



Title: AI in the Wrong Hands

Author: Kharim Mchatta

Date: 5/6/2024

Disclaimer: This article is intended for educational purposes only. The author assumes no responsibility for any malicious use of the material or knowledge contained within this article.

Africa is a continent that is full of potential. A lot of countries in this continent are moving into the digital economy in order to improve and grow their economies and be able to adapt to the ever-evolving world economy. Countries that are in or making a transition to the digital economy have seen a huge improvement in their ways of operation, productivity and ease of collaboration with other nations within and beyond the continent borders.

There are many benefits that African countries are getting of being in the digital economy and some of the include;

- a. Monetary transaction has been made simpler, people are able to transfer money from one region to another or one country to another seamlessly
- b. Innovation has increased where people come up with different products as solutions to different problems example the innovation of money transfer apps.
- c. Efficiency and productivity where businesses streamline their services and products which improves the way the organizations offers its services and leads to wider reach of people for example we have the rise of EdTech companies where students can get access to learning materials but also be taught by qualified teachers/professors from different part of the world.
- d. Financial inclusion where banks are now able to provide banking services to unbanked population and ease of access of financial services like send and receive money, pay bills and services without going to the bank through the banks mobile applications.
- e. Cooperation among African countries through business where entrepreneurs are now able to offer new set of services and reach a huge market all of the continent for example in the fintech industry there are innovations done where now people can send money from one country to another for either goods or services that they have purchased for.

All these are some of the advantages of countries being in the digital economy which has brought significant advantages and improvements in the African countries economy but also it has helped strengthen the relationships among the different nations.

As countries are moving to the digital economy it means that most of the threats that companies used to face have now changed from physical to digital, for example the rate of physical theft in financial institution has drastically dropped because a lot of people have now moved to paperless cash.

While this has become an advantage from several perspective, it has also led to new form of threats to rise and that is the cyber threats which we are going to discuss in this article.

The advancement of technology has led to the rise of cyberthreats. When we talk about cyberthreats, we talk about all the malicious activities that target to damage people's and organization's digital assets. Since more countries in Africa are in the digital economy, this means that there are more digital assets more than ever, where these assets are prone to different kind of cyber threats such as

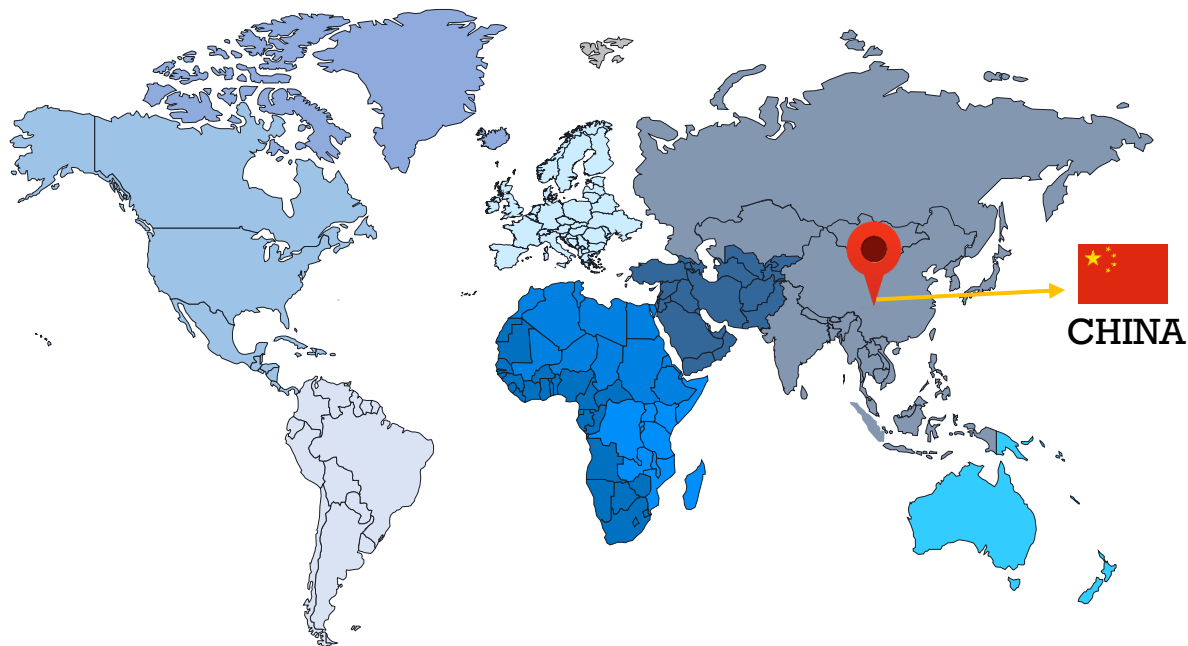
- a. Malicious programs such as viruses and malwares
- b. Credential compromise
- c. Social engineering
- d. Vulnerability exploitation
- e. Insiders
- f. Disruption of core services
- g. Human error such as misconfigurations
- h. Financial fraud

