KnowBe4
Human error. Conquered.

WHITEPAPER

KnowBe4 African Cybersecurity & Awareness Report 2021

Table of Contents

KnowBe4 conducted an Africa-wide survey to explore whether or not people living on the continent were prepared for the current cyberthreats being seen. The survey 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 2022 to ensure robust and strategic cybersecurity.

The survey interviewed more than 763 people across Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria and South Africa, just as it did in the 2020 report, and the results showed that many of the challenges and considerations impacting users then were equally challenging in 2021. The significant shift in behaviours introduced by the pandemic continued to dominate, which meant that many of the security concerns and vulnerabilities present in 2020 remained a concern.

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 cyberthreat, but that still has a ways to go.

KEY FINDINGS

The KnowBe4 African Cybersecurity Awareness Report 2021 focused on several key questions around cybersecurity awareness and behaviours to gain a holistic view of the continent's security awareness stance, and the risks that cyberthreats posed to individuals. The survey spanned eight countries with 763 people and really highlighted some of the areas that require focused attention and forethought as organisations move into 2022.

The following are the key insights gleaned from Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria, and South Africa:

- The pandemic is still playing a major role in influencing working behaviours and patterns. Only 38% of respondents have returned to their offices or are accessing the internet from their office network, while 55% continue to work from home.
- 32% of respondents were affected by cybercrime while working from home, and one-third (33%) of the attacks were social engineering.

- 71% use their mobile data to access the internet, while 63% use their mobile phone for mobile banking and payments.
- WhatsApp remains the popular app of choice at 91%, with email at 75% and Telegram at 52%.
- The number of people concerned about cybercrime in 2021 is 72%.
- 30% tend not to share their personal information, an increase from 23% in 2020, and only 10% are very likely to do so, which is a slight improvement on the 13% of people who would have comfortably shared their data in 2020.
- Training and insights are needed to ensure that people can identify and mitigate the risks. This is supported by the fact that 54% of respondents did not know what a ransomware attack is, which is no improvement from 2020.
- 26% have experienced a social engineering attack over the phone (vishing).
- 34% have lost money because they fell victim to a scam.
- 21% have forwarded a spam or hoax email, 35% have clicked on a phishing email, and 55% have had a virus on their PC in the past.

These numbers remain in line with 2020's results, highlighting how complex this landscape has become and how many people have been caught by cybercrime, even though they believe they can identify the risks and the threats.

CYBERSECURITY AWARENESS: THE AFRICAN LANDSCAPE

One of the key elements of the survey was to find out exactly how vulnerable individuals and organisations are, and what challenges they face as they juggle remote and hybrid working frameworks. It is important to understand where the gaps in understanding are, especially as people access networks and corporate data from multiple locations and can potentially put the entire organisation at risk.

Some of the statistics should give the organisation pause.

Around 54% of Africans surveyed believe that trusting an email from people they know is secure enough—a worrying increase on 52% in 2020. Social engineering via email, such as Business Email Compromise (BEC scams) remains one of the most successful forms of cyber attacks today for this very reason. People are quick to click on links or open attachments sent to them from people who they know, not realising that cybercriminals have potentially hacked or spoofed (impersonated) their friend's, colleague's or supplier's accounts.

This risk is compounded by the fact that 54% do not know what ransomware is, and yet 44% believe that they can easily identify a security threat. Further, 48% do not know what multi-factor authentication is or how it can help them remain secure.

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

Answers	2019 Percent	2020 Percent	2021 Percent
Trojan Virus	33.86%	32.67%	32.63%
Botnet	9.14%	5.22%	6.55%
Ransomware	**36.71%**	**48.22%**	**45.7%**
Drive-by Download	20.29%	13.89%	15.07%

