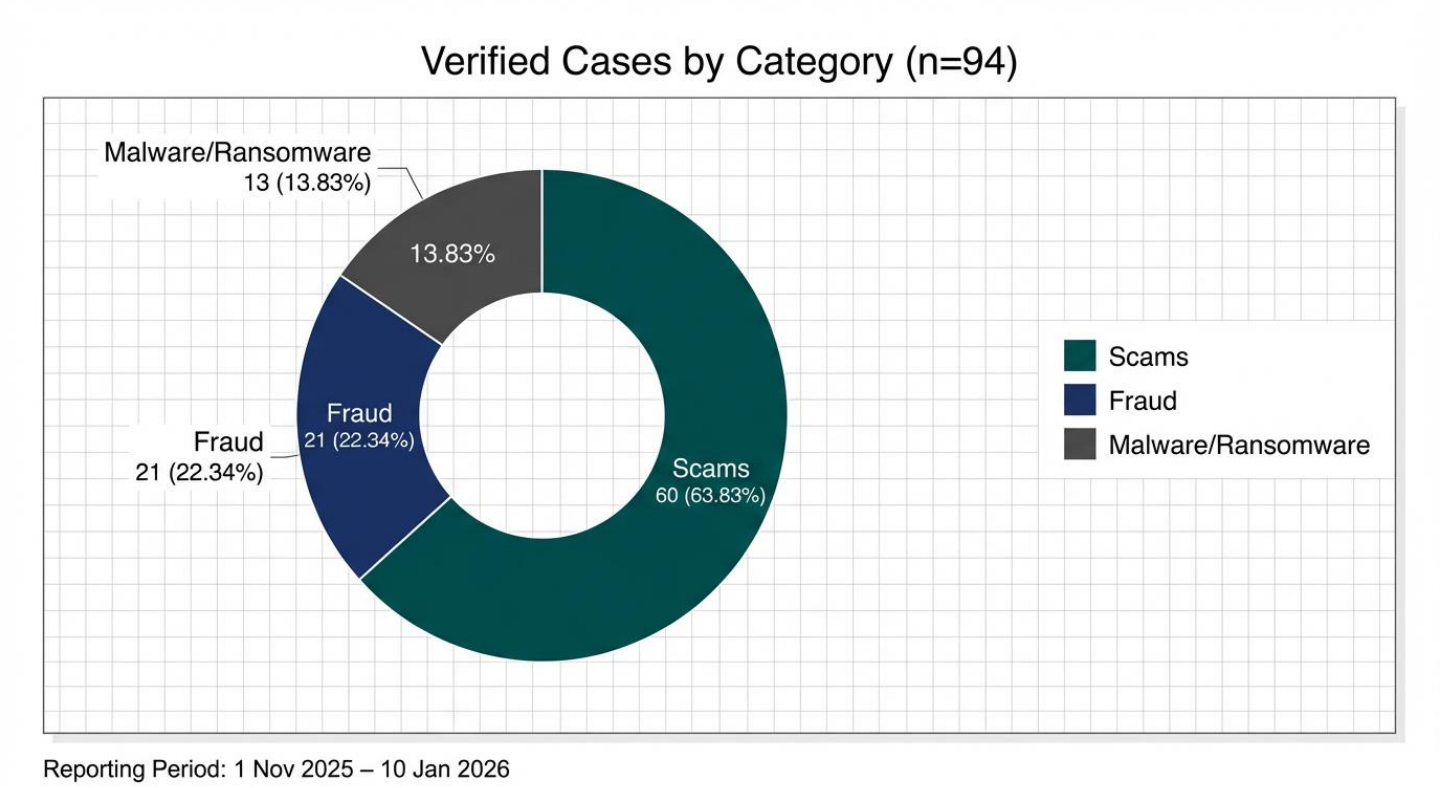
Accuracy, transparency, and public trust take precedence over speed or scale.
This approach ensures ScamDetect™ remains a credible national intelligence asset, capable of supporting prevention, policy, and coordinated response as the platform matures.

