KnowBe4
Human error. Conquered.

2023 Online Scams in Africa Report

by Anna Collard
SVP Content Strategy &
Evangelist KnowBe4 Africa

2023 Online Scams in Africa Report

Table of Contents

INTRODUCTION

KnowBe4 has undertaken a survey into the growing problem of online scams and how these pervasive threats are affecting people across Africa. The survey focused on what factors contributed to a person ultimately falling victim to a scam, the types of scams experienced and how it affected victims both financially and psychologically.

The survey spanned 800 individuals across Morocco, South Africa, Kenya, Botswana, Nigeria, Ghana, Egypt, and Mauritius and covered a broad range of age groups, with the majority sitting in the 25-34 age group (38%), closely followed by the 35-44 age group (22%), 18-24 (20%), 45-54 (11%) and over 54 (7%). All respondents were employed during the time of their participation.

Several common themes emerged throughout the survey, particularly around the external and internal factors influencing human behaviours and how these put people at risk of falling for a scam.

Here are some of the highlights:

- Overall, nearly 40% of respondents said they had fallen for an online scam
- 43% of victims were distracted and multi-tasking when they fell for the scam – this figure was higher in Nigeria and South Africa at 53% and 46%, respectively
- More than half (53%) of respondents felt a significant or very significant impact to their lives

The findings, taken from individuals working across multiple industries and in different roles, showed that online scams remain a pernicious and malicious threat that require vigilance and awareness. In this report, the results are analysed to show what they mean for individuals and organisations across Africa.

40% of respondents fell victim to an online scam

43% of victims were distracted or multi-tasking

24% of initial contact done via email (Social media 19%)

54% of victims rated the impact of the scam as significant

KEY FINDINGS

In June 2023, KnowBe4 conducted an African-wide survey by polling 800 people across Morocco, South Africa, Kenya, Botswana, Nigeria, Ghana, Egypt, and Mauritius.

The survey focused on several key questions around online scams, personal behaviours, impact to victims and overall awareness as to gain a holistic view of the risks facing those living and working on the continent.

The following are the key insights:

- Nearly 40% of respondents have fallen for an online scam, 33% have come across one, 19% have never fallen for a scam, while 8% did not know what it is.
- 43% of the victims of a successful online scam were distracted and multi-tasking when they fell for it.
- In Nigeria, social media (32%) was the primary form of contact for a scam while email leads in South Africa (28%).
- Different emotions are felt by people in different countries with most admitting to feeling naive or embarrassed, as well as angry. In Morocco, the primary emotion felt was anger while in Mauritius it was a loss of trust.
- It took most respondents several months to recover after falling for an online scam.
- Financial scams affected 48% of respondents who fell victim, followed closely by investment scams that affected 30% of respondents, and crypto scams that caught 29% of respondents.
- Of those who were successfully scammed, 53% were convinced the offer was legitimate because the website looked real.

These numbers highlight an increasingly sophisticated cyberthreat landscape and that online scams have evolved.

Cybercriminals are using emerging technologies and emotive approaches in well-written emails as well as deep fake enabled impersonations on WhatsApp and other messaging apps. The key is to understand what these threats are and how they have evolved so people can protect themselves from both the financial and emotional impact.

UNDERSTANDING THE THREAT

One of the key priorities of the survey was to uncover the primary reasons why people fall for online scams and what type of scams are emerging as the highest risk at this time. In light of the fact that nearly 40% of the 800 respondents across eight countries had fallen for a scam, it seems evident that this is a threat affecting a large proportion of the African population. It is also becoming increasingly sophisticated as cybercriminals seek out new ways of tricking consumers to unwittingly participate in their scams.

Types of Scams

The respondents who said yes to having fallen for an online threat were asked what type of scam had affected them. The results highlight how much effort cybercriminals are putting into their approaches and their understanding of human psychology. They know what types of messages are most likely to trigger an emotional reaction in their victims and they then exploit these reactions.