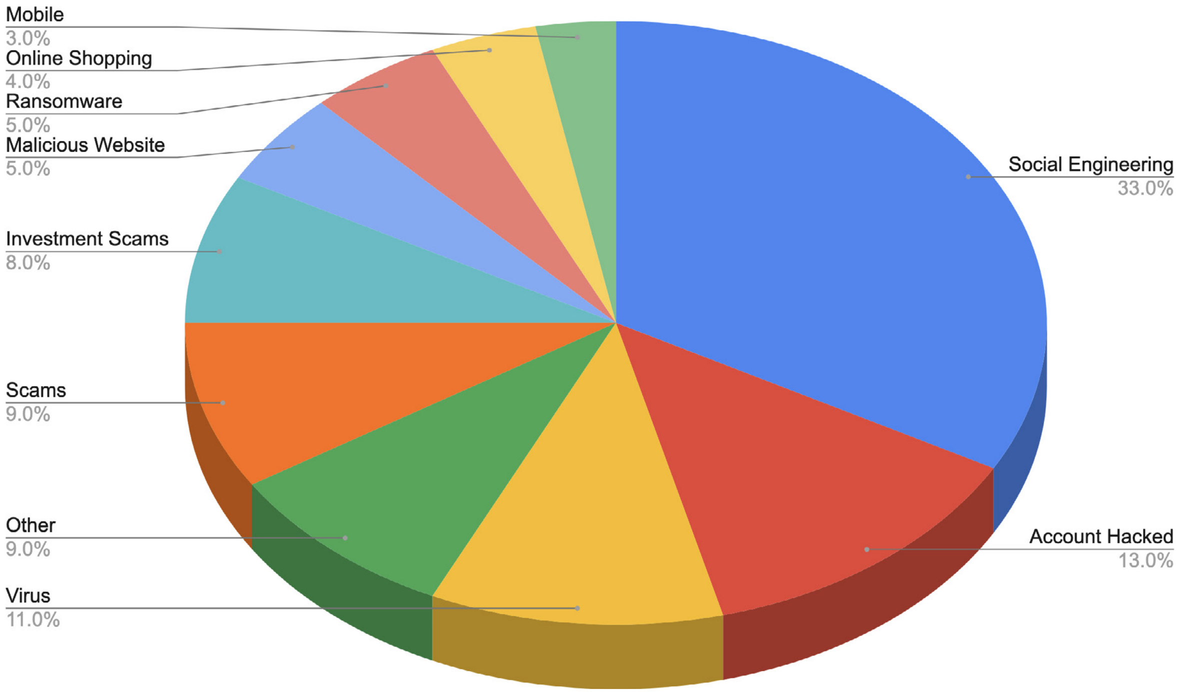
Finally, 36% have fallen for a phishing email and 55% have had a malware infection. Both numbers are up from 2020, which were 30% and 52% respectively. And, 32% of respondents were affected by cybercrime while working from home.

The challenge that lies ahead for business and employees is to address the gaps in knowledge and understanding to better protect both. People still need training and insight into the threats that could put them at risk, and the tools that can help them be more secure and aware. It is a complex landscape, one that is becoming increasingly challenging to navigate as cybercriminals evolve their own tools and approaches to catch the unwary or the unprepared.

TYPES OF CYBERCRIME EXPERIENCED

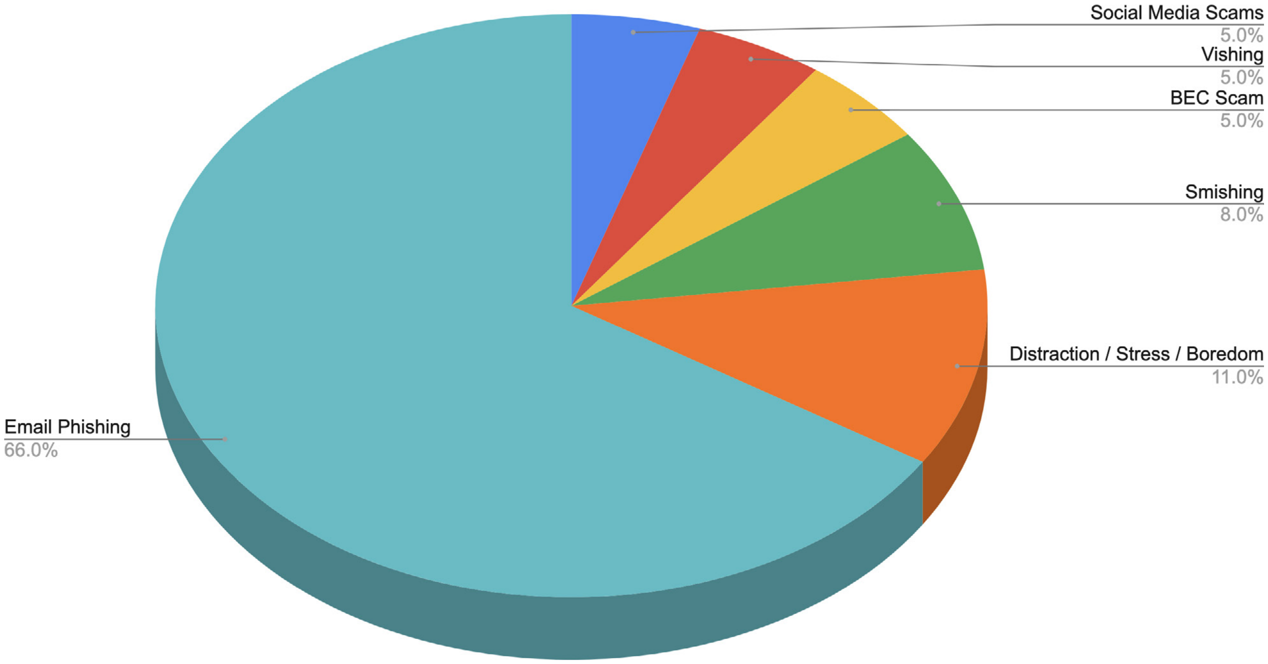
To establish a clear picture of the security mindset and landscape, the survey asked respondents whether they had been affected by cybercrime while working from home. 31.98% said yes, and this is a concern. It is a high number of people who have experienced an attack while working from home, putting both the business and those individuals at risk.

