KnowBe4
Human error. Conquered.

KnowBe4 African Cybersecurity & Awareness Report 2023

by Anna Collard

SVP Content Strategy &
Evangelist KnowBe4 Africa

KnowBe4 African Cybersecurity & Awareness Report 2023

Table of Contents

KEY FINDINGS

Since 2019, KnowBe4 has conducted annual Africa-wide surveys to explore whether or not people living on the continent were prepared for the current cyberthreats, what the state of cryptocurrency and blockchain security is and how organisations instill a culture of cyber throughout Africa.

The latest surveys sought to unpack the areas of weakness that should be of concern to both individuals and organisations, shining a light on those areas that need to be addressed in 2023 to ensure robust and strategic cybersecurity.

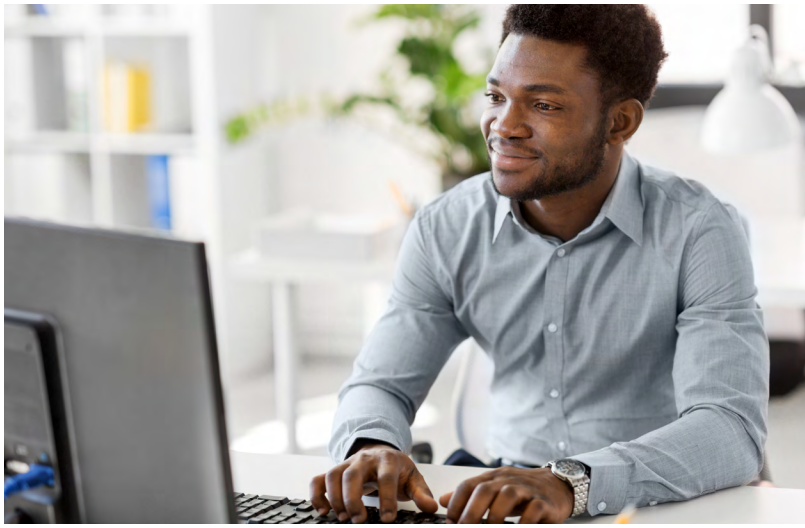
With a median age of just 19.7 years[1], Africa has the youngest population in the world. And Africa's growing youth is demanding access to global connectivity while driving technology adoption and digitalisation: mobile smart device ownership is growing exponentially, social media use is increasing and the Internet of Things (IoT) is becoming a reality. According to the IMF, sub-Saharan Africa is the only region in the world where nearly 10% of its gross domestic product is generated through mobile money. People across the continent depend on their mobile devices for remittances, salaries, payments, bills and shopping.

KnowBe4's Africa End User Cyber Awareness survey 2022 uncovered that 71% of the respondents from eight African countries use their mobile data to access the internet, while 63% use their mobile phone for mobile banking and payments.

With this demonstrated growing prosperity and digitisation, also comes new risks and vulnerabilities that could undermine the progress. More work needs to be done by both companies and governments alike to address Africa's users level of understanding with regards to cybersecurity and protect its citizens from cybercrime.

KnowBe4's Africa End User Cyber Awareness surveys from 2020 to 2022 uncovered that the pandemic has played a major role in influencing working behaviours and patterns amongst the 800 respondents from eight African countries. The latest 2022 survey data shows that:

- 32% of respondents will continue to work from home.
- 68% were concerned about cybercrime, however, many lacked some very basic understanding of what type of threats they are exposed to.
- 57% of respondents did not know what a ransomware attack is.
- 21% have experienced a social engineering attack over the phone (vishing) and 32% have lost money because they fell victim to a scam.
- Only 38% of the respondents believe they fully understand their security roles and responsibilities and only 21.25% strongly agreed that the cybersecurity training they received from their employers was adequate.
- As many as 36% said they had fallen victim to a crypto scam, and 57% knew people who had been victims of such scams.



1 https://www.worldometers.info/world-population/africa-population/

- In Africa, the Initial Baseline Phishing Security Test results are at an average of 31%. That means one out of three employees is likely to click on a suspicious link or email or comply with a fraudulent request.
- The number one reason for people making security mistakes, such as clicking on a phishing email, was cited as lack of awareness or training (52%), followed by distraction, multitasking and cognitive overload (38%).

METHODOLOGY & REFERENCES

This report summarises the results from multiple KnowBe4 polls, surveys and research reports:

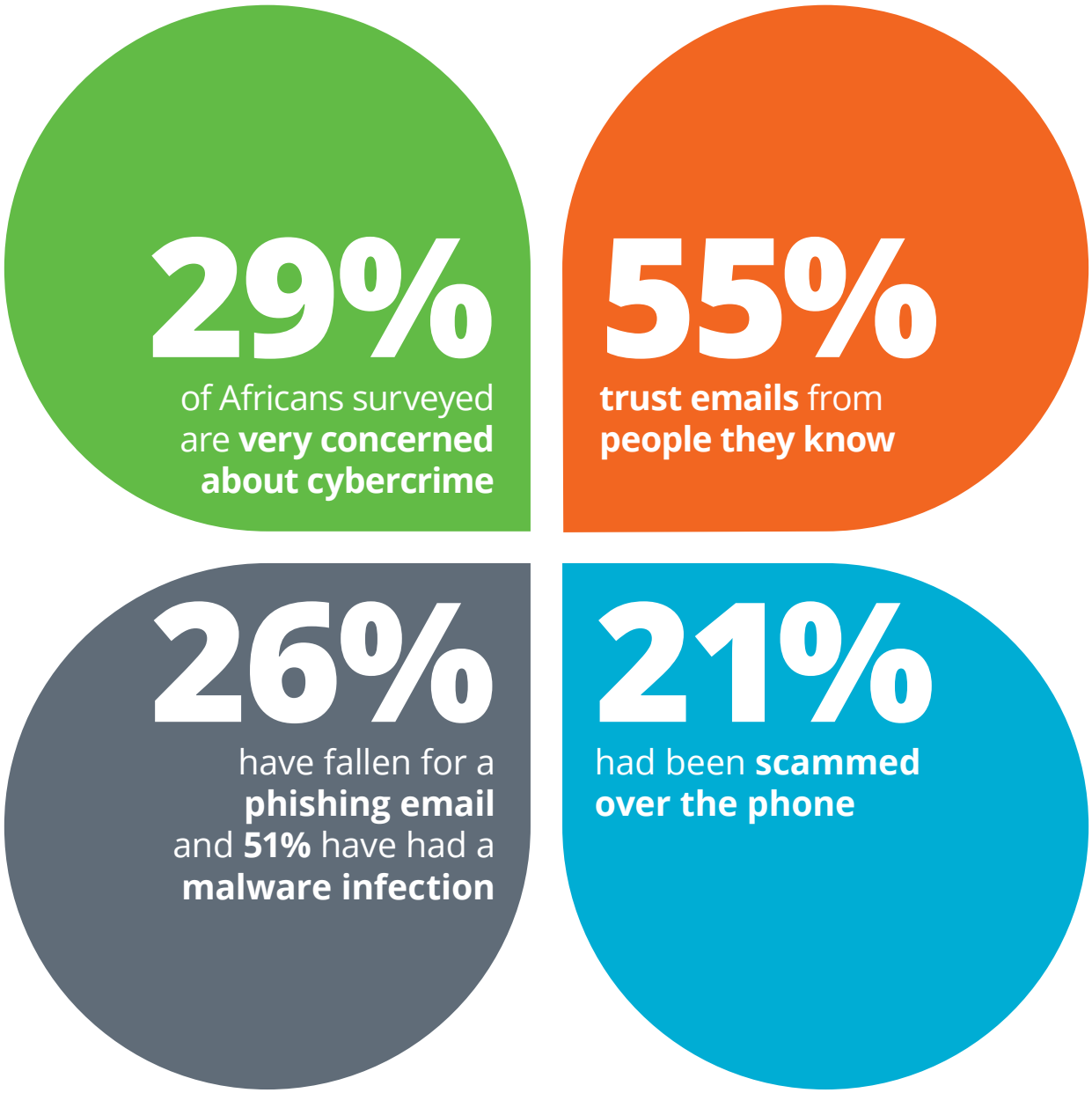
Survey / Poll	Countries	Number of Respondents	Date
KnowBe4 Africa End User Security Awareness Polls • December 2022 • December 2021 • December 2020 • December 2019	Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria and South Africa	800	December 2022 December 2021 December 2020 December 2019
KnowBe4 Africa's use of Cryptocurrency poll	Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria and South Africa	800	November 2022
KnowBe4 Deepfakes in Africa poll	Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria and South Africa	800	November 2022
ITWeb and KnowBe4 Mindfulness in Cybersecurity survey	South Africa	193	August 2022
ITWeb and KnowBe4 Metaverse, Blockchain and Web3 in South Africa survey	South Africa	176	July 2022
KnowBe4 Phish-prone Percentage Report	Global	9.5 Million (Global) 7490 (Africa)	July 2022
KnowBe4 Security Culture Report	Global	530,000 (Global) 14,121 (Africa)	March 2022
ITWeb and KnowBe4 Security Culture in South Africa survey	South Africa	182	January 2022

AFRICA END USER SECURITY AWARENESS POLL

In December 2022, KnowBe4 conducted an Africa-wide survey by polling 800 people across Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria and South Africa, just as it did in 2021. The results showed that many of the challenges and considerations impacting users in 2021 have remained unchanged.

The survey uncovers the changing shape of African cybersecurity by asking the difficult questions. Are you concerned about cybercrime? Would you give away your personal information? Would you pay to release your data if it was encrypted in a cyber attack? What type of cybercrime did you experience?

The findings, taken from individuals working across multiple industries and in various roles, showed a continent that is adapting and changing to the growing cyber threats, but that still has a long way to go to effectively mitigate risk.



Connectivity

To determine their level of connectivity, digital device use and digital skills, the poll asked respondents what devices they used, and how they connected to the internet.

97% of the participants use a smartphone, 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, and 1% said they had none of these devices.

Question: I use the following devices

#	Answers	Respondents (%)
A1	Feature Phone	8%
A2	Smart Phone	97%
A3	Laptop Computer	74%
A4	Tablet	31%
A5	Smart Television	47%
A6	Gaming Console	17%
A7	None of the above	<1%

The top application in use for work is WhatsApp (89%), followed by email (80%), Facebook (59%), Telegram (46%), Instagram (45%), Twitter (42%), Zoom (42%), LinkedIn (36%), Microsoft Teams (18%), Snapchat (18%), Slack (5%), WeChat (4%), Signal (4%) or other tools (1%).

Question: I use the following applications for work

#	Answers	Respondents (%)
A1	WhatsApp	89%
A2	Telegram	46%
A3	Signal	4%
A4	Instagram	45%
A5	Facebook	59%
A6	Snapchat	18%
A7	WeChat	4%
A8	Twitter	42%
A9	LinkedIn	36%
A10	Email	80%
A11	MS Teams	18%
A12	Zoom	42%
A13	Slack	5%
A14	Other	1%

WhatsApp was also the most-used app in respondents' private lives, with 97% using it to communicate with friends and family. For personal use, Facebook ranks second (78%), followed by Instagram (57%), email (46%), Telegram (40%), Twitter (39%), Snapchat (25%), LinkedIn (14%), Zoom (12%), Signal (3%), Microsoft Teams (2%) and other tools (1%).

71% access the internet through their mobile networks, overlapping with the 71% who access the internet through home Wi-Fi, and 36% who go online through work/office networks. 12% access the internet at internet cafes and 15% use free Wi-Fi at public places.

Most respondents (63%) use both mobile payments and mobile banking, 16% use mobile payments only, 13% use mobile banking only and 8% use none of these.

Risks of using WhatsApp for both work and personal lives

The survey shows that WhatsApp is used extensively in Africa for work, more so than in most of other developed countries, yet there is generally a lack of corporate advice and awareness about the risks of using WhatsApp or other consumer apps in a corporate setting such as:

- With WhatsApp's group messaging, it becomes very hard to understand, yet alone control with whom your data can be shared.
- The popularity of WhatsApp makes it an attractive target for cybercriminals who are inventing new scams and attack techniques against these apps on a daily basis.
- Facebook/Meta does not permit 'non-personal use' in their terms and includes data-sharing policies that most organisations will be uncomfortable with.
- And although WhatsApp is frequently targeted by cybercriminals, the risks are not limited to information security only: The use of messaging apps for both work-related and personal communications blurs the boundaries between work and personal time. The lack of disconnect from work life as people may be communicating on WhatsApp over weekends and evenings can put a company at risk of liability for causing workplace stress and mental health problems.