Of the respondents who fell victim, financial scams and theft affected nearly 50% of them, closely followed by investment scams (30%), crypto scams with fake NFT or crypto projects (29%), impersonating a brand (28%), information theft (24%), fake jobs (22%) and shopping scams (21%).

The remaining areas included Nigerian scams (17%), impersonating a trusted family member or friend (18%), law enforcement (7%), fake tax notifications (6%), holiday fraud (9%), dating or romance scam (13%), and lotto scams (15%). Ransomware, fake charities, and extortion also appeared in the list.

While the emotive nature of many of these scams, including the use of trusted names, brands, and family members, played a significant role in their success, the routes that the scammers took to get a person's attention varied.

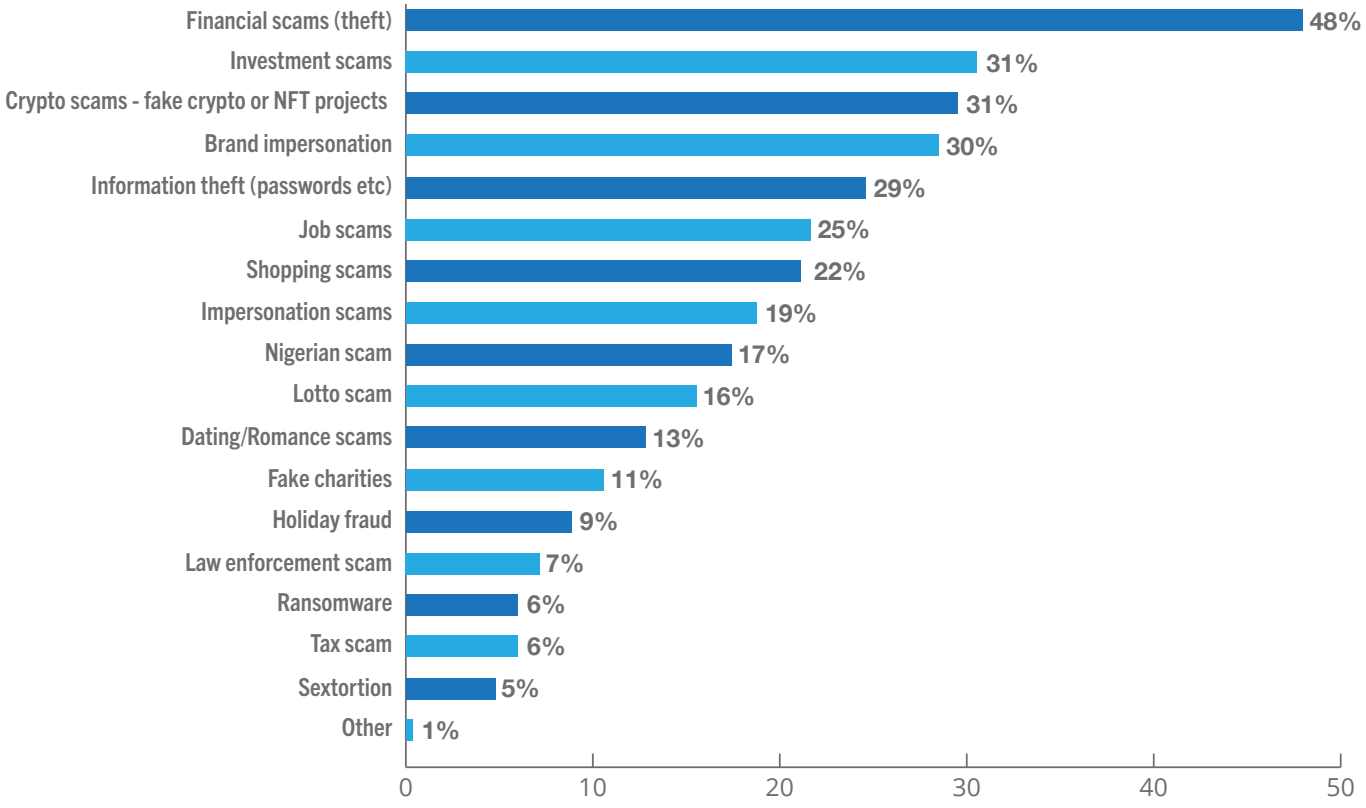

Figure 1: Type of scams experienced

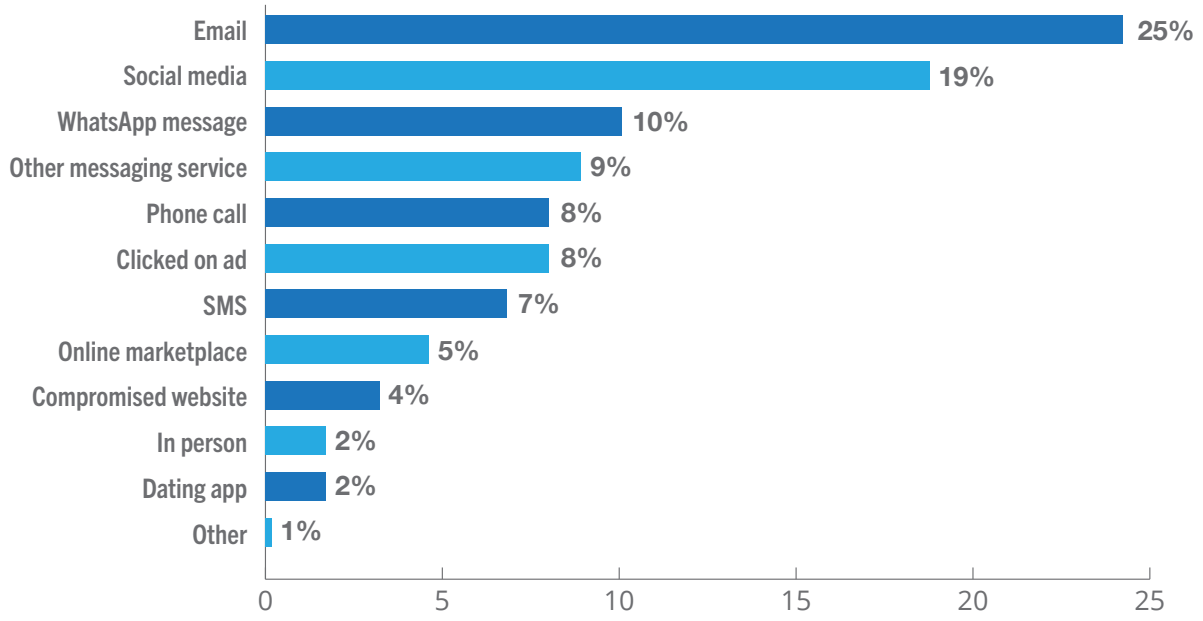

Figure 2: Initial contact made

The majority of scams made initial contact over email (24%), closely followed by social media (19%), a WhatsApp message (10%), other messaging services like Telegram (8%), malicious ads (8%), a compromised website (3%), a phone call (8%), and an SMS (7%).

Evolution of Threats

It is clear from the results of this survey that the days of spelling mistakes, obviously fake messages, and poorly hidden cons are largely over.

Most of the respondents (53%) were convinced that the contact or offer made by the scammer was legitimate because the website looked exactly like the one of a service that the respondent trusted. The second most successful attack was a message that was so convincing it triggered emotions (34%), followed by someone seeing it on social media and believing it to be legitimate (31%), and there were no spelling errors or bad grammar in the messages (25%).

These statistics paint a picture of a threat landscape that has evolved and now uses smarter techniques to trick people.

UNDERSTANDING THE VICTIMS

State of Mind

When people think of cybersecurity, they almost always think of firewalls, anti-malware, patch management, and user awareness programs. These are controls that define a solid security hygiene. But they do not take people's emotions and state of mind into account. Even with a strong firewall, a smart antivirus, a well-staffed Security Operations Centre (SOC), and frequent reminders of the threats, a single mistake by someone who is tired or distracted can compromise security.