4. KEY FINDINGS AND INTELLIGENCE INSIGHTS

4.1 Overview of Verified Cases

During the reporting period, ScamDetect™verified **94 cases** that met qualification criteria for inclusion in this intelligence report. These cases fall into three primary categories:

- **Scams:** 60 cases
- **Fraud:** 21 cases
- **Malware (Ransomware):** 13 cases



The verified cases represent only a subset of total public engagements, reflecting ScamDetect's conservative verification approach. However, even within this subset, clear and consistent patterns emerge regarding how scams are executed, who is targeted, and which systems are most exposed**.**

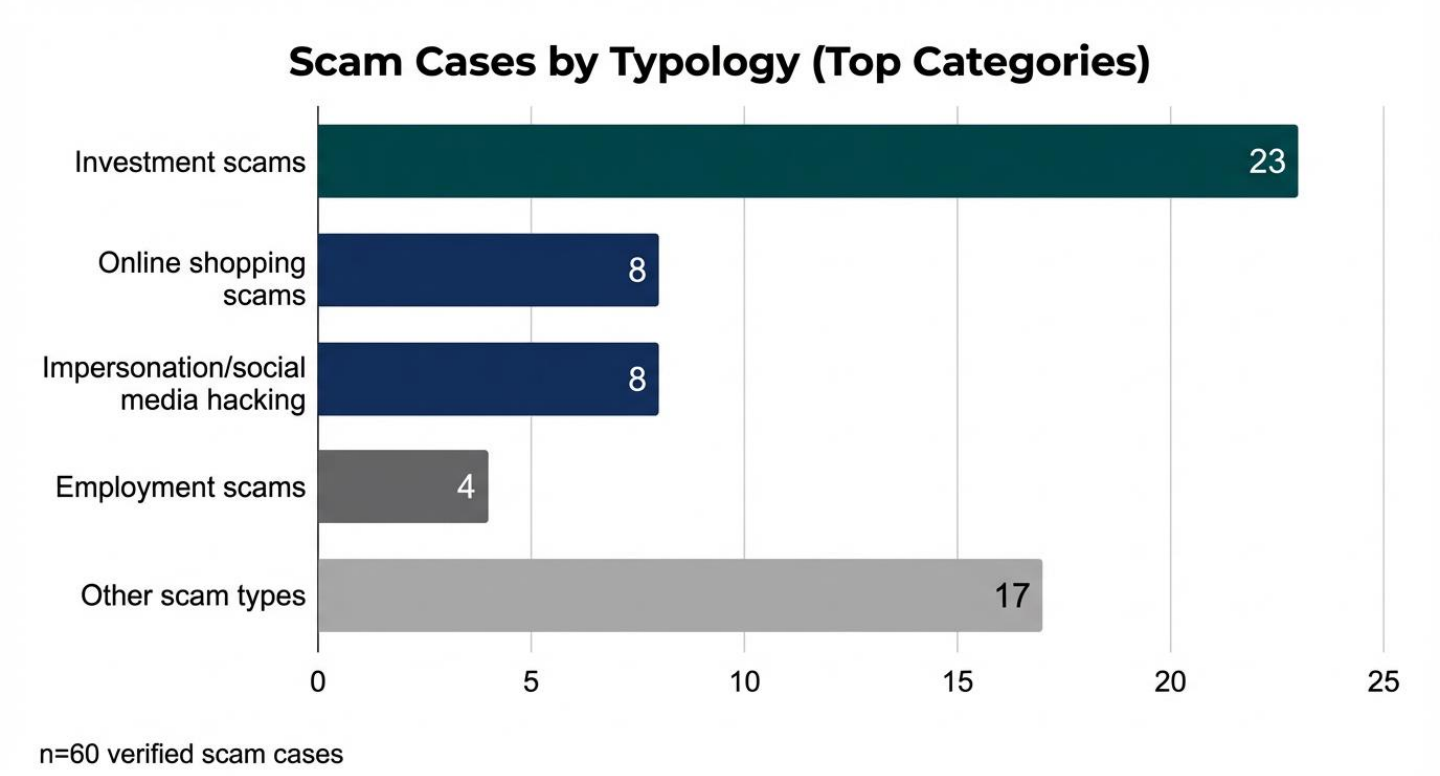
4.2 Scam Cases: Dominant Typologies and Patterns