Cybersecurity Awareness

67% respondents said they were generally concerned about cybercrime, with 29% saying they were very concerned, and 38% saying they were concerned.

19% said they were somewhat concerned, but did not understand the threats or how to mitigate them. Only 7% said they did not believe cybercrime affected them personally, and their work took care of it, while another 7% said they are not at all concerned and felt very safe.

When asked what concerns them about cybercrime, most respondents (51%) said they feared falling victim to online fraud and losing money. 24% fear identity theft, 14% were concerned for their children and family, 10% said they did not understand how to protect themselves, and 1% said they had other concerns.

Question: What concerns you about cybercrime?

#	Answers	Answers (%)
A1	I don't understand how to protect myself	10%
A2	I worry about my kids / family	14%
A3	Having my identity being stolen	24%
A4	Falling victim to online fraud / losing money	51%
A5	Other	1%

When checking to determine whether an email is legitimate, 55% said they only trusted emails from people they knew, 54% do not click on links or open attachments they were not expecting and 27% check for bad grammar or spelling as a sign the mail is not legitimate. 31% Google the sender or topic to see if it is a scam, 23% hover over links to see their origin, but only 11% do all the listed checks.

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. 43% answered correctly with Ransomware, 32% chose Trojan Virus, 18% said Drive-By Download and 8% said Botnet. This shows that people are generally still quite confused or unsure about the meaning or the terminology of digital threats.

Question: What is a cyber threat that encrypts your files and demands payments from you to release your data called?

Answers	2019	2020	2021	2022
Trojan Virus	35%	33%	33%	32%
Botnet	9%	5%	7%	8%
Ransomware	37%	48%	46%	43%
Drive-by-Download	20%	14%	15%	18%

Respondents were then asked to identify a strong password from a number of choices. 62% selected *DSM@8043&!*. A worrying 20% selected *P@$$word!* 16% chose *Summer#123* and 3% chose *Grandma1959*. 6% said none of these were strong passwords.

Fortunately, the majority of respondents could identify two-factor authentication (60%) in 2022 compared with 48% in 2019. 20% said it was 'Entering my password twice for extra security', 8% said it was Captcha generators, 9% said it was using two different passwords, and 4% said it was using a password manager.

Question: Two-factor authentication is?

Answers	2019	2020	2021	2022
Entering my password twice for extra security	24%	20%	21%	20%
Using my password plus something I own, such as an OTP generator	48%	61%	61%	60%
Captcha generators	12%	6%	6%	8%
Using two different passwords	12%	11%	8%	9%
Using a password manager	5%	5%	3%	4%

The stats above could be interpreted in that the cybersecurity industry and media have done a great job at raising awareness about cybercrime—but made less progress in terms of equipping people to understand what cybercrime actually is, and how they can defend themselves better—or what to do if they do fall victim. More work needs to be done in educating people on how to protect themselves, preferably with practical advice and less confusing terminology.

Organisational Awareness

While over half said they had received cybersecurity training from their employers, only 21% strongly agreed that the training was adequate. 34% agreed 'somewhat' that their cybersecurity training was adequate, 17% were not sure, 13% disagreed 'somewhat', 10% strongly disagreed, and 5% answered 'none of the above'.

On whether they were aware of their information security roles and responsibilities at work, 38% fully agreed, 33% agreed 'somewhat', 13% were not sure, 6% disagreed 'somewhat', and 11% fully disagreed.

While the survey did not delve into the definitions of "adequacy", it is important to note that good or adequate content needs to be well produced, delivered well, in a timely manner and relevant to the role the person is involved in. For example, if someone works 100% from the office, there is little value in sharing content about travel security. Even if the content is well produced and accurate, the recipient will feel like it is not relevant and hence inadequate in relation to their job. Corporate awareness training programs need to be mindful about correctly timing their interventions. An accountant trying to file year end returns will not be able to spend an hour watching awareness videos.

Effective training includes real-time coaching messages in response to users' security mistakes or risky behaviour based on user event data from an existing security stack to remind people in the moment when it matters most. This helps to strengthen security culture by enabling real-time coaching of your users in response to their risky security behaviour.

Types of Cybercrime Experienced

The research found that, in 2022, 34% felt very confident they could recognise a security incident if they saw one (44% in 2021), while 45% were somewhat confident.

Despite this confidence, 26% have clicked on a phishing email, 51% have had a virus infection on their computer, and 32% have lost money to a scam or con artist. 21% have been a victim of social engineering. This is a cause for concern, as email is still one of the most successful methods of cyber attack. People are quick to click on links or attachments from people or brands they think they know, as many do not realise that the account may have been spoofed or hacked.

Question: Has any of the below ever happened to you?

#	Answers	Respondents (%)
A1	I have clicked on a phishing email	26%
A2	I have forwarded a spam or hoax email	17%
A3	I've had a virus infection on my computer before	51%
A4	I've been scammed over the phone before (social engineering)	21%
A5	I've lost money due to a scam / con artist	32%
A6	None of the above	17%

To establish a clear picture of the security mindset and landscape, the survey asked respondents whether they had been affected by cybercrime while working from home. Most (80%) said they had not been affected by cybercrime while working from home. 20% said yes (compared to 32% last year).

Among the 20% who were affected by cybercrime while working from home, a multitude of scams and cybercrimes occurred, ranging from being tricked in crypto investment schemes and identity theft, to accidentally downloading viruses and being hacked.

These answers show that people are exposed to a myriad of different attack vectors while working from home or remotely. We need to continually educate people on these attack varieties and latest scams.

