KnowBe4
Human error. Conquered.

WHITEPAPER

2020 African Cybersecurity Research Report

THE CHANGING SHAPE OF AFRICAN CYBERSECURITY

The 2020 KnowBe4 African Report interviewed 900 people in Botswana, Egypt, Ghana, Kenya, Morocco, Mauritius, Nigeria and South Africa. The report set out to further explore whether or not people living on the continent were prepared for cyberthreats, and what areas of weakness should be of concern to both the individual and the organisation. The results for 2020 were significantly shifted thanks to the changes in work and life behaviour introduced by the global pandemic, but areas of weakness remained that should be addressed in order to ensure that people remain secure and aware of the ongoing cybercrime threat.

Key Findings

- The COVID-19 pandemic has fundamentally changed how people live, work and approach security.
- 67% percent of those surveyed use their smartphones on a regular basis for both payments and mobile banking.
- The number of people concerned about cybercrime has risen to 48% (from 38% in 2019) and 24% of the respondents indicated that they were affected by cybercrime while working from home.

49%

of Africans surveyed think that **trusting emails from people they know** is good enough

(53% in 2019)

28%

have **fallen for a phishing email** and 52.7% have had a malware infection

(28% in 2019)

52%

don't know what ransomware is

(64% in 2019)

39%

don't know what **multi-factor authentication** is

(52% in 2019)

Compared with the 2019 KnowBe4 African Report, it's interesting to note that respondents were even more concerned about cybercrime. In 2019, 37.86% were worried. In 2020, the number has risen by 10% to 48.44%. Across all eight countries, there's a growing awareness of the risks that come with cybercrime. This concern is mirrored in the reasons why people were concerned about cybercrime. Half of the respondents (50%) were worried about falling victim to online fraud or losing money, while 26.78% were concerned about identity theft and 14% worried about their families.

I'm concerned about cybercrime

Answers	2019 Percent	2020 Percent
Not really, I don't see how it affects me	11.57%	7.11%
Somewhat, but I'm not sure I really understand the threats or what to do against it	27.43%	25.67%
My work takes care of all of this	13.57%	13.44%
Not at all, I feel very safe	9.57%	5.33%
I'm very concerned	**37.86%**	**48.44%**

People are still taking risks, as they don't fully understand what constitutes a threat and how their use of mobile devices to manage their banking and finances can impact their security posture. They are vulnerable, as they don't realise the problems posed by the security issues they don't know, or know to recognise. Around 64.22% would give away their personal information if they believed that there was a need for it, or if they understood what it was being used for. This is a measured response in light of government and organisation requests for data to verify identity. However, the concern lies in the 7% who would give away personal information if they got something back in return, like a discount, and the 6% who do it all the time.

The Risk of Limited Insight

People still need training and more insight into the threats that could put them at risk. This is supported by the fact that only 48% could define ransomware, nearly 20% have forwarded a spam or hoax email, 28% have clicked on a phishing email, 33.11% have fallen for a con artist or a scam, and 52.7% have had a virus on their PC before. It's a complex landscape that shows how many people have been caught by cybercrime even though they believe that they're capable of identifying one. The 2020 survey found that 40% think they would recognise a security incident if they saw one. However, this is down from the 55% in 2019 who believed they could identify a security threat, showing that people are becoming more aware of the gaps in their knowledge and the risks in the environment

The KnowBe4 2019 survey found that even though nearly half of respondents across all eight countries believed that their organisations had trained them adequately, a quarter of them didn't know what ransomware was. In 2020, this figure has grown to nearly 60%, with nearly 25% disagreeing with this sentiment. This percentage needs to change if the business is interested in minimising human error when it comes to a hack or attack.

For South Africans in 2019, a worrying 31.5% thought that a cyberthreat that encrypts files and demands payments was a Trojan virus. In 2020, nearly 50% correctly identified the threat as ransomware. Egypt and Morocco thought it was a drive-by download in 2019 and incorrectly identified it as a Trojan in 2020 (47.2%), with only 23% identifying it as ransomware.

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

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

In 2019, more than 50% of respondents were not aware of what multi-factor authentication was but in 2020, the number of people correctly identifying it rose to 61.11%, showing a shift towards more awareness around security hygiene and password management. More awareness needs to be done on identifying strong passwords, as 20% thought that P@$$word offers strong protection. It does not.

Two-factor authentication is?

Answers	2019 Percent	2020 Percent
Entering my password twice for extra security	23.57%	19.78%
Using my password plus something I own, such as a One Time Password generator	**47.71%**	**61.11%**
Captcha generators	12.00%	6.22%
Using two different passwords	11.71%	10.67%
Using a password manager	5.00%	2.22%

Email is Still the Number One Attack Vector, Closely Followed by WhatsApp

Email security is one of the biggest threats facing the average user, both at work and at home, and it is one of the most common communication methods—nearly 87% use email for work, closely followed by WhatsApp with 85%. In their private lives, WhatsApp is the most popular communication channel on the continent, with 96% of respondents chatting on it with their friends and families.

76.8% reported that the pandemic changed the way they work, with more than 50% changing this for the foreseeable future.

I use the following applications for work.

Answers	Percent
WhatsApp	**85.11%**
Instagram	46.67%
Facebook	66.89%
Snapchat	15.89%
WeChat	8.44%
Twitter	43.78%
LinkedIn	39.89%
Email	**86.67%**
None of the above	2.11%

I use the following applications for my private life (friends and family).