4.2.1 Scam Category Distribution

Among the **60 verified scam cases**, the following typologies were identified:

- **Investment scams:** 23
- **Online shopping scams:** 8
- **Social media hacking / impersonation scams:** 8
- **Employment scams:** 4
- **Charity / donation scams:** 3
- **Phishing scams:** 2
- **Prize-winning scams:** 2
- **Accommodation rental scams:** 2
- **Pension fund scams:** 2
- **Online selling scams:** 2
- **Extortion / blackmail scams:** 2

This distribution confirms that investment-related deception is the primary scam threat**,** significantly outweighing transactional or opportunistic scams.



4.2.2 Intelligence Insight: Investment Scams

Investment scams account for **over 40% of all scam cases** recorded.

Key characteristics observed include:

- Heavy reliance on impersonation of trusted or influential individuals
- Use of social media and messaging platforms as primary engagement channels
- Presentation of opportunities as:
    - Exclusive
    - Time-sensitive
    - Endorsed by authority or reputation

These scams are rarely crude. Instead, they are carefully framed narratives designed to bypass scepticism through familiarity and perceived credibility.

Risk implication:
Investment scams represent a systemic trust failure, not a user education problem alone. As long as scammers can convincingly impersonate authority figures and exploit social platforms, this category will continue to scale.

4.3 Fraud Cases: Financial and Business Exploitation

4.3.1 Fraud Category Distribution

Among the **21 verified fraud cases**, the following were identified:

- **Financial fraud:** 13
- **Fake invoice fraud:** 2
- **Business impersonation:** 2
- **Loan fraud:** 1
- **Accommodation investment fraud:** 1
- **Other structured fraud types:** 2

Financial fraud dominates this category, with scammers directly manipulating payment processes rather than relying solely on persuasion.

4.3.2 Intelligence Insight: Financial Fraud

Financial fraud cases reveal a **hybrid execution model**:

Stage 1: Initial Contact	Stage 2: Escalation & Control	Stage 3: Financial Extraction
• Social media platforms • Messaging applications • Informal digital contact	• Direct phone calls • Guided payment instructions • Authority and urgency pressure	• Bank transfers • Mobile money services • Remittance platforms

This fragmentation serves two purposes:

1. Reduces traceability
2. Increases likelihood of successful extraction before detection

Risk implication:
Financial fraud is no longer isolated within a single institution or channel. Prevention requires cross-platform intelligence sharing, not institution-by-institution monitoring.

4.4 Malware and Ransomware: Latent Organisational Exposure

4.4.1 Malware Case Profile

All **13 malware reports** captured during this period relate to ransomware incidents affecting:

- Parastatals
- Large enterprises

Notably:

- Some attacks occurred as far back as **2021**
- Reporting only occurred during this recent window

4.4.2 Intelligence Insight: Delayed Reporting Risk

Delayed / Suppressed Reporting Model	Early Intelligence Sharing Model
• Incident occurs • Reporting delayed or avoided • No shared visibility • Attack techniques reused • Similar organisations targeted • Systemic exposure compounds	• Incident occurs • Early, non-punitive reporting • Signals aggregated centrally • Patterns detected early • Preventive warnings issued • Risk disrupted before scale

What Breaks the Loop?

The transition from delayed reporting to early prevention does not require perfect detection or full disclosure. It requires a trusted mechanism that enables organisations and individuals to share early signals without fear of reputational or regulatory penalty.

