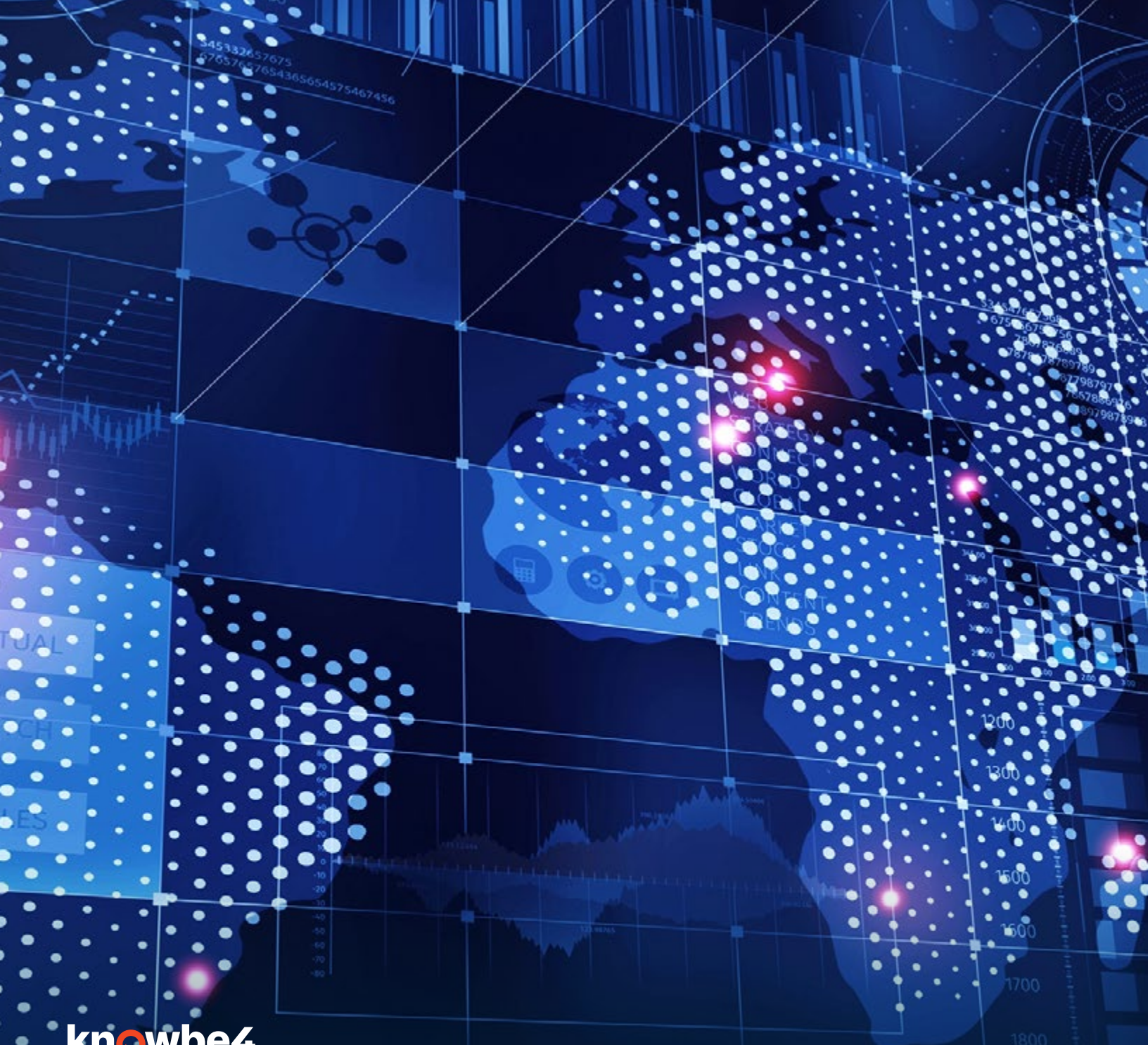


knowbe4

African Cybersecurity & Awareness Report 2025

Whitepaper

by Anna Collard
SVP Content Strategy &
Evangelist, KnowBe4 Africa

WWW.KNOWBE4.COM

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

0925US

Table of Contents

Introduction and Key Findings

Since 2019, KnowBe4 has conducted an annual survey to determine how prepared African smart-phone and Internet users are for cybersecurity threats. Set against the backdrop of the growing rise of artificial intelligence (AI) and its potential to spread disinformation, cyberthreats today are increasingly more sophisticated than they were in the past, although they still rely on human weakness.