Answers	Percent
WhatsApp	**95.89%**
Instagram	61.44%
Facebook	81.00%
Snapchat	25.67%
WeChat	10.67%
Twitter	44.67%
LinkedIn	20.11%
Email	60.67%
None of the above	0.33%

Most people don't realise how to identify a risky email or WhatsApp message, or how their actions can result in their systems becoming infected. In 2019, while more than half of respondents in Botswana, Egypt, Kenya, Ghana, Morocco and Mauritius had enough security smarts to avoid clicking on links or opening attachments they didn't expect, a startling 46% still trusted emails from people they knew. In 2020, this number rose to 49.33%. In South Africa, those statistics were completely turned around in 2019—more than half of respondents (52%) trusted emails from people they knew, while only 49.5% didn't open attachments they did not expect. In 2020, these figures are now on a par with the rest of the continent with 52% trusting emails from people they know and 60% do not click on links or open attachments they did not expect.

Email remains one of the most successful forms of cyber attack 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 systems to spread malware or launch other forms of attacks. Cybercriminals can easily mimic contact lists or use email addresses that look as if they've come from trusted institutions, and a simple click can unleash a ransomware attack that can hold an entire company, government or home hostage.

The Impact of the Pandemic

Nearly 50% of the respondents will continue to work from home. Twenty-four percent of the respondents indicated that they were affected by cybercrime while working from home. Only 30% of respondents believe that their governments prioritised cybersecurity in their policies.

Has COVID-19 changed the way you work?

Answers	Percent
Yes, I had to work from home and will continue to work from home	**49.22%**
No	22.22%
Somewhat, I used to work remotely or from home before	18.22%
Somewhat, I hope to continue to work from home even after the pandemic	10.33%

Were you affected by cybercrime while working from home?

Answers	Percent
Yes	23.78%
No	**76.22%**

Survey Highlights Urgent Need for Security Awareness Training

For organisations, it has become critical that they train employees around security best practices and the various methodologies used by cybercriminals. This not only helps to minimise the growing risk of human error that's allowing threats to bypass their complex and powerful security systems, but also helps to protect their employees.

The survey has highlighted the areas that are most vulnerable and where people need more help in learning about cyber threats, especially since 50% will continue to work from home. Employee training is one of the most important defence mechanisms—employees need to learn how to spot social engineering attacks such as phishing, understand why weak passwords put them at risk, and how multi-factor authentication works, how to protect their home networks and what to do in the event of a security incident.

It's also important to bust some of the most common security myths. Not all malicious emails are badly written, ransomware is sophisticated and clever, and mobile devices can be infected. The most common platforms used by respondents to connect with friends and family were WhatsApp (more than 90%) and email (more than 86%) in their professional world. Both of these platforms are actively being used by cybercriminals for social engineering attacks.

Sixty-seven percent of Africans use their mobile devices for financial transactions and mobile banking—therefore, educating consumers on how to spot social engineering attacks (often conducted via the phone, WhatsApp and SMS) and how to defend against mobile malware should be a priority of industry and governments alike.

Education and awareness is key to ensuring people are aware of the risks, understand the threats and make more concerted efforts to protect themselves.

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.

COUNTRIES INCLUDED IN SURVEY

Botswana
69 | 7.67%

Egypt
92 | 10.22%

Ghana
49 | 5.44%

Kenya
163 | 18.11%

Morocco
33 | 3.67%

Mauritius
46 | 5.11%

Nigeria
91 | 10.11%

South Africa
357 | 39.67%

Additional Resources

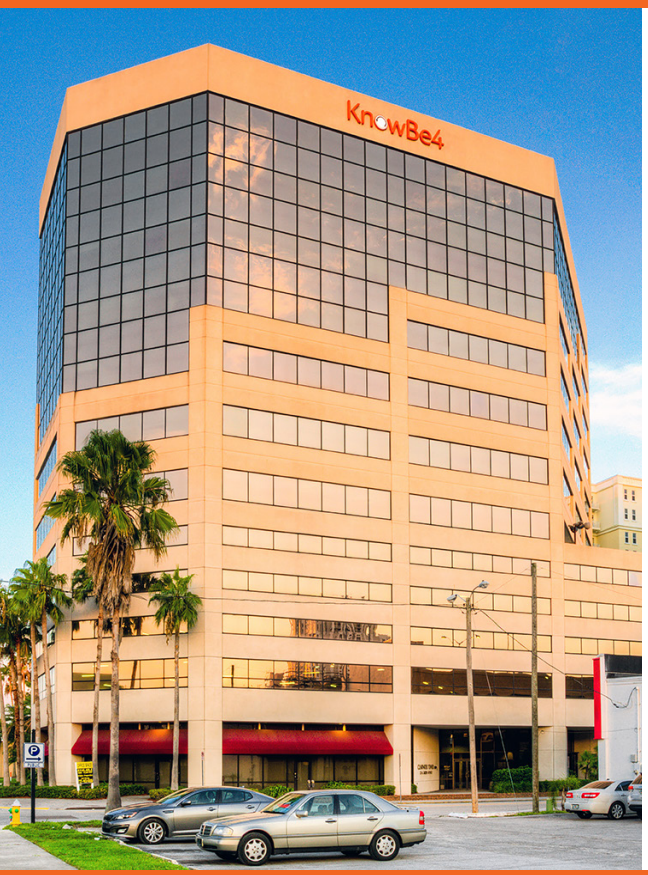
Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Automated Security Awareness Program
Create a customised Security Awareness Program 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 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 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 better 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

V112320