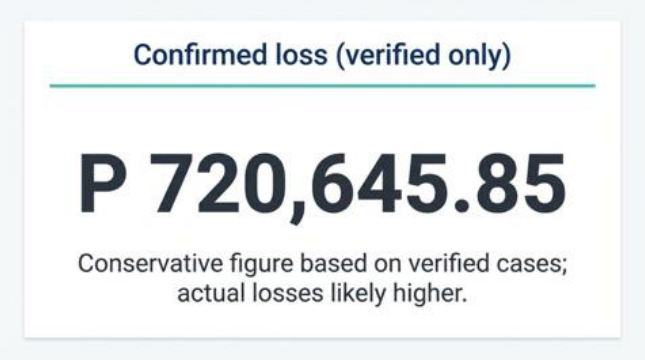
ScamDetect™ breaks the delayed reporting loop by:

1. Providing a neutral, non-punitive reporting and intelligence platform
2. Aggregating early-stage signals across sectors and institutions
3. Detecting repeat patterns and campaign indicators before losses escalate
4. Enabling responsible intelligence sharing without expanding enforcement mandates

By restoring visibility at the earliest stages of cyber and fraud activity, ScamDetect™ converts isolated incidents into shared intelligence, reducing repeat compromise and strengthening systemic resilience.

4.5 Financial Impact Snapshot

- **Total confirmed financial loss (verified cases): BWP 720,645.85**
- Losses primarily occurred through:
  - Mobile money platforms
  - Bank transfers
- Many victims were unable to provide proof of loss, particularly for mobile money transaction



This figure should be viewed as conservative, representing only confirmed and verifiable losses.

Risk implication:
Actual economic impact is likely significantly higher, particularly when considering:

- Unverified reports
- Near-miss cases
- Reputational and psychological harm

4.6 Cross-Cutting Patterns Across All Categories

Across scams, fraud, and malware cases, several cross-cutting patterns emerge:

1.	**Social platforms are the primary entry point**	Facebook, WhatsApp, and similar platforms dominate first contact.
2.	**Trust is the primary exploit**	Authority, familiarity, and legitimacy cues are more important than technical tricks.
3.	**Payment systems are reactive, not preventive**	Transactions often occur before risk is detected or challenged.
4.	**Victims span all demographics**	Early data shows no clear age or income immunity.

4.7 Strategic Intelligence Conclusion

The key finding from this reporting period is not simply that scams exist, it is that current systems allow them to repeat, adapt, and scale**.**

ScamDetect's early data confirms that:

- Scam and fraud risks are **systemic**, not isolated
- Prevention must occur **before funds move**, not after
- Intelligence must flow **across institutions**, not remain siloed

Without coordinated early-warning intelligence, these patterns will persist and financial losses will continue to compound.

5. IMPLICATIONS AND STRATEGIC RECOMMENDATIONS

5.1 Why These Findings Matter

The findings in this report point to a critical reality:

Scams and fraud in Botswana are no longer isolated incidents affecting careless individuals. They represent a systemic national risk that exploits gaps between digital platforms, financial systems, enforcement mechanisms, and public awareness.

The intelligence shows that:

- Trust-based scams are scaling faster than traditional controls
- Fraud models adapt quickly to enforcement and platform changes
- Delayed detection multiplies financial and social harm

Without coordinated intervention, these risks will compound rather than stabilise**.**

5.2 Implications by Stakeholder Group

5.2.1 Implications for Government and Regulators

What the intelligence shows:

- Scam and fraud activity cuts across financial services, telecommunications, digital platforms, and cyber domains
- No single regulator or agency has full visibility of the threat landscape
- Policy responses are reactive and fragmented

Implication:
A siloed regulatory approach is structurally incapable of managing a cross-sector threat.

Recommendation:

- Establish a national scam and fraud intelligence coordination framework
- Recognise ScamDetect™ as an early-warning intelligence partner, not a parallel enforcement body
- Enable structured data-sharing agreements across regulators, banks, telcos, and law enforcement

5.2.2 Implications for Financial Institutions

What the intelligence shows:

- Fraud losses occur before alerts or interventions are triggered
- Scammers exploit speed, convenience, and fragmented payment channels
- Victims often follow guided payment instructions in real time

Implication:
Transaction monitoring alone is insufficient without contextual intelligence**.**

Recommendations:

- Integrate external scam intelligence feeds into fraud detection systems
- Implement pre-transaction risk prompts for high-risk scam indicators
- Collaborate across institutions to identify repeat scam patterns and mule pathways

5.2.3 Implications for Telecommunications and Digital Platforms

What the intelligence shows:

- Social media and messaging platforms are the dominant entry points for scams
- Impersonation and fake identities are core enablers of fraud
- Content takedown often occurs after damage is done

Implication:
Platform trust mechanisms are being weaponised faster than they are enforced.