Of the 32% that had experienced an attack, the vast majority (33%) were tricked by social engineering. The second most common form of attack was a hacked account (13%), followed by a virus (11%), investment scams and general scams (9%) and ransomware (5%).



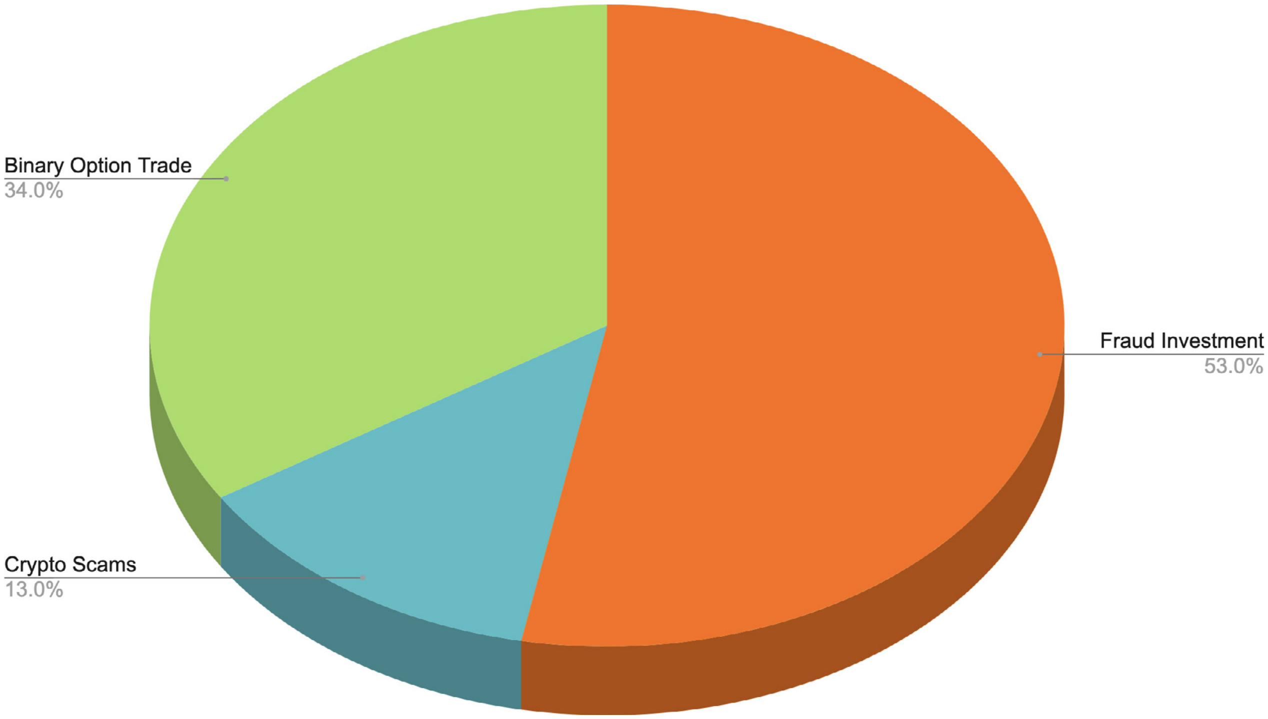
The social engineering attack that most successfully breached user defences was email phishing (66%), followed by smishing (8%), social media scams (5%) and vishing (5%). Interestingly, social engineering attacks were 11% successful because respondents were bored or clicked on something as a distraction.

Social Engineering



When investments scams were broken down, the most successful was the fraudulent investment scam at 53% followed by crypto scams at 34% and binary option trading at 13%.

Investment Scams



Cybercrime: Are People Concerned?

Over the past year, attitudes have changed. While there are still some people who struggle to understand how cybercrime works or its impact, most are starting to pay attention. In 2020, when asked if they were concerned about cybercrime, 26.30% of respondents said they were somewhat concerned but not really sure if they understood the threats or what to do against them. In 2021, this figure dropped to 13.89%, showing a marked shift in attitude and understanding. 71.43% said that they were concerned or very concerned in 2021.

However, the survey did test people's awareness of cyberthreats by asking what type of cyberthreat they believed would encrypt files and demand payments. This opened a digital can of worms—while nearly 46% accurately identified this as ransomware, 32% believed it was a Trojan and 15% a drive-by download. In Egypt, only 29% correctly identify ransomware, in South Africa 52% and in Kenya 63% of the respondents got it right, showing that there are differences in awareness levels by country. What this clearly shows is that despite location people still need more training around the definitions of specific attack vectors so they can avoid them more efficiently.