The survey polled 800 employed adults who are smart device users across multiple sectors in seven African countries: Morocco, South Africa, Nigeria, Ghana, Egypt, Kenya, and Botswana, to assess their cybersecurity awareness. While not fully representative of Africa's diverse population or those still digitally excluded, it serves as a valuable indicator for tracking awareness trends over time.

According to the United Nations, Africa is home to the world's youngest population, with 70% of people in sub-Saharan Africa under the age of 30. This youthful majority presents a promising opportunity for the continent's growth – provided that younger generations are empowered with the tools and support needed to reach their full potential.

The cybersecurity landscape in Africa is rapidly evolving and presents both significant challenges and opportunities. As highlighted by Interpol's African Cyberthreat report 2024, Africa has seen a notable increase in cybercrime, with ransomware, digital extortion and online scams being particularly prevalent and an increase in the financial and social impacts of these crimes.

According to the South African Banking Risk Information Centre report, cybercriminals increasingly exploited human psychology for social engineering purposes. Digital banking and mobile app crime resulted in over R1 billion being stolen in 2023 from South African consumers.

Email phishing and vishing (voice phishing) remain leading attack vectors, while criminals exploit diverse communication channels, including chat apps and social media making use of technological advancements, including AI-generated content for impersonation, extortion and data theft.

The same report outlines the emergence of 'fraud-as-a-service' platforms which provide criminals with tools, techniques, and resources, making fraudulent activities easier to execute and scale. Another worrying trend is the convergence of physical and digital crime, such as criminals using kidnapping or coercion to forcibly access victims' banking applications.

One of our survey's key findings is that Africans are more concerned about cybercrime than they were towards the end of 2023. The percentage of respondents who said they were "very concerned" about cybercrime almost doubled to 58% in 2024, compared to 29% in 2023. Fear of online fraud and losing money remained their top concern.

Another important insight is that the use of mobile financial services, both for payments and banking, increased from 63% to 85% amongst our respondent group. The high use of smart phones

58%
of respondents are very concerned about cybercrime, compared to 29% in 2023

37%
of respondents said they fell for fake news or a disinformation campaign

53%
admitted they did not know what ransomware was

35%
have lost money due to a scam

for financial transactions underscores the importance of mobile-centric security education.

While 83% of respondents expressed confidence in their ability to recognise a security incident if they saw one, 53% admitted they did not know what ransomware was, 37% of respondents said they fell for fake news or a disinformation campaign and 35% of respondents have lost money due to a scam.

This disconnect highlights the critical issue of overconfidence, which can be particularly dangerous in cybersecurity, as it creates a false sense of preparedness, leaving individuals and organisations more vulnerable to threats they may not fully understand or anticipate.

Our survey aims to identify key vulnerabilities that should be a priority for individuals, organisations and policy makers, highlighting areas that should be addressed in 2025 to achieve stronger levels of cybersecurity.

Despite increased concern about cybercrime among the survey's respondents, there are still gaps in knowledge and practice that need to be addressed.

Survey Results and Interpretation

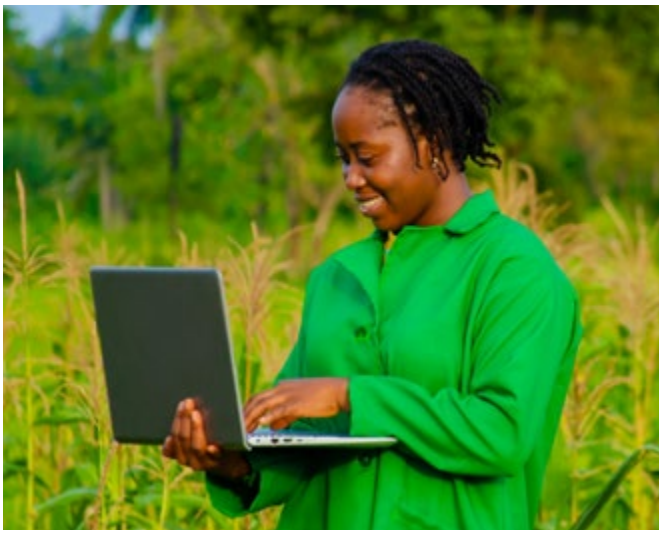
In September 2024, KnowBe4 conducted a survey by polling 800 adults aged between 30 to 60 across seven African countries – Morocco, South Africa, Nigeria, Ghana, Egypt, Kenya and Botswana. All of the respondents were employed in sectors ranging from financial services, government and health care to real estate and telecommunications. The goal of the survey was to assess respondents' cybersecurity awareness, digital habits and online security practices. While not fully representative of Africa's diverse population or those still digitally excluded, it serves as a valuable indicator for tracking awareness trends over time.