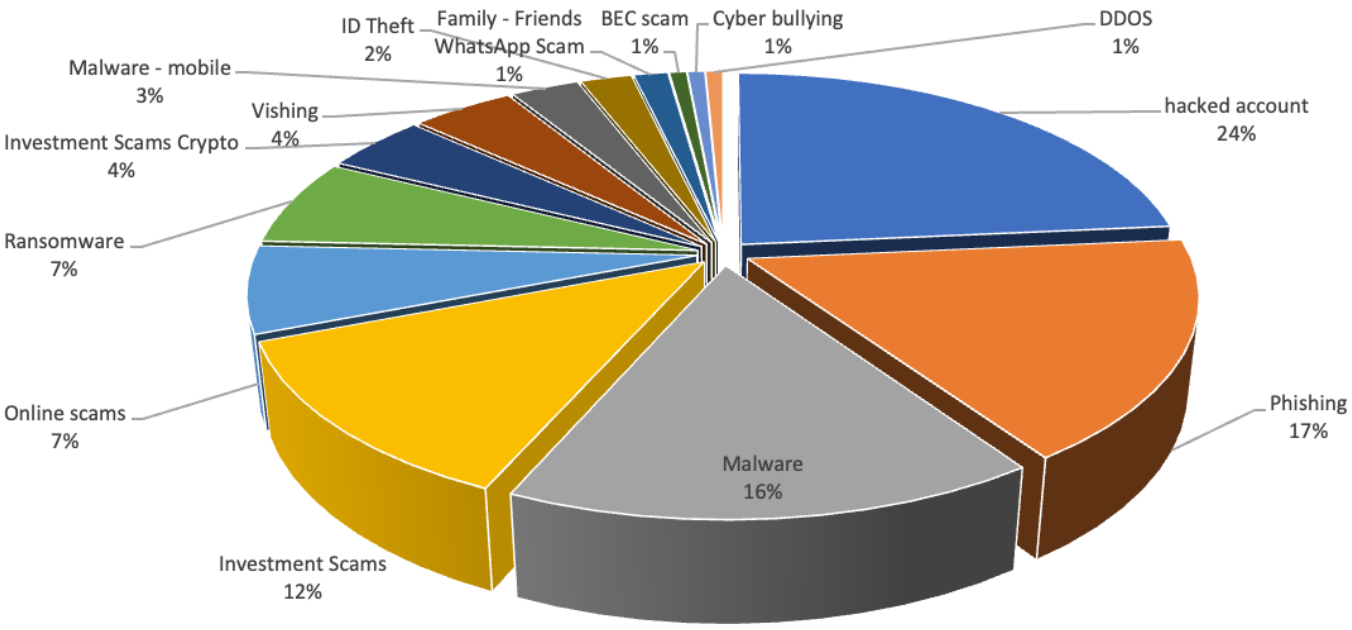


Figure: Types of attacks experienced while working from home.

Most survey respondents said they were hesitant to give away personal information, with 29% saying they tended not to share personal details such as their identity number, and 51% saying they would share this information only if there was a real need to do so, and they understood what it was being used for. 13% said they parted with personal information if they could not avoid it.

Worryingly, 7% are comfortable sharing personal information, with 4% saying they are likely to do so if they can get something in return—such as a discount, and 3% saying they share personal information all the time.

Question: How likely would you give away your personal information?

#	Answers	Answers (%)
A1	1. I tend not to share my personal details as I'm concerned about my privacy	29%
A2	2. If I can't avoid it	13%
A3	3. Only if there is a real need for it and I understand what it is being used for	51%
A4	4. Likely, if I can get something in return like a discount	4%
A5	5. Very likely, I do it all the time	3%

Deepfakes

The survey polled 800 adults in Mauritius, Egypt, Botswana, South Africa and Kenya to determine their awareness of the risk of Deepfakes.

Nearly three-quarters of them (74%) said they had believed a communication (email/direct message), or a photo or video to be true, and later discovered it was fake.

51% of respondents said they were aware of Deepfakes, while 28% were not, and 21% were unsure, or had a little understanding of what they were.

While respondents were not 100% clear on what Deepfakes were, most (72%) said they did not believe that every photo or video they saw was genuine. However, 28% believed 'the camera never lies'.

On the types of communications with a friend or contact they would most likely consider legitimate, 67% trusted WhatsApp/Direct messages, 43% would trust a video, 42% would trust an email, 39% trust a voice note, and 13% would trust a social media post.

On the question 'Would you believe a video showing an acquaintance in a compromising situation, even if this would be out of character for them?', most people would be hesitant to do so. Nearly half (49%) said they would speak to the acquaintance in person to get to the bottom of the matter, and 14% said they would never believe such a video. However, as many as 21% said they would believe the video, and 17% said that while they would be surprised, they believe a video is impossible to fake.

Question: Would you believe a video showing an acquaintance in a compromising situation, even if this would be out of character for them?

SINGLE SELECTION

Q4. Would you believe a video showing an acquaintance in a compromising situation, even if this would be out of character for them?

#	Answers	Answers (%)
A1	Yes	21%
A2	Never	14%
A3	I'd be surprised, but video is impossible to fake	17%
A4	I'd speak to them in person to get to the bottom of it	49%

The response was similar when asked if they would believe a video showing a high profile person in a compromising situation, even if this would be out of character for them. 50% said they would give them the benefit of the doubt, and watch legitimate news for confirmation, and 19% said they would never believe such a video. However, a total of 36% would believe the video, with 13% of them saying that video was impossible to fake.

On the question 'Would you act on an email, recorded voice clip or video from your boss, instructing you to carry out a task they wouldn't normally ask you to do?', most respondents would be cautious. 57% would speak to the boss in person to confirm the instruction, and 23% said they would not do so, especially if the instruction involved large sums of money or anything out of the ordinary. However, 21% would follow the instructions without question.

Asked to select clues they think would give away a fake in written communication, respondents said the language, spelling and expressions used aren't the person's usual style (72%), the request or the message is out of the ordinary or unexpected (63%) or other clues (5%), such as the way the person was addressed, the timing of the communication being wrong, or the facts in the communication not corresponding with internal knowledge.

On clues in audio communication, most respondents (75%) selected 'The words, tone and accent sound unlike the person being emulated, followed by 'The speech doesn't flow naturally' (54%), and 'The request or the message is out of the ordinary, alarm signals should go off' (45%).

When asked 'What clues do you think would give away a Deepfake in a video?', respondents selected 'their mouth movements don't sync with the audio' (73%), 'The request or the message is out of the ordinary, alarm signals should go off' (49%), 'Their head movements seem odd' (49%), 'The person doesn't blink' (46%), and 'The person's skin colour looks unnatural' (44%).

Adoption of Cryptocurrencies

The vast majority of respondents (81%) knew what cryptocurrency was, with a further 15% saying they knew of it but were not clear on how it worked, and 4% saying they did not know what it was.

Most respondents were keen to invest in cryptocurrency, with 52% having done so already and 21% saying they would like to. 27% had not done so.

The primary goal for their investments was long term profit (69%), followed by quick profit (39%), finances not tied to local banks (18%) and to benefit from next-gen trading and transactions (16%).