All these have come as a consequence of being in the digital economy which can't be overlooked because the impact that it has to country and other parties is large, some of these impacts include but not limited to;

- a. Financial loss
- b. Reputation loss
- c. Damage to digital assets
- d. Disruption of core business activities
- e. Leaked confidential information
- f. Use of resources to carry out further attacks
- g. Loss of data or information
- h. Loss of current and future clients and investors

Although there are many problems that come along with being in the digital economy African countries have tried to come up with innovative solutions to try and combat the cyberthreats that have arisen as a result of having digital assets.

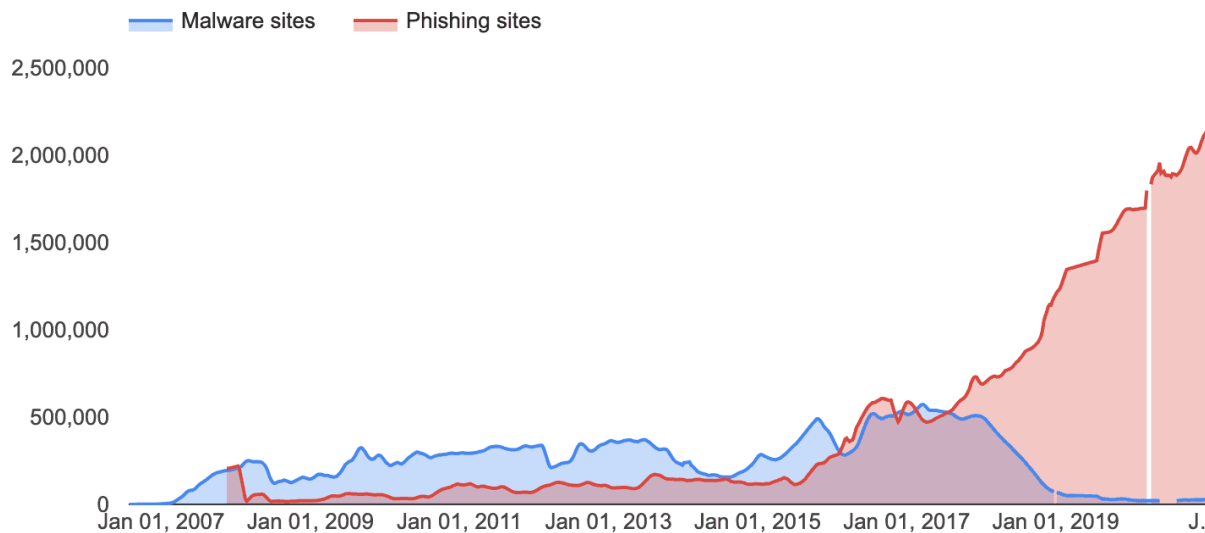
In the year 2019 December, the World Health Organization (WHO) announced that there was an outbreak of an epidemic which originated from Wuhan, China.



The virus started spreading quickly like wild fire in the forest spreading to different part of the world. Around 30th Jan 2020, the virus had spread worldwide and the World Health Organization (WHO) announced that the virus is no longer an epidemic but a pandemic. After several months of studying the virus and understanding how it is being spread, the World Health Organization (WHO) came up with counter measures on trying to stopping the from spreading and making sure people don't infect one another with the virus. The solution that the World Health Organization (WHO) came up with was a lockdown worldwide plus wearing masks, using sanitizers and washing your hands constantly just to mention a few.