Recommendations:

- Strengthen impersonation detection and reporting escalation processes
- Share anonymised scam pattern data with national intelligence partners
- Support rapid takedown workflows for confirmed scam campaigns

5.2.4 Implications for Law Enforcement

What the intelligence shows:

- Many scams are never formally reported to police
- Cases that are reported often arrive after evidence has degraded
- Patterns across cases are rarely consolidated

Implication:
Enforcement visibility is incomplete, not due to lack of effort, but lack of upstream intelligence.

Recommendations:

- Use ScamDetect™ intelligence as a triage and prioritisation tool
- Focus resources on repeat patterns and organised campaigns
- Encourage early, non-punitive reporting pathways

5.2.5 Implications for the Public

What the intelligence shows:

- Anyone can be targeted
- Familiar faces and trusted names are routinely abused
- Shame and fear suppress reporting

Implication:
Public education must evolve beyond basic awareness.

Recommendations:

- Normalise reporting of attempted scams and near-misses
- Promote early reporting even when no money is lost
- Shift messaging from **"don't fall for scams"** to **"report fast to protect others"**

5.3 Cross-Cutting Strategic Recommendations

Across all stakeholder groups, the intelligence supports five core strategic actions:

1.	**Move Upstream**	Detect scams before money moves, not after loss occurs.
2.	**Share Intelligence, Not Just Alerts**	Patterns matter more than individual cases.
3.	**Treat Trust as Critical Infrastructure**	Impersonation and identity abuse must be addressed as systemic risks.
4.	**Reduce Reporting Friction**	The easier it is to report, the earlier intelligence emerges.
5.	**Adopt Prevention as a Shared Responsibility**	No single institution can solve this alone.

5.4 Role of ScamDetect™ Going Forward

Based on the findings and stakeholder implications, ScamDetect's role is to:

- Serve as a neutral intelligence aggregator
- Provide early-warning signals across sectors
- Enable evidence-based policy and prevention
- Support, not replace, enforcement and regulatory functions

ScamDetect™ does not seek authority, it seeks coordination**.**

5.5 Closing Strategic Statement

This first public report demonstrates that scam and fraud risk is knowable, detectable, and preventable when intelligence is captured early and shared responsibly.

The cost of inaction is not just financial, it is erosion of trust in digital systems, institutions, and public confidence. The opportunity ahead is to shift from reaction to prevention.

6. OUTLOOK AND NEXT STEPS

6.1 Short-Term Outlook (Next 3–6 Months)

As ScamDetect™ transitions from soft launch to official national rollout, several developments are expected in the near term:

- **Increased reporting volumes** as public awareness expands and reporting channels stabilise
- **Improved data quality** as education initiatives help reporters submit more complete information
- **Clearer trend visibility**, enabling earlier identification of coordinated scam campaigns
- **Deeper institutional engagement**, particularly from financial services, telecoms, and large enterprises

During this phase, ScamDetect's primary focus will remain on intelligence accuracy, trust, and governance, rather than rapid expansion.

6.1.1 Emerging Scam Threat: Bank KYC-Impersonation & OTP Harvesting

Although outside the formal reporting period of this report, ScamDetect™ has identified a rapid increase in post-period reports involving a specific and highly effective scam model targeting bank customers.

In these cases, victims are contacted by callers impersonating bank officials under the pretext of KYC compliance, account verification, or fraud prevention. Victims are instructed to disclose one-time passwords (OTPs) sent by their bank, under the false assurance that the code is required to secure their account.

Once the OTP is disclosed, scammers gain legitimate authenticated access to the victim's online banking profile. Funds are then rapidly transferred and withdrawn through mule accounts or cash-out mechanisms, often within minutes of access being obtained.