Among those who had invested in cryptocurrency, most (47%) selected a broker and exchange platform that had been recommended to them. 40% used a broker and exchange platform they had read about in advertising or articles, 38% made their choice based on influencers and social media promotions, and 33% found them through online search. 4% said an agent had contacted them.

As many as 36% said they had fallen victim to a crypto scam, and 57% knew people who had been victims of such scams. The most common scam reported, at 59%, was being tricked into investing

through a broker or platform that was not legitimate. 41% who were scammed said they had been tricked into sending currency to a compromised wallet or direct to a scammer, 22% had invested via a bogus app, and 13% had been tricked into sharing their private keys. Most lost under USD500 to the scammers, but 14% had lost over $500.

Despite this, the vast majority who had been scammed would invest in crypto again. Only 9% said they would never do so again, while 36% would definitely, or had already invested in crypto again, and 55% would do so, but be more cautious in future.

Emerging NFTs

The survey also looked into Non Fungible Tokens (NFT) projects, finding that 54% of respondents were aware of them, 27% were not, and 19% were not clear on how NFTs worked.

18% had already invested in NFTs, and 25% planned to, while 57% had not done so. 9% had already fallen victim to an NFT scam.

Emerging technologies and new ecosystems will always lure people with promises of quick returns. And this is precisely the environment where scammers and criminals thrive.

We are not here to tell people what they can and cannot do with their own money and investments, but we have to showcase and warn people about some of the dangers and scams that can be found within the crypto ecosystem.

METAVERSE, BLOCKCHAIN AND WEB3 IN SOUTH AFRICA

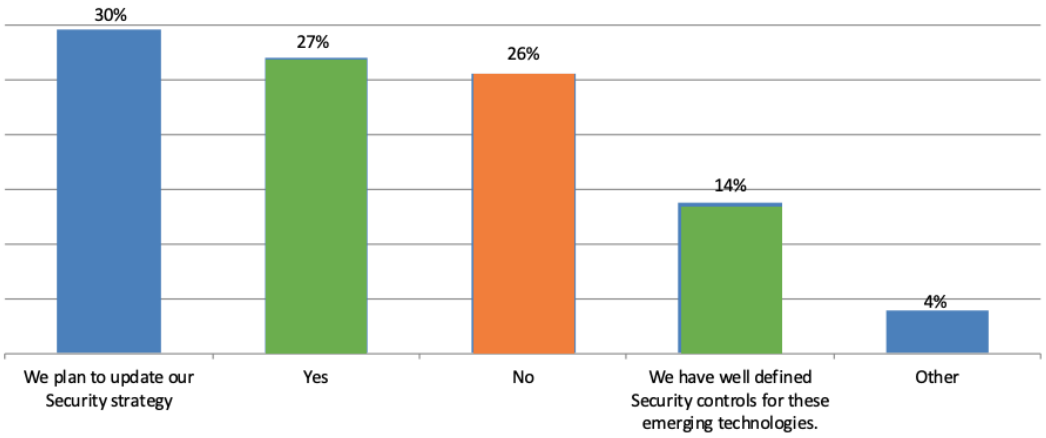
In partnership with ITWeb, KnowBe4 conducted a survey across 176 South African organisations on the use of Metaverse, Blockchain and Web3.

Just over half (54%) of the survey's respondents said they had plans to participate in the metaverse. The majority of respondents (82%) said their businesses did not use blockchain technology, with only 18% saying that they did. However, 83% said that their companies planned to deploy blockchain technology.

When asked whether they were excited about the opportunities of Web 3.0, 57% of respondents said yes, they were a proponent of a more decentralised future internet; 26% said they did not know what it was about; and 15% said they did not believe the technology catered for the hyped-up promises of Web 3.0.

When asked if they were considering the metaverse, Web 3.0 or Blockchain in their security plans, 27% said 'yes', 26% said 'no' and 30% of respondents said they planned to update their security strategy. 14% said they had well defined security controls for these emerging technologies.

Question: Are you considering the Metaverse, Blockchain or Web3 in your security plans?



THE LINK BETWEEN MINDFULNESS AND CYBERSECURITY

In partnership with ITWeb, KnowBe4 conducted a survey across 193 South African organisations on cyber stress and wellness during August 2022. The objective of the survey was to assess how a changing environment is impacting IT professionals and corporate workers, and whether mental stress and burnout are increasing cyber risk.

The majority of respondents (82%) said staff mental health and wellbeing were important in their organisation.

The number one reason for people making security mistakes, such as clicking on a phishing email, was cited as lack of awareness or training (52%), followed by distraction, multitasking and cognitive overload (38%) and stress or feeling overworked or overwhelmed (36%).

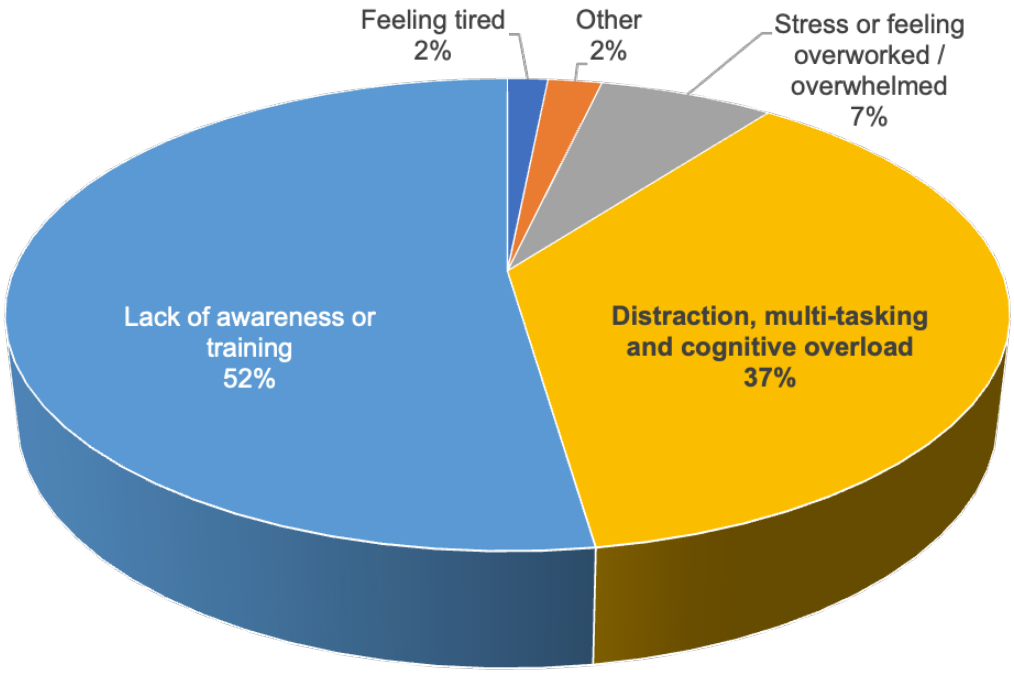


Figure: Reasons people make security mistakes, South Africa ITWeb & KnowBe4 survey 2022

70% of respondents said that the most effective way to improve their company's security culture would be more security awareness and training. This was followed by in-the-moment training such as phishing simulations (54%), offering people mindfulness tools and training to be less distracted (49%) and behaviour-based monitoring and interventions (49%).