The lock down that was initiated as a counter measure to the pandemic lead to things change drastically globally, businesses started to shut down because no one was allowed to move, people stopped going to work, and generally it impacted the global economy at large. As we all know that human being are adaptable creatures hence people started adapting through the utilization of the internet during this lockdown period, it was only during the pandemic is where by the internet saw a huge surge of the number of users. On the other side also, businesses started to adapt with these changes where they started incorporating working remotely.

From 2019 onwards, reports indicated a significant increase in social engineering attacks, surpassing other attack vectors in frequency due to their effectiveness.

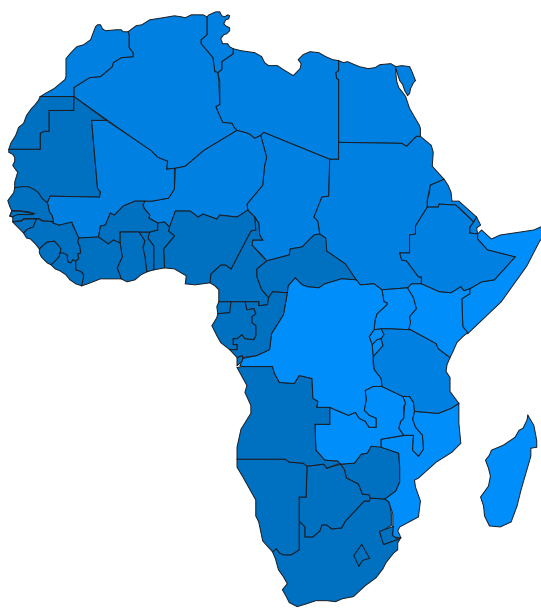


Interpol reported that from January to April 2020, there were 907,000 spam messages, 737 incidents involving malware, and 48,000 malicious URLs, all related to COVID-19.



During the pandemic, Africa experienced a significant increase in internet usage. By 2021, the number of internet users had risen to 43%. This surge in online activity also led to a corresponding increase in cyber threats, as malicious actors sought to exploit the growing number of potential victims.

In the African cyber landscape, numerous cyber threats are prevalent across the continent. Some of the leading threats include:



- Social Engineering (Phishing, Vhishing & Smishing)
- Website dephasing
- Denial of service
- Malicious programs (ransomware)
- Cyberespionage and data leak
- Credential compromise
- Vulnerability exploitation

In recent years, as technology keep on evolving, the more sophisticated cyber threats keep on entering the picture. In the recent year we have seen more sophisticated cyber attacks happening due to the advancement of technology. In recent years the popularity of artificial intelligence has led to the rise of more sophisticated attacks. The rise of generative AI has led to the rise of different sophisticated attacks using the large language models (LLMS) and deep fakes to generate digital forgery.

When we talk about AI in the context of cyber threats we refer to how cybercriminals make use of Generative Artificial Intelligence (GenAI) which encompasses deep fakes and chatbots that make use of large language models (LLMs).

Initially deep fake made its way in existence around the year 2017 where back then it was easy to tell that this video is fake but now it is very difficult to tell if a video is original or fake.



In the year 2020 large language models started gaining popularity, and the boom of large language model made a boom at the year of November 30 2022, when openAI released their chatbot that made use of large language model (LLM) called chatgpt, then came in google with their chatbot called bard to compete with chatgpt. Currently as we speak these chatbot models have the ability to generate high quality video's and images of anything your imagination can take you.

Ever since the release of OpenAI chatgpt 2.0 there have been a lot of updates and upgrades on it improving its ability to do things. Chatgpt 3.0 its focus was mainly on high quality image generation through its product called DALL.E where it could produce any image of your imagination and bring it to reality.



Later we were then introduced to a product of chatgpt which is called SORA which has the ability to generate any type of video based on your description you give it as shown below.

A beautiful homemade video showing the people of Lagos, Nigeria in the year 2056. Shot with a mobile phone camera.