Just as it did in 2023, the 2024 survey aimed to uncover the challenges facing African users and organisations in the current cybersecurity landscape. Many challenges remain the same, but some are new, such as the alarming increase in AI-assisted cyberthreats, including the rise of deepfake technology. The response of African users to these challenges remains key.

The survey reveals the evolving landscape of African cybersecurity by tackling tough questions:

- Are you worried about cybercrime?
- Would you share your personal information?
- Would you pay to recover your data if it were encrypted in a cyberattack?
- What kinds of cybercrime have you encountered?

The survey results yield useful insights into African users' cybersecurity awareness, digital habits and security practices.



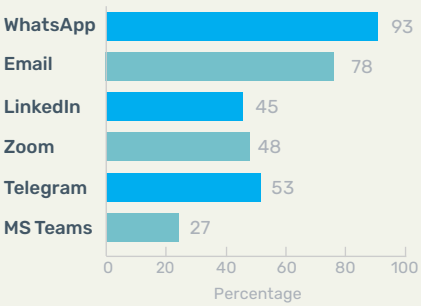
Connectivity and Application Usage

To determine their level of connectivity, app usage and digital skills, the poll asked respondents what devices they used and how they connected to the internet. The survey found that the overwhelming majority use a smartphone (97%), while 74% use a laptop, 47% have a smart TV, 31% use a tablet and 17% have a gaming console. Only 8% use a feature phone.

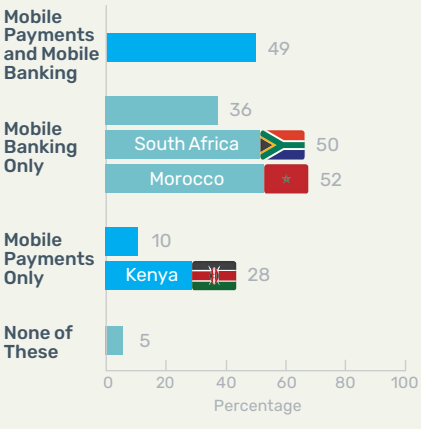
The top application for work use is WhatsApp (93%), followed by email (78%), LinkedIn (45%), Zoom (48%), Telegram (53%), X (33%) and Microsoft Teams (27%). Although ChatGPT was not included as an option, another 2024 survey by KnowBe4 found that this AI app was used by 42% of respondents, mostly for research and to save time.

WhatsApp was also the most-used app in respondents' private lives, with 97% using it to communicate with friends and family. Compared to the 2023 results, the 2025 survey found that work-related usage of WhatsApp rose slightly from 89% to 93%.

What applications do you use for work?



Do you use your mobile phone to do payments or banking?



In terms of mobile financial services, almost half of respondents (49%) use both mobile payments and mobile banking, 36% use mobile banking only, 10% use mobile payments only and 5% use none of these. The survey found that compared to the 2023 poll, the usage of mobile financial services (for both payments and banking) increased from 63% to 85%, with 95% of respondents using either a form of mobile payment, mobile banking or both.

In terms of country comparisons, Kenya leads in mobile payment adoption, with 28% of respondents using mobile payment apps, significantly above the continental average of 10%. When it comes to mobile banking, South Africa and Morocco show a higher-than-average use of mobile banking at 50% and 52% respectively, compared to the continental average of 36%. The high use of mobile financial transactions coupled with an increase in mobile threats, underscores the importance of mobile-centric security education. For instance, according to the Communications Authority of Kenya (CA), mobile application threats detected in the three months leading up to September 2024 surged by 333% compared to the same period the previous year in Kenya, with perpetrators primarily aiming to steal sensitive user data such as login credentials, and financial details.

