KnowBe4
Human error. Conquered.

WHITEPAPER

African Cybersecurity Research Report

HEAD'S UP AFRICA. YOU'VE BEEN PHISHED.

Key Findings

The 2019 KnowBe4 African Report with over 800 respondents across South Africa, Kenya, Nigeria, Ghana, Egypt, Morocco, Mauritius and Botswana has found that people living on the continent are not prepared for the cyber threat. 65% of respondents across all eight countries are concerned about cyber crime.

They are vulnerable, as they're not aware of what they don't know. From ransomware to phishing to malware and credential theft, users are not protecting themselves adequately because they mistakenly think they're informed, ready and prepared. Around 55% believe that they would recognise a security incident if they saw one.

Of all the countries surveyed, Kenyans (75%) and South Africans (74%) were the most concerned about the risk of cyber crime and yet respondents were comfortable giving away their personal information as long as they understood what it was being used for (Kenyans 26.59% and South Africans 57%). It's a worrying trend—many phishing scams will use any means necessary to tease out valuable nuggets of personal information and phone calls or emails from so-called 'trusted sources' are among the most common methods used.

53%

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

28%

have **fallen for a phishing email** and 50% have had a malware infection

64%

don't know what ransomware is and yet believe they can easily identify a security threat

52%

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

I’m concerned about cybercrime

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

The Risk of Not Knowing What I Don’t Know

The problem is that most users are not aware of how cyber criminals operate and the tools that they use. More than half of respondents across all eight countries felt very confident that they would recognise a security incident or issue if they saw one, but a significant percentage have had a PC infection, and more than a quarter had fallen for a scam. In South Africa, 50% of respondents had their PCs infected, while in Kenya, Ghana and Egypt, this number rose to 67%.

55%

confident in recognising a security incident

Have any of the below ever happened to you?

Answers	Percent
I have clicked on a phishing email	28.14%
I have forwarded a spam or hoax email	19.00%
I have fallen for a con artist/scam before	27.71%
I’ve had a virus infection on my computer before	50.43%
None of the above	16.71%

The KnowBe4 survey found that even though nearly half of respondents across all eight countries felt that their organisations had trained them adequately, a quarter of them didn’t know what a ransomware was. For South Africans, a worrying 31.5% thought that a cyberthreat that encrypts files and demands payments was a Trojan virus and 26.9% of Kenyans agreed. Egypt and Morocco thought it was a drive-by download, while Ghana thought it was a botnet.

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

Answers	Percent
Trojan Virus	33.86%
Botnet	9.14%
Ransomware	36.71%
Drive-by Download	20.29%

More than 50% of respondents are not aware of what multi-factor authentication is or the benefit thereof. Using stolen credentials was the third most common attack vector used in successful breaches and applying multi-factor authentication, which is combining your password with something that you own, such as a One-Time-Password app on your phone, which reduces this risk significantly.

Two-factor authentication is?

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

Phishing Still Number One Attack Vector of Successful Data Breaches

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—more than 70% of those surveyed use email to collaborate with friends and colleagues. Most people don't realise what a risky email looks like or how their actions can result in their systems becoming infected. While more than half of respondents in Botswana, Egypt, Kenya, Ghana, Morocco and Mauritius have enough security smarts to avoid clicking on links or opening attachments they don't expect, a startling 46% still trusted emails from people they knew. In South Africa, those statistics are completely turned around—more than half of respondents (52%) trust emails from people they know, while only 49.5% don't open attachments they have not expected.

Email remains one of the most successful forms of cyber attack today for this very reason. People are quick to click on links or attachments sent to them from people who they know, not realising that cyber criminals have potentially hacked or spoofed (impersonated) their friend's, colleague's or suppliers' systems to spread malware, or launch other forms of attacks. Cyber criminals 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. According to Verizon's 2019 Data Breach Report, email phishing is still the number one attack vector used in successful breaches. Closely followed by malware infections and the use of stolen credentials—both of which are attack vectors commonly accomplished via phishing. Phishing and social engineering attacks are not just limited to email—they have spread to other communication channels such as WhatsApp and the phone. With WhatsApp use at more than 90% in Africa, this is a serious concern.

I use the following applications to connect with friends or colleagues

Answers	Percent
Whatsapp	94.00%
Instagram	66.71%
Facebook	85.71%
Snapchat	24.43%
WeChat	8.00%
Twitter	54.14%
LinkedIn	38.00%
Email	69.71%
None of the above	0.43%

Phishing Myths

Another myth around phishing scams is that they are badly written with terrible language and rude offers. While these still exist, they are no longer the norm. Cyber criminals have become incredibly sophisticated and prey on this lack of understanding. Across all eight countries, more than a quarter of respondents checked for bad grammar and spelling to determine whether or not an email was legitimate. Interestingly, more than a quarter had also clicked on a phishing email. It turns out that yes, Africa has been phished and will continue to fall prey to this insidious attack unless they recognise the need for training and a deeper understanding of security threats.