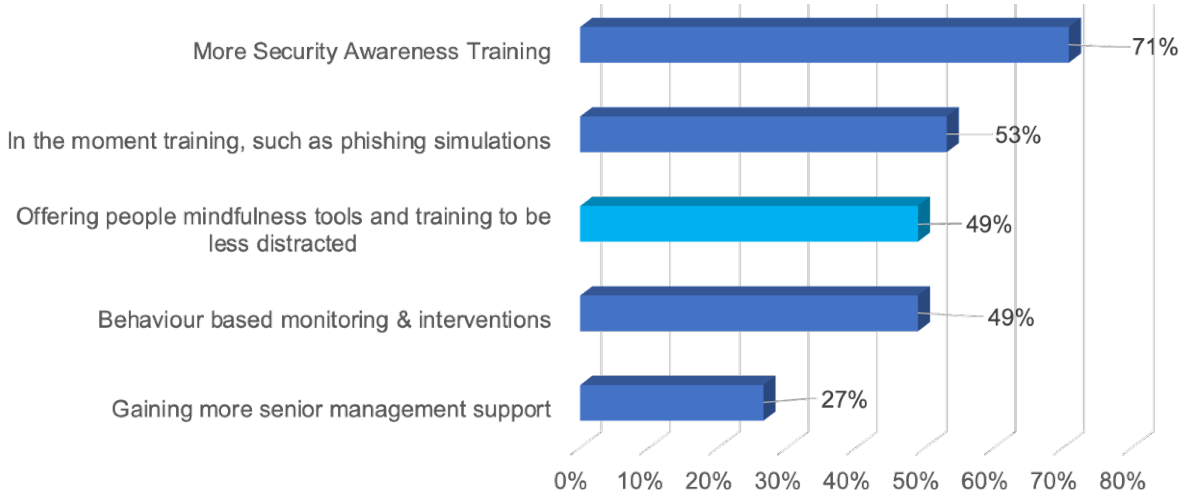


Figure: Ways to improve security cultures, ITWeb and KnowBe4 survey South Africa 2022

View the full report

KNOWBE4 SECURITY CULTURE REPORT

Security culture is the ideas, customs and social behaviours of an organisation that influence their security. Where security awareness is one's knowledge of risk, security culture encompasses knowledge as a starting point, but also includes seven additional critical dimensions: attitude, behaviour, cognition, communication, compliance, norms and responsibilities.

The 2022 KnowBe4 Security Culture Report is the largest study of its kind, measuring organisations' security cultures and surveying more than 530,000 employees across 2,910 organisations worldwide.

Dimension	Definition
Attitudes	The feelings and beliefs that employees have toward the security protocols and issues
Behaviours	The actions and activities of employees that have direct or indirect impact on the security of the organisation
Cognition	Employees' understanding, knowledge and awareness of security issues and activities
Communication	The quality of communication channels to discuss security-related topics, promote a sense of belonging and provide support for security issues and incident reporting
Compliance	The knowledge of written security policies and the extent that employees follow them
Norms	The knowledge of and adherence to unwritten rules of conduct in the organisation
Responsibilities	How employees perceive their role as a critical factor in sustaining or endangering the security of the organisation

The research provided a security culture score, which is a measurement that describes the overall security culture of an organisation. By aggregating the scores of organisations in each industry, we can learn how each industry compares across the seven outlined dimensions of security culture. In general, a score below 80 is considered moderate, and a score below 60 is poor to moderate.

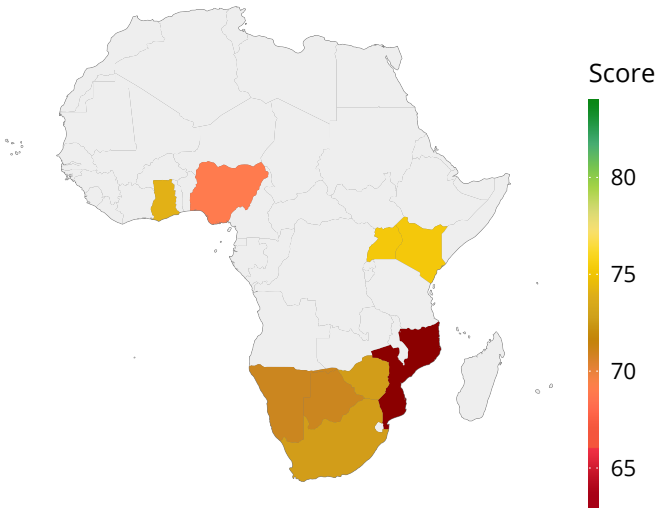
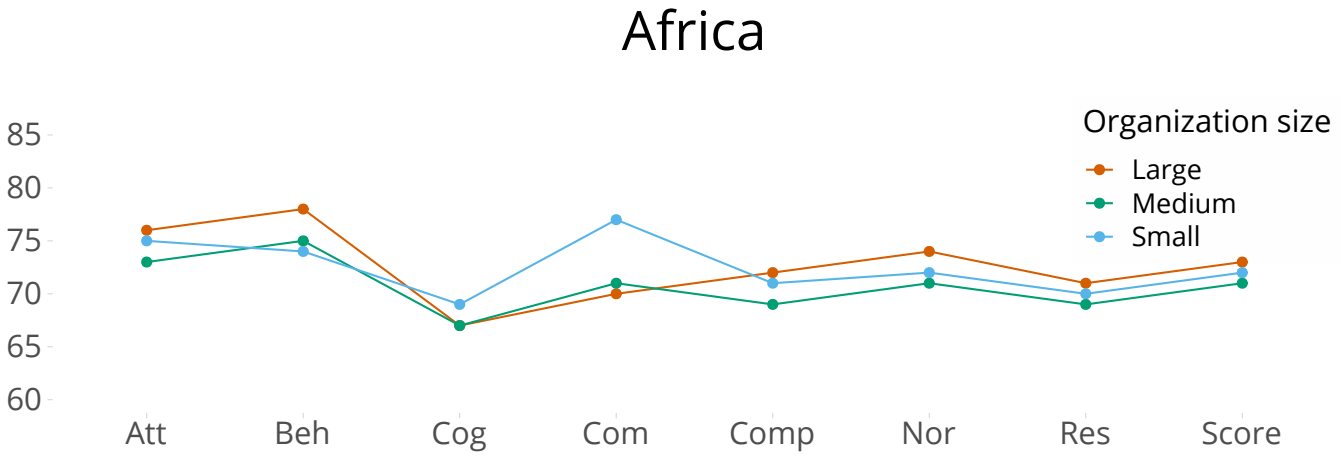