Looking more broadly, the continued rise in mobile-data usage underscores Africa's mobile-first approach to internet connectivity. This trend has significant implications

for cybersecurity.

Increased digital financial inclusion: The rise in mobile banking and payments indicates greater financial inclusion through digital means, which is generally positive for economic development in Africa.

Increased attack surface: Firstly, more mobile usage and mobile financial services users means a larger attack surface for cybercriminals. Users are generally less vigilant on their smartphones and tablets compared to traditional computers, making them more susceptible to malicious attacks. Secondly, with more people conducting financial transactions on potentially unsecured and secondhand devices, the risk and impact of cybercrime have increased.

The growing trend of unlocked cellphone theft in the region highlights this issue. In South Africa, an average of 189 cellphones are stolen daily, with women being predominantly targeted. Stolen devices, particularly when unlocked at the time of theft, grant criminals access to sensitive data, including banking apps and personal information.

Blurred lines between personal and professional: The increase in WhatsApp usage for work (from 89% in 2023 to 93% in 2025) shows a further blurring of lines between users' personal and professional lives. This can lead to increased risks, as personal devices may not have the same level of security as corporate-managed devices.

Need for mobile-centric security education: The survey results suggest a pressing need for cybersecurity education that focuses specifically on mobile security and best practices for using personal devices for work-related tasks. There's also a clear need for cybersecurity education specifically tailored to mobile financial services, focusing on secure transaction practices and recognising financial fraud attempts.

Cybercrime Concerns

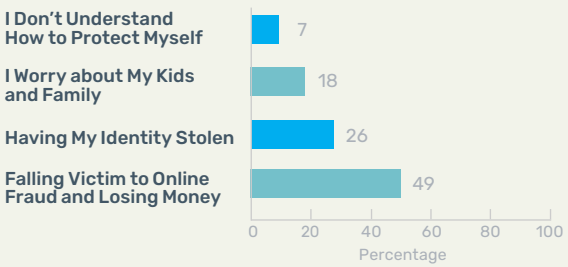
Cybercrime remains a big worry for the majority of respondents. Many noted that they were concerned about cybercrime, with 58% saying they were very concerned, 26% saying they were concerned.

When asked what concerns them about cybercrime, almost half of the respondents (49%) said they feared falling victim to online fraud and losing money, while 26% fear identity theft, 18% were concerned for their children and family and 7% said they did not understand how to protect themselves.

Comparing the 2024 and 2023 survey results, the most striking finding is that the number of respondents who are very concerned about cybercrime almost doubled from 29% to 58%. Fear of online fraud and losing money remain the top concern, with 49%. The significant jump in high-level concern about cybercrime has both

The number of respondents who are very concerned about cybercrime almost doubled from 29% to 58%

What concerns you about cybercrime?



positive and negative implications.

Increased awareness: This dramatic increase suggests that awareness campaigns and possibly personal experiences have significantly raised consciousness about cyber threats. This heightened awareness can potentially lead to more cautious online behaviour.

Potential for cybersecurity fatigue: However, such a high level of concern also risks leading to cybersecurity fatigue – a phenomenon where individuals become overwhelmed by constant security warnings and may ignore them.

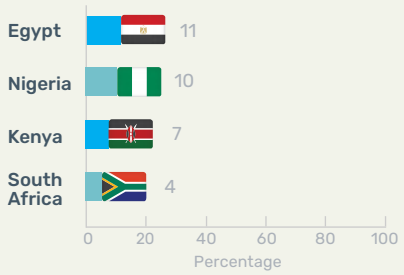
Focus on financial impact: The persistent focus on financial fraud suggests that economic consequences remain the most tangible and concerning aspect of cybercrime for most individuals. Future awareness campaigns could leverage this to make cybersecurity more relatable and urgent.