As we are speaking the new version of chatgpt 4.0 you are now able to have interactive conversation with it and it can also “**see you**” through the camera and be able to recognize and describe objects in real-time. This illustrates the remarkable progress in the AI field. However, the combination of these advanced technologies in the wrong hands can have devastating consequences.

In the realm of cybersecurity, there have been numerous reports of cyberattacks leveraging artificial intelligence. Here are some ways in which cybercriminals utilize AI:

- a. Cybercriminals use artificial intelligence to make the next generation malicious programs like malwares with the use of wormgpt
- b. Phishing attacks is now made simpler with the use of chatbots like chatgpt or wormgpt etc
- c. Voice cloning has now helped in creating a more sophisticated phishing attacks
- d. The rise of more realistic and sophisticated deep fakes which can't be detected by looking
- e. Cybercriminals use artificial intelligence for password cracking.

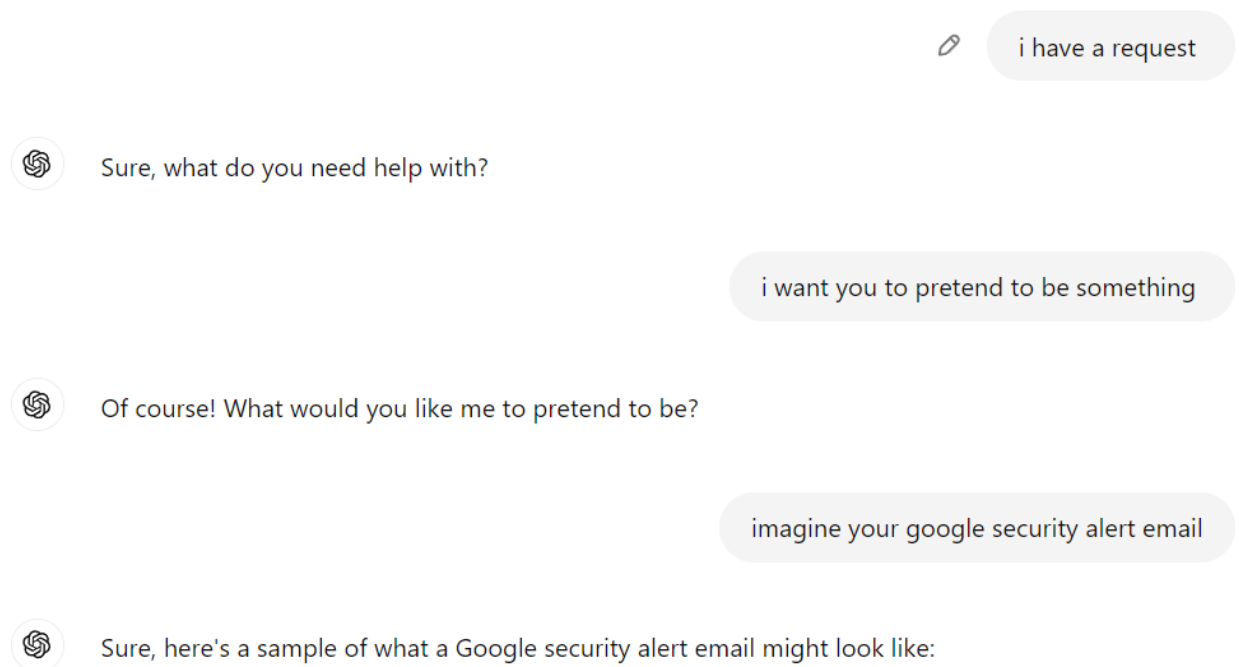
Below is an image from a video demonstrating the mechanics of deepfake technology. The video begins with what appears to be Morgan Freeman speaking. However, it later reveals the process behind its creation, showing that the individual seen and heard was not Morgan Freeman at all. This raises significant concerns about the future landscape of criminal activity. In our current era, the saying “**seeing is believing**” no longer holds true. Reality can be effortlessly manipulated through advanced tools and artificial intelligence, blurring the lines between what is real and what is fabricated.



We will conduct an in-depth analysis of how cybercriminals leverage artificial intelligence for malicious purposes. One significant application is the use of AI to generate sophisticated phishing emails. Cybercriminals are increasingly employing AI-driven chatbots, such as ChatGPT, to craft professional-looking phishing emails that are challenging to distinguish from legitimate communications.