Figure: Security culture score in Africa. The sample size varies from country to country. For more details, please refer to the method section.

Security Culture in Africa

In Africa, there is a tradition and interest in security culture, especially in South Africa (73), where we expected a higher level of security culture than was achieved. In the other countries in Africa where we have data, we see very wide variations in security culture, which is likely explained by limited sample sizes. We expect to see more African countries measuring security culture in the future. In the meantime, we urge organisations and governments to focus on the human aspects of security and invest in education and training.



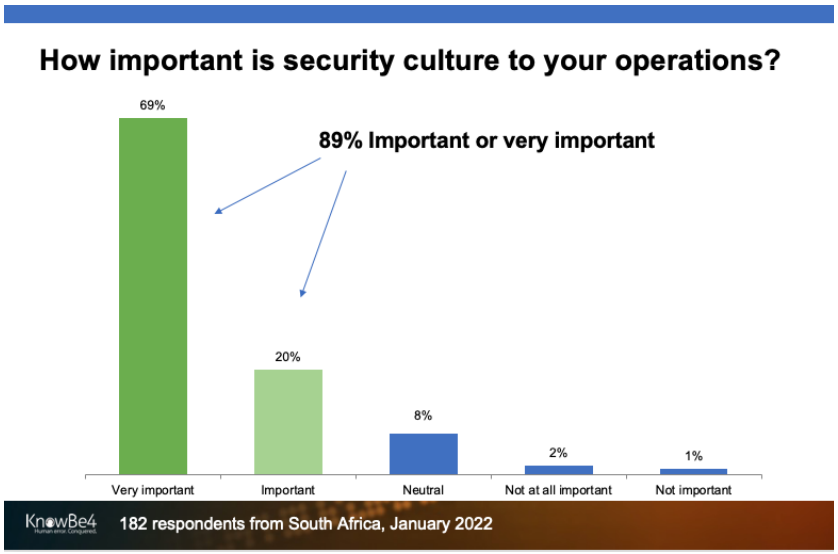
In Africa, we see that large organisations generally do better than others when it comes to security culture. There are two notable differences: the Cognition and Communication dimensions, where small organisations perform much better than the others. Africa has a sample size of 52 organisations with 14,121 employees.

[Access the full KnowBe4 Security Culture 2022 report here]

Security Culture in South Africa

In partnership with ITWeb, KnowBe4 conducted a survey across 182 South African organisations on security culture during January 2022.

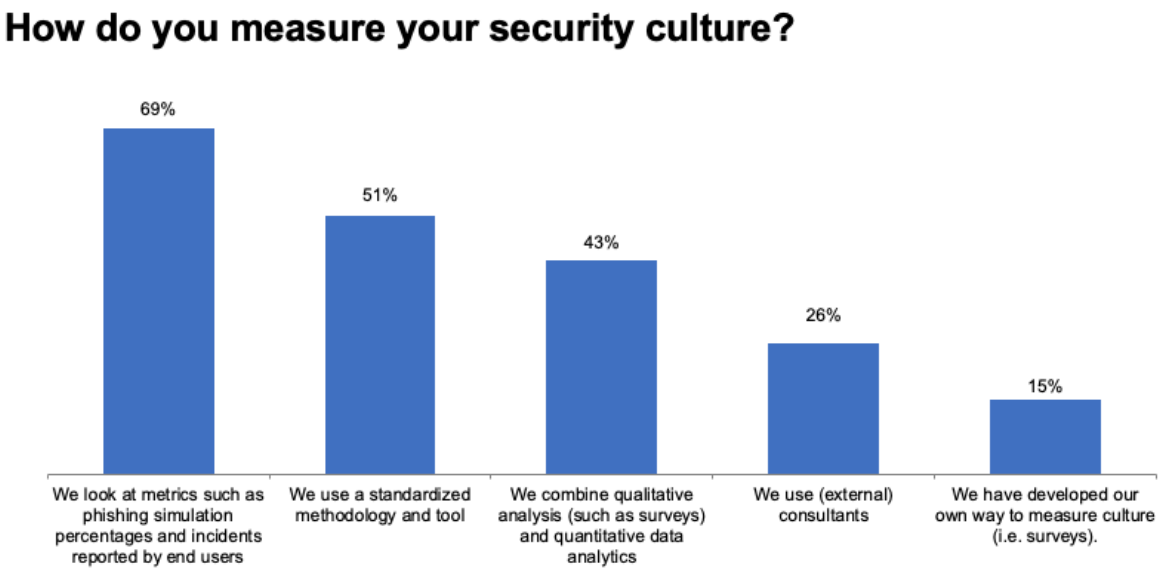
Almost all of the survey respondents (89%) agreed that security culture was important to their operations. The same percentage (89%) agreed that security culture was important to their customers and clients.