Personal Data Security

The percentage of respondents very unlikely to give away personal information dropped from 29% to 15%

Understanding of strong passwords decreased slightly from 62% to 58%

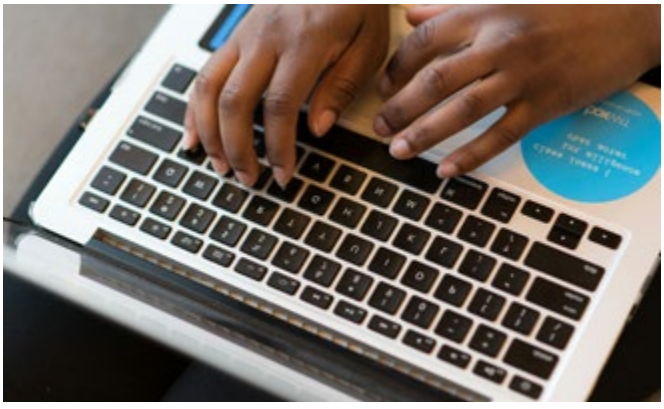
Respondents very likely to give away their personal information



Most respondents are hesitant to give away personal information, with 15% saying they tend not to share personal details, such as their identity number, 47% saying they would share this information only if there was a real need to do so and 24% parting with personal information if they can't avoid it. Worryingly, 14% are comfortable sharing personal information, with 8% saying they are likely to do so if they can get something in return, such as a discount, and 6% saying they share personal information all the time.

Comparing this year's results to the previous survey, the percentage of respondents very unlikely to give away personal information almost halved from 29% to 14%. This is a concerning trend and reveals the need for more training on personal security. This is further emphasised by the lack of understanding among respondents about what constitutes a strong password and multi-factor authentication. Understanding of strong passwords slightly decreased from 62% in 2023 to 58% in 2025, while comprehension of multi-factor authentication remained stable at around 58%.

Respondents were asked to identify a strong password from a number of choices. A worrying 26% selected P@$$word! Asked to define multi-factor authentication, 58% answered correctly, saying it was "using my password plus something I own". However, 22% said it was "entering my password twice for extra security" and 9% said it was using two different passwords.



Among respondents very likely to give away their personal information are those living in Egypt (11%), Nigeria (10%) and Kenya (7%). South African respondents were more cautious, with only 4% very willing to give away their personal data, compared to the average of 5.5%. This trend could indicate several issues, which are discussed below.

False sense of security: Increased familiarity with digital platforms might breed complacency. African users may feel more comfortable sharing personal information online, underestimating the risks involved.

Information fatigue: Constant requests for personal information in the digital age might normalise the practice, making people less cautious about sharing, especially if incentives like discounts are offered.

Lack of practical knowledge: While general concerns of cybercrime has increased, practical knowledge about protecting personal information may be lacking. This suggests a need for more specific, actionable education on safeguarding personal data.

Cybersecurity Awareness and Training

Over half of respondents said they had received cybersecurity training from their employers, with 33% strongly agreeing that the training was adequate. Asked whether they were aware of their information security roles and responsibilities at work, 40% fully agreed, 31% agreed somewhat and 11% weren't sure.

In terms of awareness and training, 43% felt very confident they could recognise a security incident if they saw one, 41% said they "somewhat agree" they could recognise a security incident, 13% weren't sure and 3% disagreed.

When checking to determine whether an email is legitimate, 54% said they only trusted emails from people they knew, 53% don't click on links or open attachments they weren't expecting and 25% check for bad grammar or spelling. To test respondents' knowledge further, KnowBe4 asked them to identify the name of a cyber threat that encrypts files and demands a payment to release data: 47% answered ransomware, 28% said trojan virus, 18% said drive-by download and 8% said Botnet.

Comparing this year's results to the previous survey, it is encouraging that both respondents' level of cybersecurity training and their ability to recognise cybersecurity threats has risen. Those who strongly agreed that their employer provided adequate cybersecurity training increased from 21% to 33%, while confidence in recognising security incidents improved, with 43% now "strongly agreeing" compared to 34% previously.

These improvements suggest positive developments in corporate cybersecurity culture, namely corporate investment and improved self-efficacy.

Corporate investment: The increase in perceived adequate training indicates that organisations are investing more in cybersecurity awareness. This could be driven by increasing regulatory requirements or a growing recognition of the importance of human factors in social engineering attacks.

Improved self-efficacy: Higher confidence in recognising security incidents suggests that training

is not only more widespread in Africa, but also more effective. Employees feel better equipped to deal with potential threats.