Out of those who responded yes to falling for an online scam, nearly 43% were distracted, busy, and multi-tasking at the time. This is a significant finding as it underscores how distraction plays a role in making people more susceptible to online attacks.

Following closely behind being distracted, 20% of respondents were working when they fell for the scam, 18% were relaxed and happy, nearly 14% were tired, 6% were travelling, and nearly 6% were hungry.

It seems the way a person feels and their levels of distraction can influence how a scammer can catch them unaware.

Financial and Emotional Impact

The survey showed that negative emotions associated with a successful online scam are potentially more damaging than the amount of money lost as a result. Most of the respondents did not suffer major financial losses from the online scam. 24% took several months and 10% took more than a year to recover financially, while the rest either had no losses or recovered in a few days or weeks.

However, when it came to recovering from the emotional impact of the incident, the majority (22%) said it took them a few months, with 11% saying it took more than a year.

When asked how much money they lost thanks to the scam, 40% of the victims said they lost the equivalent of $US100, 30% lost between US$100 and US$1,000, and nearly 9% lost more than US$1,000.

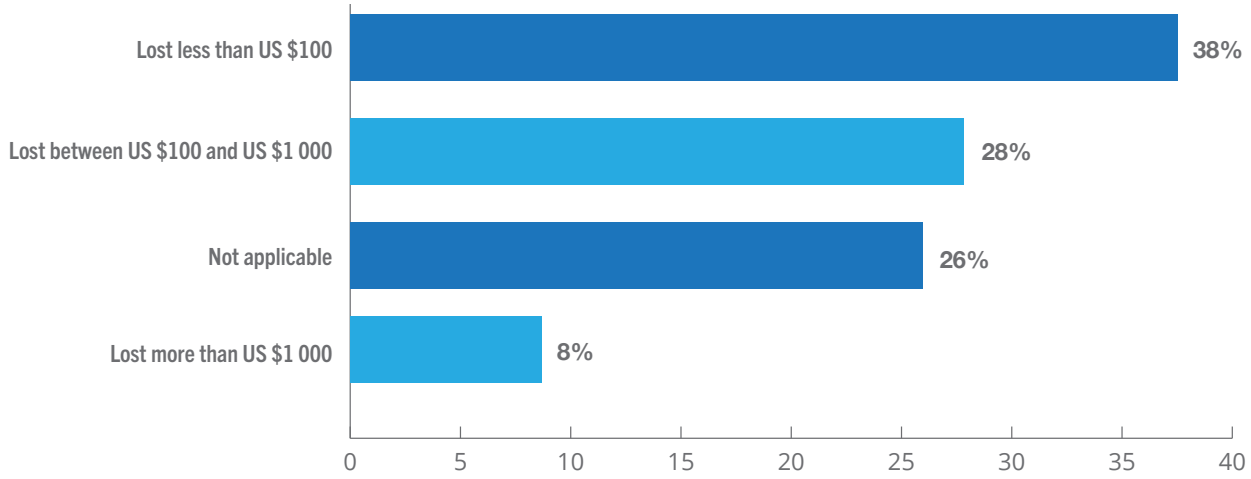

Figure 3: Financial Impact

PSYCHOLOGICAL SIGNIFICANCE OF IMPACT

While nearly 8% of respondents who cited that falling for an attack had no impact, and 14% barely had any impact, the majority believed that falling for a scam had an effect on their psychological well-being. More than half (53%) of respondents felt a significant or very significant impact and 18% felt a somewhat significant psychological impact.

These results point to how the experience serves to add to the impact of a successful scam.