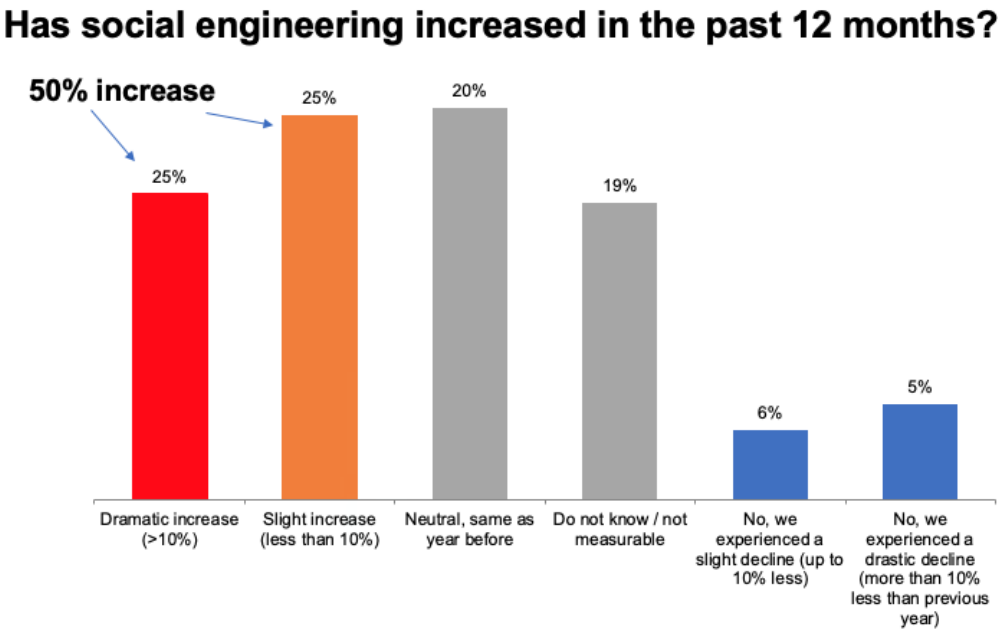
Most respondents (66%) currently assess or measure their cybersecurity culture.

The companies that measure their cybersecurity culture use various methods. Some 69% of respondents said they used metrics such as phishing simulation percentages and incidents reported by end users.

Half (51%) of responding businesses said they used a standardised methodology and tool, while 43% said they combined qualitative analysis (such as surveys) and quantitative data analytics. A quarter of the respondents (26%) used external consultants.



Social engineering is also on the rise. A quarter of the survey's respondents said they had experienced an increase in social engineering over the past 12 months, while another 25% replied that they had experienced the same amount of social engineering as the year before. Eleven percent said they had seen a decline in social engineering over the past year and 19% were unable to measure this. Almost half (40%) of respondents reported an increase in users reporting scams on chat applications such as WhatsApp, Signal, Telegram and others.



Just under half (41%) of respondents run a security awareness programme, but feel they should be doing more. 31% provide awareness and training targeted at different audiences and combine this with frequent phishing simulations and 28% are currently not running any security awareness and culture programmes.

When asked to list improvements that could be made to their security awareness and culture programme, respondents prioritised the following:

- Collect and analyse user behaviour data (56%)
- Measure and assess its effectiveness (52%)
- Add more simulation techniques (such as phishing simulations) (45%)
- Improve effectiveness of content & delivery (i.e. more gamification, better tailored to audience) (43%)
- Add in disciplinary actions (i.e., warnings for users not participating or failing phishing tests multiple times) (32%)
- Add in more rewards (25%)

PHISH-PRONE PERCENTAGE IN AFRICA

The KnowBe4 2022 Phishing By Industry Benchmarking Study analysed a data set of over 9.5 million users, across 30,173 organisations, with over 23.4 million simulated phishing security tests, across 19 different industries.

Each organisation's employee susceptibility to these phishing attacks is known as their Phish-prone™ Percentage (PPP) and it indicates how many of their employees are likely to fall for social engineering or phishing scams. These are the employees who might be tricked into clicking on a link, opening a file infected with malware or transferring company funds to a cybercriminal's bank account. A high PPP indicates greater risk, as it points to a higher number of employees who typically fall for these scams. A low PPP is optimal, as it indicates the staff is security-savvy and understands how to recognise and shut down such attempts.

The initial baseline phishing security test was administered within organisations that had not conducted any security awareness training from the KnowBe4 platform. Users received no warning, and the tests were administered on untrained people going about their regular job duties. The results continue to indicate high risk levels year-over-year.

In Africa, the Initial Baseline Phishing Security Test results are at an average of 31.4%. That means one out of three employees was likely to click on a suspicious link or email or comply with a fraudulent request.

Phish-prone %		
1-249 Users	**250-999 Users**	**1000+ Users**
30.20	27.43	32.38

Access the full report here

RECOMMENDATIONS

Despite fairly widespread awareness of the risks of fraud, scams and cybercrime, African businesses and users remain somewhat uninformed about how to mitigate them, and are thus vulnerable. This points to a need for intensified training and awareness programmes:

- Africa needs more public private collaboration to address people's "unconscious incompetence" with regards to cybersecurity, address the gaps in security skills and digital literacy and protect its citizens from cybercrime.
- More awareness is needed to showcase and warn people about the dangers and scams that can be found within the crypto ecosystem. The reliance on social media to make informed decisions about investments into crypto or NFT projects calls for tighter regulation of influencers. The case against Kim Kardashian and Floyd Mayweather shows that even well-known celebrities are being used to promote crypto scams and its wide adoption and interest in Africa makes people vulnerable targets.
- The cybersecurity industry and media need to make terms and their messages easier for people to understand and reduce the confusion around threats and technology.
- Criminals will use all communication channels. We need a simplified framework so people can identify red flags regardless of the technology or medium (i.e., identify red flags whether on email, voice, SMS, chat apps, social media or through emerging technologies like metaverse, Web3.0, etc.).
- Better awareness is not necessarily MORE training. It is targeted, timely and delivered in the right medium.
- Organisations need to improve corporate security awareness and culture programmes by measuring and assessing their effectiveness through simulations (such as phishing simulations) or survey techniques.
- The use of consumer apps like WhatsApp for corporate and personal lives increases risk and staff mental health problems. Combat this by defining policies and centralised platforms for corporate communications and start wellness and mindfulness programs.
- Combining corporate wellness and mindfulness programs with cybersecurity awareness can help teach users techniques such as slowing down and tapping into their senses, to help them calm down, improve concentration and overall performance. It will also make people less susceptible to social engineering attacks such as clicking on phishing emails or falling for other online scams.

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 Programme
Create a customised Security Awareness Programme for your organisation

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. Realising that the human element of security was being seriously neglected, KnowBe4 was created to help organisations 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 attacks and enterprise-strength reporting to build a more resilient organisation with security top of mind.

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

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4 Africa | The Planet Art, 32 Jamieson St, Cape Town, 8001, South Africa
Tel: +27.21.813.9264 | Email: Popcorn@KnowBe4.com

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

02D01K03