Issue of overconfidence: However, although increased confidence to spot cybersecurity threats among users is generally positive, it's important to ensure this confidence is well-founded. For example, while 83% of respondents expressed either high or some level of confidence in their ability to recognise a security incident if they saw one, 53% admitted they did not know what ransomware was. This disconnect highlights the critical issue of overconfidence, often linked to the Dunning-Kruger effect — a cognitive bias where individuals overestimate their competence in areas where they lack knowledge. In cybersecurity, this overconfidence can be particularly dangerous, as it creates a false sense of preparedness, leaving individuals and organisations more vulnerable to threats they may not fully understand or anticipate.

Cybercrime Experiences

More than half of respondents (51%) said they had previously had a virus infection on their computer, 35% had lost money due to a scam or con artist, 32% had clicked on a phishing email, 23% had been scammed on a phone call and 37% had fallen for fake news or a disinformation campaign.

Comparing the 2023 survey to the 2025 results, phishing victims rose from 26% to 32%. Virus infection experiences remained stable at around 51%, while financial losses due to scams increased slightly from 32% to 35%.

These figures paint a complex picture of the cybercrime landscape in Africa.

Sophistication of phishing attacks: The increase in phishing victims despite increased awareness among respondents suggests that phishing attacks are becoming more sophisticated and harder to detect. It also shows a gap between awareness and practical application of cybersecurity knowledge.

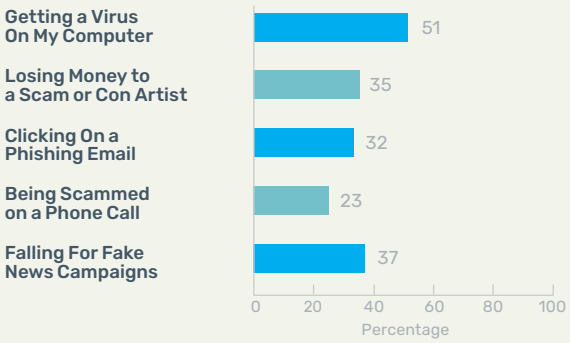
Persistent threat landscape: The stability in virus infections and slight increase in financial losses suggest that the overall threat level remains high. Cybercriminals are adapting their tactics to overcome improved awareness and technical defences.

Need for practical training: These results highlight the need for more hands-on, practical cybersecurity training in Africa that goes beyond theoretical knowledge to develop real-world skills in identifying and avoiding threats.

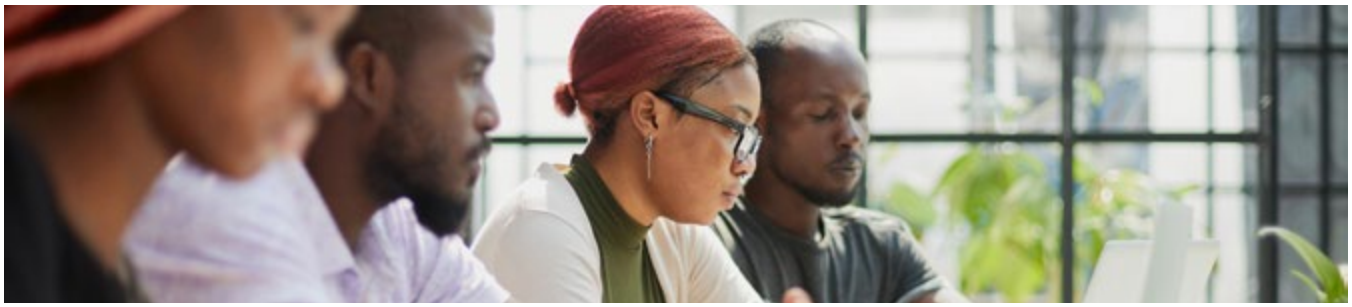
Phishing victims rose from 26% to 32%

Financial losses due to scams increased from 32% to 35%

Has the following ever happened to you?



Conclusion and Recommendations



The 2025 survey reveals a nuanced picture of cybersecurity awareness in Africa. Overall, there are positive trends in awareness and corporate training, as well as an increase in the adoption of mobile banking and payments. However, there are also concerning developments, particularly in personal information security and the practical application of cybersecurity knowledge.