Importantly, these incidents do not involve compromise of bank systems or malware infection. Instead, they exploit the human layer of authentication, using social engineering to co-opt bank security controls designed to protect customers.

Emerging risk implications:

- OTP-based authentication remains vulnerable to real-time social engineering
- Losses occur before post-transaction controls or alerts are triggered
- Victims often perceive the activity as "unauthorised hacking," despite authentication occurring within legitimate banking workflows

This emerging pattern reinforces the need for upstream intervention, including:

- Explicit warnings at OTP issuance points
- Public education focused on *when* OTPs should never be shared
- Cross-institution intelligence sharing to identify repeat scam scripts and caller patterns

While these cases are not included in the statistical findings of this report, they represent a credible near-term escalation risk and will be incorporated into future reporting cycles should the trend persist.

6.2 Medium-Term Outlook (6–12 Months)

With sustained participation and structured partnerships, ScamDetect™ is expected to evolve into a national scam and fraud intelligence capability.

Key milestones anticipated include:

- Regular public intelligence reports (quarterly and annual)
- Sector-specific intelligence briefings for:
    - Financial services
    - Telecommunications
    - Large enterprises
- Enhanced classification of scam and fraud typologies
- Integration of advanced analytics and risk scoring models
- Expansion of reporting channels to reduce friction further

At this stage, ScamDetect™ will increasingly support policy formulation, regulatory coordination, and preventative intervention.

6.3 Long-Term Outlook (12 Months and Beyond)

Beyond its initial national focus, ScamDetect™ is designed to scale regionally and continentally, recognising that scam and fraud ecosystems do not respect national borders.

Long-term outcomes include:

- Cross-border intelligence collaboration within SADC and Africa
- Comparative regional fraud and scam trend analysis
- Shared early-warning indicators across countries
- Positioning ScamDetect™ as a trusted African digital risk intelligence platform

This expansion will be governed by the same principles of ethics, sovereignty, and trust that underpin its national role.

7. CALL TO ACTION AND PARTICIPATION FRAMEWORK

7.1 For the Public

ScamDetect™ invites members of the public to:

- Report scams and suspicious activity as early as possible
- Report attempted scams, even where no money was lost
- Encourage others to report without fear or shame

Early reporting protects not just the individual, it protects the wider community.

7.2 For Financial Institutions, Telecoms, and Enterprises

ScamDetect™ invites institutions to:

- Engage in structured intelligence-sharing discussions
- Explore non-intrusive integration of scam intelligence into risk workflows
- Contribute anonymised insights that strengthen collective prevention
- Participate in sector-specific intelligence briefings

Participation is voluntary, governed, and focused on risk reduction, not blame.

7.3 For Government, Regulators, and Law Enforcement

ScamDetect™ invites public institutions to:

- Recognise scam and fraud as a cross-sector national risk
- Support coordination frameworks that enable early-warning intelligence
- Engage ScamDetect™ as a neutral intelligence partner
- Use intelligence outputs to inform policy, awareness, and enforcement prioritisation

ScamDetect™ does not seek enforcement authority, only alignment and coordination.

7.4 Shared Responsibility Statement

Scam and fraud prevention is a shared responsibility.
No single entity, public or private, can see the full picture alone.

When intelligence is:

- Reported early
- Analysed responsibly
- Shared ethically

The entire system becomes more resilient.

7.5 Closing Statement

This first ScamDetect™ Public Intelligence Report represents the beginning of a national conversation, not the conclusion.

The intelligence presented here confirms that scam and fraud risks are real, evolving, and preventable. The path forward requires trust, collaboration, and a willingness to act before harm occurs.

ScamDetect™ stands ready to support that shift.

_____

Submitted by:
Douglas Sekgweng
Managing Director
E-Detectives (Pty) Ltd

Founder _ScamDetect

Contact Channel: info@edetectives.co.bw and info@scamdetect.co.bw

Tell: 3111171 / 73233490

www.scamdetect.co.bw