BIZCOMMUNITY

Report reveals Africa is not fully prepared for cyber attacks

The 2019 KnowBe4 African Report collated insights from more than 800 respondents across South Africa, Kenya, Nigeria, Ghana, Egypt, Morocco, Mauritius and Botswana to determine their understanding of the growing, global cyber threats.

Across all eight countries, the majority of respondents (65%) expressed concern about cybercrime, but most (53%) still trusted emails from people they knew and didn't know how to identify ransomware (64%). The statistics in the report show that the biggest vulnerability facing people on the continent is a lack of knowledge.

"People cannot protect themselves because they don't realise the extent of the cyber threat or how it presents itself," explains Anna Collard, CEO, Popcorn Training. "Most users are not aware of how cybercriminals operate and the tools they use. A significant number of respondents claimed that they were confident that they could recognise a security threat (55%) and yet they gave away personal information, trusted emails and attachments, or fell prey to PC infections or scams."

People can't protect themselves against threats that they do not recognise, or understand. Forty-six percent of the respondents in Botswana, Egypt Ghana, Morocco and Mauritius trusted emails from people they knew. This is a concern because fraudulent use of personal data and risky attachments from hacked email accounts are responsible for a significant percentage of cybercriminal attacks.

Beware of gender-based cybercrimes

19 Feb 2020

Email security remains one of the biggest threats, at home and at work, because it is one of the most common communication methods and cyber attack vectors. More than 80% of those surveyed use email to collaborate with friends and colleagues but are unsure as to exactly what a risky e-mail looks like or how their opening it can compromise their security and systems. People click on links and attachments from people they know without realising that cybercriminals have potentially hacked these accounts.

“Cybercriminals can easily mimic contact lists or use email addresses that look like they come from trusted sources such as your bank, insurance company or from your friends and family,” says Collard.

“A single click then unleashes malware, such as ransomware, that can cause immense personal and professional harm. More than a quarter of respondents clicked on a phishing email or fell victim to a cleverly designed cyber scam – it is essential to educate people so they can recognise online risks and protect against them.”

Email scams are no longer badly written with terrible language and rude offers. Those still exist, but there are plenty of clever and personalised emails that are catching people unawares, getting them to click on links and divulge personal information that’s used to access their bank accounts and systems.

The survey underscored how often people are caught out by phishing and scam emails because they don’t recognise them – 28% clicked on a phishing email, 19% have forwarded one, and 50% had a virus infection on their computer.

I've been hacked! What do I do?

John Mc Loughlin 21 Feb 2020

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 a more than 90% use of WhatsApp in Africa, this is a serious concern.

The survey also found that more than 90% of respondents used a smartphone and more than a quarter connected their devices to the internet using a free Wi-Fi connection in a public space.

This is risky as cybercriminals 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.

“Organisations have to train employees around security best practice,” concludes Collard. “Ransomware and phishing doesn’t just happen to other companies – everyone is vulnerable. The survey found that even though nearly half of respondents felt their companies had trained them adequately, a quarter didn’t know what ransomware was. If people don’t understand the threat, they can bring it into the business and cause untold damage.”

Wait...is that the real Facebook?

19 Feb 2020

The survey has highlighted the areas that are most vulnerable and where people need the most help. Training in cybersecurity threats and best practices such as using multi-factor authentication is critical.

It’s also important to bust some of the most common security myths. Not all malicious emails are badly written, phishing can be sophisticated and clever and delivered to users mobile devices. Education is key to ensuring that employees are aware of the risks, understand the threats and make more concerted efforts to protect themselves and their workplaces.

Download the KnowBe4's African Cybersecurity Research Report.