While cybersecurity awareness is growing in Africa, there is still a significant need for more comprehensive and effective human risk management and training programmes. The high use of mobile devices and applications, particularly for financial transactions, underscores the importance of mobile-centric security education. Despite increased concern about cybercrime, there are gaps in knowledge and practice that need to be addressed to improve overall cybersecurity posture across the continent.

Key recommendations for future cybersecurity initiatives in Africa include bridging the gap between user awareness and behaviour, focusing on mobile-centric, practical security education, and establishing programmes for continuous reinforcement. These initiatives should also integrate innovative approaches to human risk management, such as digital mindfulness, second-nature vigilance, and adaptive trust strategies.

Bridge the awareness-behaviour gap: While increased concern about cybercrime is encouraging, it's critical to transform this awareness into actionable security behaviours. This includes equipping individuals to recognise and respond effectively to phishing, protect personal information, and apply vigilance in digital interactions. Programmes should leverage adaptive trust mechanisms—training individuals to discern when trust is warranted online and when caution should prevail.

Mobile-centric, practical security education: Tailored cybersecurity training for Africa's mobile-first population is vital. Programmes must address the unique challenges of securing mobile financial transactions and mitigating risks associated with smartphones and tablets. Emphasising interactive, scenario-based training will help users internalise security principles, fostering second-nature vigilance in their digital habits.

Regular reinforcement: To counter cybersecurity fatigue, organisations must prioritise continuous reinforcement of best practices. This should focus on building security-conscious habits over time through regular updates, engaging reminders, and practical exercises. Introducing digital mindfulness into training frameworks can help users develop heightened meta-awareness, enabling them to pause, assess, and make informed decisions in risky online situations.

A new paradigm for human risk management: The African cybersecurity landscape requires a holistic and adaptive approach to human risk management. By combining traditional training with techniques like digital mindfulness, fostering second-nature vigilance, and cultivating adaptive trust mindsets, we can equip individuals to navigate digital risks more confidently. By embracing these recommendations, African organisations can ensure their cybersecurity initiatives are not only reactive to immediate threats but also sustainable in building long-term resilience and security-conscious cultures.

References

Business Daily (2024). Kenya smartphone attacks quadruple as hackers target Android gadgets https://www.businessdailyafrica.com/bd/corporate/technology/kenya-smartphone-attacks-quadruple-4818812?

Dunning, D. (2011). The Dunning–Kruger Effect: On Being Ignorant of One's Own Ignorance https://www.sciencedirect.com/science/article/abs/pii/B9780123855220000056

Interpol (2024). INTERPOL AFRICAN CYBERTHREAT ASSESSMENT REPORT 2024 https://www.google.com/url?q=https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%2520Cyberthreat%2520Assessment%2520Report_2024_complet_EN%2520v4.pdf&sa=D&source=docs&ust=1733755105628083&usg=AOvVaw0k1aygOrKHa8vF-05StJbw

Institute for Security Studies ISS (2023). Cellphone theft: another indicator of South Africa's policing gaps https://issafrica.org/iss-today/cellphone-theft-another-indicator-of-south-africas-policing-gaps?

KnowBe4 African Cybersecurity and Awareness Report (2023). https://info.knowbe4.com/research-2023-african-cybersecurity-awareness-report

KnowBe4 Generative AI in the Middle East and Africa Survey (2024). https://www.knowbe4.com/hubfs/Generative-AI-in-the-Middle-East-and-Africa-Survey_EN-GB.pdf

KPMG (2022). Africa Cyber Security Outlook. https://assets.kpmg.com/content/dam/kpmg/ke/pdf/thought-leaderships/2022/KPMG%20Africa%20Cyber%20Security%20Outlook%202022.pdf

SABRIC (2024). ANNUAL CRIME STATISTICS 2023. https://www.sabric.co.za/media/vjyn5f4d/sabric-annual-crime-stats-2023-2.pdf

United Nations (2021). Young People's Potential, the Key to Africa's Sustainable Development. https://www.un.org/ohrlls/news/young-people%E2%80%99s-potential-key-africa%E2%80%99s-sustainable-development

Free Phishing Security Test

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

Free Email Exposure Check

Find out which of your users emails are exposed before the bad guys do

Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization

Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain

Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk. For more information, please visit www.KnowBe4.com

knowbe4

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