When looked at against the backdrop of how often they've been caught by a phishing email, it's clear that users still don't realise how easily they can fall prey to a well-designed email.

The biggest concern is that this lack of awareness around cybersecurity impacts a person's life, identity and work. Humans are one of the most common causes of a business being held by ransomware or crippled by malware, data breaches or plain financial fraud. Their inadvertent clicking on an attachment, sharing personal information or carrying an infection into work on their mobile device can cause these types of issues.

People Have the Hots for Public Hotspots

The survey found that more than 90% of respondents used a smartphone and more than 70% used a laptop computer to connect to the internet, using either data from their mobile network (more than 80%) or through their home network. However, more than a quarter of respondents connected their devices to the internet using a free Wi-Fi connection in a public space. This is risky, as cyber criminals make use of public places to trick people into connecting to their malicious hotspot in order to connect to the person's machine or to steal their information.

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 the cyber criminal. People need to stop thinking that phishing and ransomware only happen to other people or big businesses—everyone is vulnerable. One of the reasons why spam continues to rise in quantity is because it works often enough to be of value. According to the September 2019 Cisco Talos Email and Web Reputation Centre report, the average spam volume for the year was 409.51 billion. That's compared with the paltry 68.90 billion emails that are legitimate. Spam works because somebody always clicks on the link.

Training in cybersecurity threats, methodologies, entry points and vulnerabilities has become critical for the organisation. 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 helps to protect their employees.

The survey has highlighted the areas that are most vulnerable and where people need the most help in learning about cyber threats. Employee training is definitely one of the most important points—employees are not aware of how their use of free Wi-Fi networks can potentially infect the organisation, nor are they as aware of email and phishing threats as they believe. It's also important to bust some of the most common security myths. Not all malicious emails are badly written, phishing is sophisticated and clever, and mobile devices can be infected. The most common platforms used by respondents to connect with friends and colleagues were WhatsApp (more than 90%) and email (more than 70%), and both of these platforms have been compromised. Educating users on how to strengthen their password practices by applying multi-factor authentication is another easy step to significantly reduce risks.

Education is key to ensuring that employees are aware of the risks, understand the threats and make more concerted efforts to protect themselves from infection.

Contact us at KnowBe4 Africa for locally relevant training content and our award-winning integrated simulated phishing platform to help you make your users more aware.

COUNTRIES INCLUDED IN SURVEY

Botswana

Egypt

Ghana

Kenya

Morocco

Mauritius

Nigeria

South Africa

Additional Resources

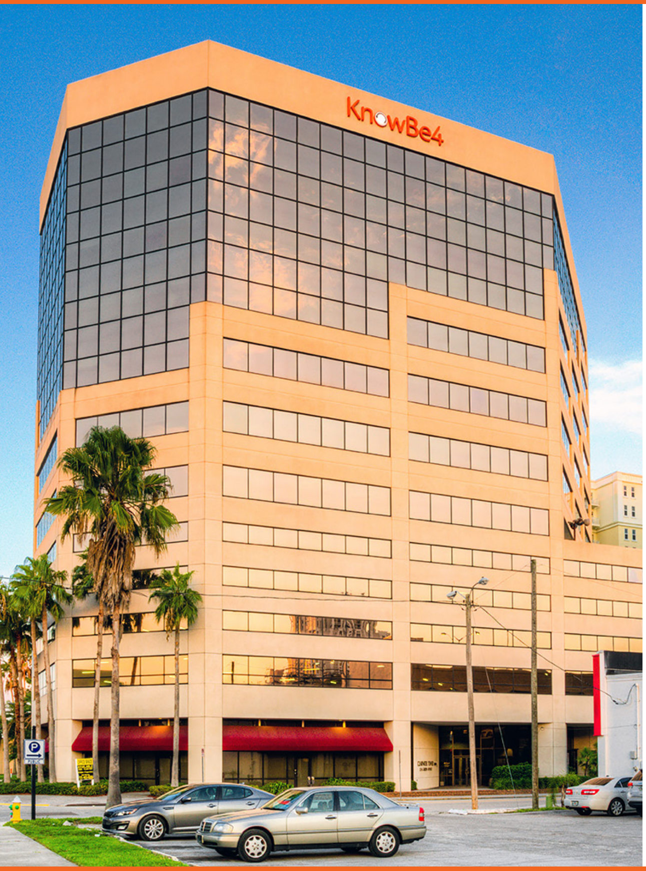
Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Automated Security Awareness Program
Create a 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 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 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 | www.PopcornTraining.com | 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