The survey also asked users if they could identify a strong password from a provided list, and 20% believed that P@$$word! was a good choice. This is a very easy password to guess for a professional cybercriminal. Fortunately, the majority of respondents could identify multi-factor authentication (61%) in 2021 compared with 48% in 2019.

However, the concern here, beyond business vulnerabilities, is that more than 30% of users do not know what two-factor authentication is and at least 40% are not using a secure password, yet 63% use their mobile phones to do payments or banking. This risk is further compounded by the fact that around 49% of users would give away personal information if there was a real need for it, which is down from the 63.98% in 2020, and a relatively measured response considering the need for personal identity verification when using specific government and financial services. However, the concern lies in the 10% who do it all the time.

Cybercrime: The Access Point

When it comes to security, one of the key areas of opportunity is how people access and use their devices and the internet. If companies recognise these behaviours, then they are far better placed to adapt strategies and training programmes to help modify and manage them. In 2021, the most common ways of accessing the internet were through a mobile network (71.43%) and a home Wi-Fi network (65.66%). Reflecting changing working conditions and the introduction of hybrid operating frameworks, there was an increase in the use of office networks (38.40%). The most common device used is the smartphone (95%), followed by laptops (75.49%) and tablets (33.42%).

Amongst the survey respondents, WhatsApp remains the single most popular application for work at 90.83%, with email following fairly close behind at 75.23% and Telegram at 51.77%. Facebook (65.79%), Zoom (45.09%), and Instagram (49.41%) come in to complete the top six. Interestingly, Microsoft Teams (15.86%) scored significantly lower than its competitor, Zoom (45%).

What is interesting about these figures is that email remains a very high communication contender, but it is equally one of the biggest security threats. This number dipped in 2021 compared with 2020, which saw 87% of users use email for work, while WhatsApp only had 85% of the market. However, even though people are more concerned about cybercrime and the impact it can have on their lives and business, they are still not fully aware of how to identify the threats.

The research found that, in 2021, 44.30% of users believed that they could confidently recognise a security incident if they saw one, while 36% were somewhat confident, and yet 35.52% have clicked on a phishing email, 54% have had a virus infection on their computer, and 34% have lost money to a scam or con artist. Nearly 22% of respondents have forwarded a spam or hoax email and 25% have been a victim of social engineering. The challenge is that email is still one of the most successful methods of cyber attacks as people are quick to click on links or attachments from people they know, as they do not realise that the account may have been spoofed or hacked.

Has any of the below ever happened to you?

#	Answers	Respondents (%)
A1	I have clicked on a phishing email	35.52%
A2	I have forwarded a spam or hoax email	21.36%
A3	**I've had a virus infection on my computer before**	**54.52%**
A4	I've been scammed over the phone before (social engineering)	25.69%
A5	I've lost money due to a scam / con artist	34.21%
A6	None of the above	11.14%

This is compounded by the fact that people are still placing too much trust into existing systems and people, in spite of the fact that many would have received a phishing email by someone they knew. In 2020, 52% of users trusted an email from someone they knew, and this number increased to 54% in 2021. However, users are paying attention to security information. More than 55% do not click on links or open attachments that they are not expecting. People are exhibiting some security smarts when it comes to email security, but there are holes that must be filled to fully mitigate the risks to people and businesses.

THE CYBERSECURITY CONCLUSION

The 2021 KnowBe4 Cyberthreat Report reveals a security threat landscape that has modified and adapted to changing working conditions and security concerns over the past year. While certain behaviours continue to have an impact on the security posture of the organisation and the individual, there is growing awareness around how the threats work and the best ways to minimise the risks. However, it remains critical that organisations train employees around security best practices and the ever-evolving methods employed by cybercriminals to catch their attention and trip them up. Only 40% of the respondents believe they fully understand their security roles and responsibilities and only 28% believed that their employers have adequately trained them in cybersecurity.

The survey has shined a spotlight on the gaps and cracks that still exist, which should help inform where organisations should focus their training and where people need the most help in learning about cyberthreats. This is particularly relevant as the world moves into hybrid working frameworks. More than 55% of respondents are hoping to continue working from home for the foreseeable future.

Employee training is one of the most powerful tools at the organisation's disposal, as it helps to minimise the vulnerabilities introduced by human errors—errors that can bypass even the most sophisticated security system and cause chaos. Employees need to learn how to recognise social engineering, vishing, smishing and phishing attacks, understand why weak passwords put them at risk, how two-factor authentication works, and why that well written post could actually be malicious. It is important that they know the most common security myths and how to defend themselves at work, at home and on the move.

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.

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 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