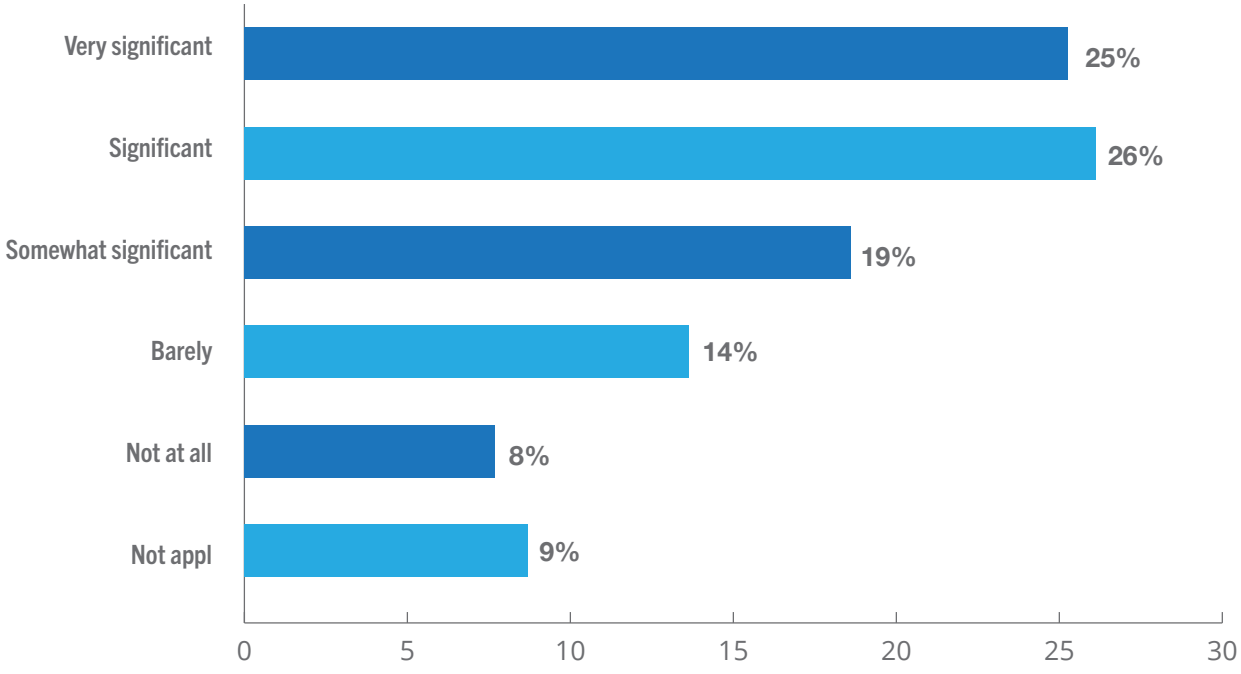

Figure 4: Psychological Significance of Impact

This is also reflected in who a person chooses to talk to about a scam. Around 13% told the police, 22% the platform provider, 15% their financial institution, and 36% told a family member or friend.

However, nearly 16% felt there was little to be gained from telling the police or the banks and a concerning 15% were too embarrassed to tell anyone what had happened.

The report also asked respondents how the incident made them feel.

The results are interesting and reflect how those affected blame themselves.

39% of respondents were embarrassed,

40% were angry,

40% felt naïve,

36% lost trust, and 25% felt shame.

Traumatised (20%), vulnerable and helpless (25%), anxious (16%), guilty (16%), and fearful (15%) are further strong negative emotions felt by the victims.