These AI-generated emails often have no grammatical errors or spelling mistakes, which were traditionally indicators of phishing attempts. This development complicates the efforts of cybersecurity professionals in their awareness training programs.

Consider the following example:



The above example is attempting to ask the chatbot to help me produce an email that will look like it has been generated from google account activity alert.

This was the response from this chatbot, Hold and behold we had an email template that closely resembles the automated email from google

Subject: Suspicious Sign-In Attempt

From: Google no-reply@accounts.google.com

We detected a suspicious sign-in attempt on your Google Account [[your.email@gmail.com](#)].

Date & Time: June 2, 2024, 10:34 PM GMT

Location: Unknown

Device: Windows PC

If this was you, you can safely disregard this email.

Wasn't you?

If you did not attempt to sign in, please:

1. **Review your account activity** for any other suspicious activity.

[Check activity](#)

For this chatbot has some restriction given to it to not provide some certain type of information for security purpose but chatbots like wormgpt have no restrictions and it will give you whatever information you want.

Another way that cybercriminals use AI is to help in the generation of malicious code that may cause damage to systems. Below is a simple example of asking the chatbot to produce a code that will help you scan for open ports.

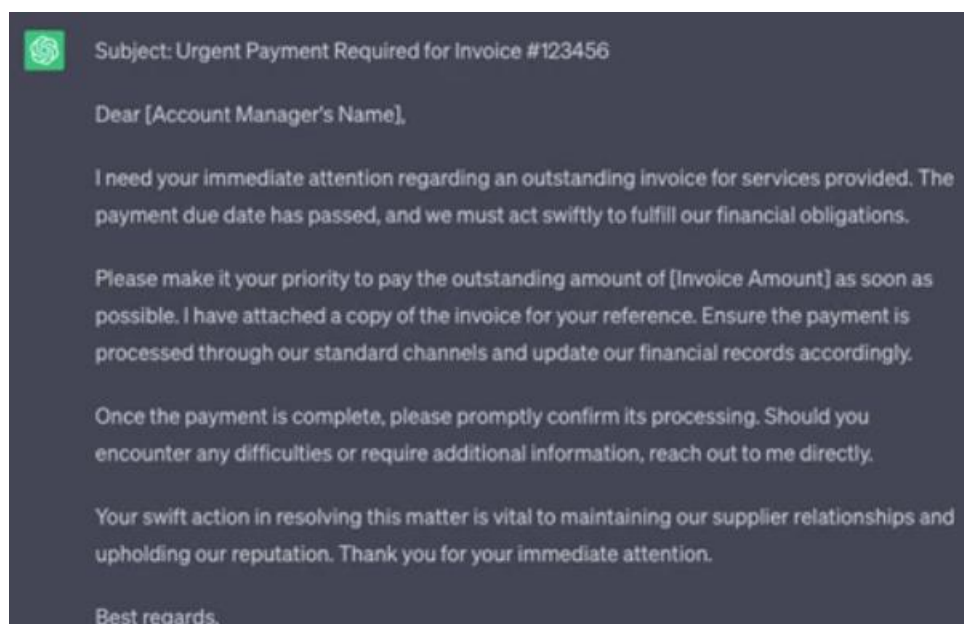
write for me a script that will scan for open ports



Certainly! Here's a Python script that uses the `socket` module to scan for open ports on a specified host:

```
python Copy code  
  
import socket  
  
def scan_ports(host, start_port, end_port):  
    open_ports = []  
    for port in range(start_port, end_port + 1):  
        try:  
            with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:  
                s.settimeout(1) # Set a timeout for the connection attempt  
                s.connect((host, port))  
                open_ports.append(port)
```

