Vodacom Business shares an important cybersecurity message

Issued by We-Worldwide

13 Nov 2023

The growth of digitalisation and rapid development of advanced technologies has brought about a whole new age of convenience and ease both in business and at home. But, as with most things, the good is not without the bad. As the world has become progressively more connected, cybercrime, once a minor concern, has grown so significantly since the onset of the pandemic that experts now consider it among the top threats to businesses across the globe.

Cybercrime began gaining momentum in 2019 when criminals realised they could take advantage of misaligned networks as businesses were forced into new work-from-home models. By 2020, the number of cybersecurity victims per hour had increased from 40 in 2018 to 90. In the same period, hourly losses increased by nearly 56% from $308,219 to $479,452. Despite businesses becoming more settled in the new normal, with more established networks, these numbers have continued to rise. In 2022, hourly financial losses sat at $1,175m, nearly triple that of 2019. And yet, even with the growing cyber threat landscape, only 33% of companies believe they may fall victim to a cyberattack.

As numbers continue to rise and businesses struggle to keep up with the changing threat landscape, it has become clear that swift and effective intervention is needed at all business levels. This is the aim of the latest Vodacom Business cybersecurity campaign.

“As businesses have adopted more digital technologies, the attack landscape has grown significantly, introducing several new vulnerabilities that organisations were unprepared for. In addition to the growing attack landscape, AI and machine learning technologies have improved malicious programs' efficacy and development speed,” said Kabelo Makwane, managing executive for the Cloud, Hosting, and Security at Vodacom Business. “This campaign aims to tackle the problem head-on, from the basement to the boardroom, by giving people a first-hand experience of what is possible.”

The campaign has been launched in collaboration with several local radio stations to show one of the newest trends in cybercrime – voice cloning. Using the very same technology adopted by criminal syndicates, Vodacom has used AI to mimic lead radio presenters' voices and used these to create a simulated hacking experience. During the short stunt, Vodacom has managed to include three key points: firstly, the premise of the stunt involves the presenter receiving an email from their station manager requesting they download an attachment, a request which is not often made. This is a prime example of the kind of attack which, in 2021, caught out 1 in 5 internet users and was responsible for over half the total data

breaches that year.

The second important message to be found in this stint is just how convincing scams can be, thanks to the latest in AI and machine learning technologies.

“In the same way that AI and machine learning have led to advancements in cybersecurity, so too have they helped advance cybercrime,” said Makwane. “Beyond the processing power which is now available to these criminals, it has given them the ability to tailor their attacks right down to using your manager's voice, or even their face.”

This new wave of innovation is currently on the rise. Targeting both individuals and businesses, criminals need only around a 30-second recording to accurately mimic a person’s voice. This technique is so effective that, according to recent reports, around 83% of Indian citizens have lost money due to AI voice scams. There are also several businesses included in the list of victims, with one CEO wiring €220 thousand to a scammer, believing them to be the head of their German parent company.

This leads us to the final important message of this stunt. That is the role which humans play in cybersecurity.

“Many still consider the onus of cybersecurity to land on the lap of the CTO or head of security. While it is the responsibility of this individual and their team to oversee the organisation's safety, the landscape is such that it is the responsibility of every single employee to keep the organisation safe,” said Makwane. “Investing in cybersecurity means more than investing in the latest technology. Without buy-in from your entire staff, your organisation will never be truly secure. That was the goal of this campaign, to demonstrate not just the cunning of cybercriminals, but also to stress the importance of company-wide cyber awareness, from basement to boardroom.”

According to a recent report, 82% of data breaches were the direct result of human error born out of ignorance rather than malicious intent. Despite this disproportionately large number, only 3% of IT spending was assigned to addressing this problem. According to Vodacom Business, the intent behind this campaign was to try and address this problem on a country-wide scale by giving people a real-life example of just how real cybercrime is.

“Our ultimate goal is to create a safer online space for everyone in South Africa,” concluded Makwane. “Cybersecurity is not being taken seriously enough. We encourage businesses of all sizes to turn to Vodacom Business to ensure your business is fit for a secure future. Beyond our cutting-edge technology, we understand the human side of securing your business. Through education and simulated experiences, we want to help organisations achieve digital security to accelerate their growth without fear of interruption.”

As we approach the festive season, a time for promotions, specials, and random acts of voucher-baring kindness, it is crucial that everyone remain alert to the ever-present threat which cybercrime poses. Because while you sip mimosas on the beach or take a nap in the December sun, #ThreatsNeverSleep