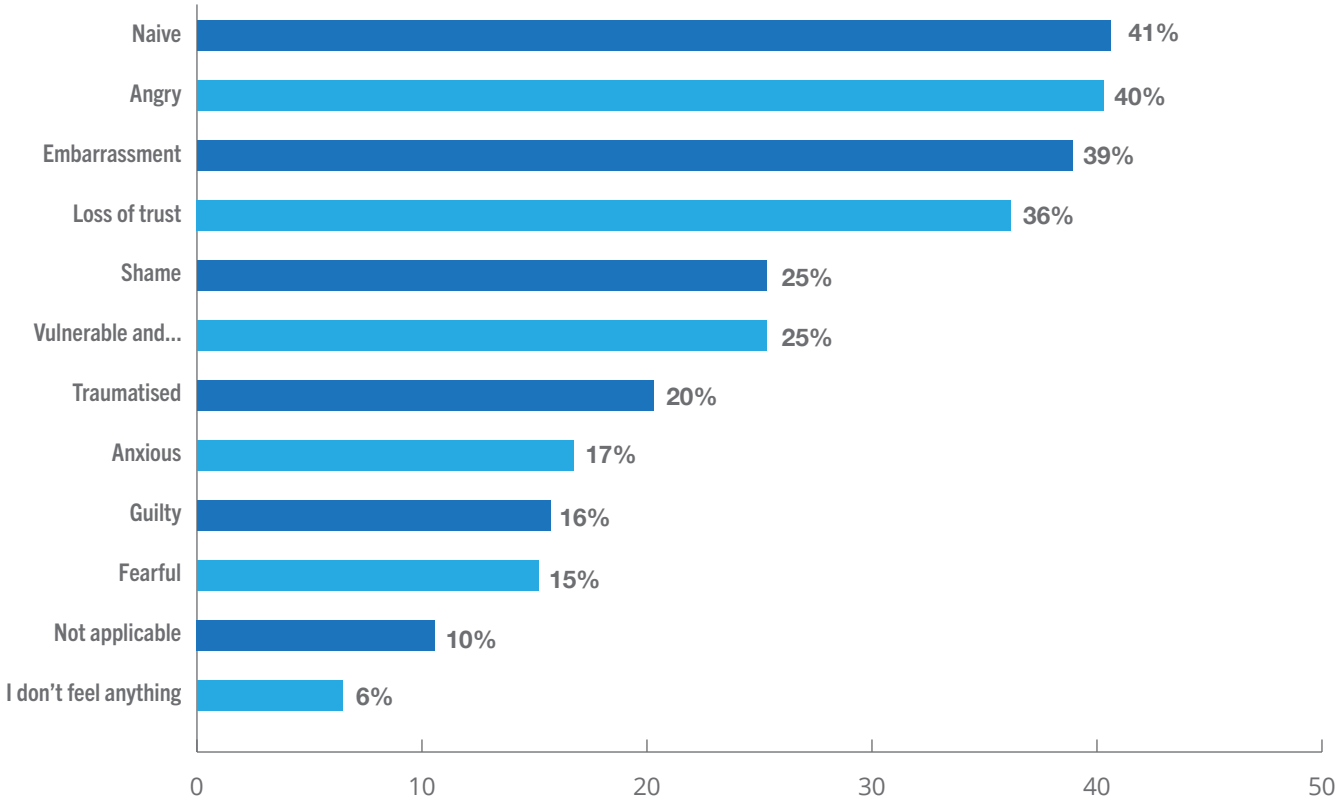

Figure 5: Emotions Felt by Victims

LOOKING AHEAD: PROTECT AND PRESERVE

The survey revealed that online attacks affect people most often when they are multi-tasking or distracted and had mostly negative emotional impacts.

However, some positive outcomes emerged as well. Most respondents (75%) became more cautious and aware of online scams, only 13% still felt vulnerable to them, and 71% warned others about their experience. Despite the increased caution, many still felt unprepared, highlighting the need for consistent training and awareness of scams and their risks.

The survey also explored how many companies provided security awareness training to their employees. The results showed that only 23% of the respondents received frequent training and 9% received both training and phishing simulations. 22% received training only once a year and 25% received no training at all.

As employee training is one of the most powerful tools to help people be aware of online scams, it is an essential investment for the organisation. When employees learn how to recognise the risks, they can protect both themselves and the organisations they work for.

Contact us at KnowBe4 Africa for locally relevant training content and our award-winning integrated simulated platform to help you make your users more aware of online scams and how to protect against them.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01D08K01