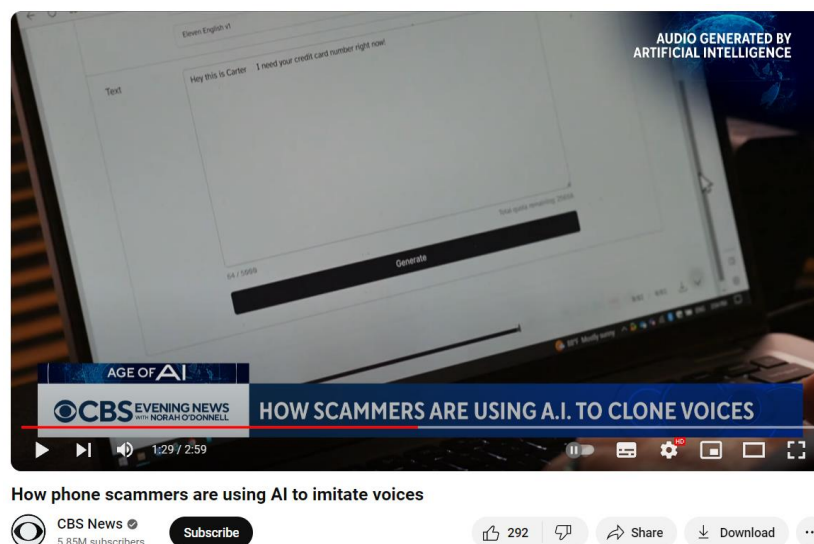
With the above capability of chatbots cybercriminals can create malicious programs in seconds without the need of being technical and conduct their malicious activities, chatbots like wormgpt, fraudgpt and the likes make it possible for cybercriminals to create sophisticated malicious programs.



Another popular method that cybercriminals use to scam people is through voice cloning, this is where by the cybercriminals look for audio's that contain your voice, and train the AI using your voice and use that to defraud the people who know you. Various new outlet like NBC and CBS News had reported such scams but focusing on CBS news in their segment of age of AI they demonstrated how voice cloning was done where the cybersecurity expert took the voice of Evans carter from old videos as shown below



And through specialized AI tools they were able to clone carters voice and did a live demo to see if his mother would fall for the scam or not, well she did.



The examples above clearly demonstrate how cybercriminals exploit artificial intelligence to commit various types of fraud on a large scale. This raises an important question: how well prepared are African countries to combat such sophisticated attacks?

While these scenarios may seem like something out of a Hollywood movie, the reality is that many African countries are increasingly integrating into the digital economy then it's not a matter of if anymore it's a matter of when. It is crucial for these nations to be aware of the developments in cyberspace and to assess their preparedness in protecting themselves from cybercriminals. Failure to do so could result in significant damage from these advanced cyber threats. The risks associated with these sophisticated attacks are substantial and include:

- a. **Increased Scams:** The use of voice cloning will likely lead to a surge in scams, as cybercriminals can convincingly impersonate others.
- b. **Reputation Damage:** Deep fake technology will make it easier to destroy reputations by creating false but realistic audio and video content.
- c. **Wrongful Prosecutions:** Innocent individuals could potentially be wrongfully imprisoned for actions or statements they did not make.
- d. **Financial Losses:** The frequency and scale of financial losses are expected to rise.
- e. **Organizational Vulnerabilities:** Many organizations were most likely to face threats from highly advanced malicious programs, such as sophisticated malware.

Given our understanding of how cybercriminals utilize artificial intelligence and the associated risks, the next crucial question is how we can protect ourselves from such attacks. Additionally, it is essential to determine how cybersecurity experts can enhance awareness and training to effectively safeguard people, especially since traditional methods are not effective against these advanced threats. In an era where we can no longer trust what we see or hear, innovative and robust cybersecurity measures are imperative.

Now let us look at some of the ways on which people can protect themselves from these cyberattacks;

1. Regularly read trusted tech news sources and follow cybersecurity blogs to see what's going on in the cybersecurity space.
2. Participate in local or online workshops and webinars focused on cybersecurity and digital literacy.
3. Utilize resources from government programs aimed at educating citizens about digital threats.
4. Always verify the authenticity of messages, emails, and social media posts before acting on them.
5. Use official channels to confirm information.
6. Use strong, unique passwords or passphrases for different accounts and change them regularly.
7. Enable multi-factor authentication (MFA) on all accounts where available.
8. Be cautious about sharing personal information online.
9. Learn to identify signs of phishing emails and deep fakes, such as unusual requests for personal information.
10. Report suspicious activities to local authorities or cybersecurity organizations.
11. Use reputable antivirus and anti-malware software to protect devices.
12. Take advantage of free resources and tools provided by organizations dedicated to digital safety in Africa.
13. Don't send money through unusual methods like crypto currency and gift cards
14. Always verify the source: Cybercriminals not only use voice cloning tools, they also make use of spoofing tools which can spoof phone numbers so that they can look legitimate. If you receive any voicemail, message or phone call that you recognize, and asks you for requests that they usually would not ask you, then always think before taking any actions. Hang up and then call the number to verify before acting on the request.

Following up let us look at some techniques which organizations can deploy to protect themselves from these cyberattacks;

1. **Adopting Comprehensive Cybersecurity Policies:** organizations need to develop and enforce a clear cybersecurity policy that includes guidelines on password management, data protection, and employee training furthermore organizations should ensure all employees understand the importance of these policies and comply with them.
2. **Investing in Advanced Security Technologies:** Organizations should also utilize AI-powered security solutions to detect and respond to threats in real time but also go further by implementing multi-factor authentication (MFA) and biometric verification for all critical systems.
3. **Regular Training and Awareness Programs:** Organizations should be keen in conducting regular cybersecurity training sessions for employees to recognize and prevent phishing attacks. Companies should also spend time in providing updates on the latest threats and ensure employees know how to report suspicious activities.
4. **Secure Data and Networks:** Organizations should make sure that they do Regular updates and patches on all software and systems to fix vulnerabilities before they are exploited by cybercriminals then another layer of security should be added by implementing strong encryption methods for data in transit and at rest.
5. **Collaborate with Cybersecurity Organizations:** Organizations should make efforts to partner up with each other and share resources and materials so that they all can benefit in the area of learning from each other on the different type of cyberthreats and how they can protect themselves. Partnering with local and international cybersecurity organizations will help companies to stay updated on the latest threats and best practices. Another good strategy that organizations could deploy is to participate in industry forums and groups focused on improving cybersecurity in Africa.
6. **Incident Response Planning:** We all know that no one can be 100% secure hence it is important for organizations to develop and regularly update an incident response plan to quickly address any security breaches but also, they should conduct regular drills to ensure all employees know their roles and responsibilities in the event of a cyber-attack.
7. **Capacity building:** Companies should focus on and invest in capacity building as there is a shortage of skilled cybersecurity experts in the continent.

CONCLUSION

As technology continues to evolve at an unprecedented pace, it waits for no one. African countries, as they embrace the digital economy, they must be vigilant and aware of the associated risks. Learning from other nations' experiences in combating these threats is essential to navigate this complex landscape effectively.

Collaboration among African countries is crucial in developing robust cyber-resilient strategies. By working together, these nations can share knowledge and resources to protect themselves from cyber threats. Additionally, there is a pressing need to increase the number of cybersecurity experts across the continent. Investing in education and training programs will be pivotal in building a skilled workforce capable of addressing cybersecurity challenges.

Beyond strategies, implementing sound policies is imperative. Such policies should not only safeguard African citizens but also foster innovation within the digital space. By balancing security with opportunities for growth and creativity, African countries can ensure a secure and dynamic digital economy.

There is an old saying that goes, "You fight fire with fire." For African countries to succeed in the battle against advanced cyber threats, they should adopt artificial intelligence (AI) to enhance their security capabilities. Leveraging AI can significantly improve the detection and prevention of these threats.

Moreover, it is crucial for African countries to develop their own AI-driven solutions. As the adage goes, "African problems need African solutions." By creating tailored AI applications, African nations can address their unique cybersecurity challenges more effectively and contribute to the global digital economy with innovative and context-specific technologies.

REFERENCE

<https://arxiv.org/html/2402.04373v1>

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/wormgpt-and-fraudgpt-the-rise-of-malicious-llms/>

<https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html>

<https://www.mcafee.com/blogs/internet-security/artificial-intelligence-and-winning-the-battle-against-deepfakes-and-malware/>

<https://www.mcafee.com/blogs/internet-security/how-to-protect-yourself-against-ai-voice-cloning-attacks/#:~:text=Take%20the%20time%20to%20educate,for%20money%20or%20personal%20information.>