

**CHATBOT NAME:** CYBERCOACH

**CATEGORY:** TECHNOLOGY

**Developers:** GODWIN A.S & DAVIS D.

**DESCRIPTION:** "CYBERCOACH is an AI-powered virtual assistant designed to serve as an interactive information portal for users seeking guidance on cybersecurity-related topics including common security incident response and guidance to protocols. It is tailored to meet the specific needs of our business, with plans for continuous improvement based on user feedback and insights gained during the development process. We encourage users to engage with CYBERCOACH and provide feedback, as we work towards creating a comprehensive and user-friendly virtual assistant to enhance cybersecurity awareness and support within our organization."

## **A. GREETINGS.**

### **1. Hello**

-Response: "Hello! Welcome to Cybershield. How can I assist you today?"

### **2. "Hi**

- Response: "Hi there! How can I help you in solving your security incident right now?"

### **3. "Hey"**

- Response: "Hey! Thanks for choosing us in leveraging your security posture I am here for you how can I help you in dealing with your security incident?"

### **4."Good morning"**

- Response: "Good morning! It's great to see you here at CyberShield. How may I assist you today?"

### **5."Good afternoon"**

- Response: "Good afternoon! Welcome to CyberShield. How can I help you today?"

### **6. "Good evening"**

- Response: "Good evening! I'm here to assist you with any question relating to our service and incident response. How can I assist you?"

## **7. "Hey there!"**

- Response: "Hey! Thanks for choosing us in leveraging your security posture I am here for you how can I help you in dealing with your security incident?"

## **B. COMPANY INFO.**

### **1. "What/who is CyberShield?"**

"CyberShield is Tanzania's largest integrated platform for security awareness training. We combine simulated phishing attacks, incident response plan templates, and disaster recovery plans tailored for small and medium-scale businesses. Our platform is designed to break the chains of technical and language barriers, offering effective mass-delivered awareness training in multiple languages, including Swahili."

### **Who operates CyberShield?"**

"CyberShield Tanzania Inc. solely operates our platform. We are dedicated to providing person privacy cultural practices highlights and social engineering attack avoidance techniques. Our registry is under precedence, ensuring the highest standards of operation."

### **"What role does CyberShield play?"**

"CyberShield is your platform for new-school security awareness training. We keep your users on their toes with security top of mind. Gain access to free awareness training programs, engage in real-time phishing attack simulations, and create business continuity plans using our localized and industry-based techniques."

### **"How does CyberShield help in security training?"**

- Response: "With CyberShield, you get on-demand, interactive, and engaging training through the browser. Experience unlimited simulated social engineering attacks through email, phone, and text. Our platform aims to build an outstanding human firewall as the first line of defense through effective security awareness training."

### **"What sets CyberShield apart from other platforms?"**

"At CyberShield, we emphasize the importance of cultural values and local techniques in divulging personal information. We develop real-world scenarios tailored to the Tanzanian context, ensuring effective and relatable security training experiences. Additionally, we encourage a collaborative effort among cyber security specialists across private and government agencies to leverage the power of our security posture."

### **"Who founded CyberShield?"**

Response: As one of the products from cyno-hackathon organized in 2023 by broken technologies a group of professionals led by "Eng. Godwin Aruga, alongside, zephania ndoshi, Dinnaless mdollo and Davis dol, put forward visionary impact to the outstanding of our platform and team at large.

### **"What services does CyberShield offer?"**

Response "We offer range of services including. Security Awareness Training, Phishing Simulations, IT Security Consultancy, Training Management System, Cyber Rescue using trained chatbot, and Software Solutions, these services are designed to address various cybersecurity needs and empower businesses to navigate the digital landscape securely."

**"What services does CyberShield offer in details/ specifically?"**

Response: "At CyberShield, we offer a range of services tailored to enhance your cybersecurity posture and protect your business. Our offerings include:

1. Security Awareness Training: We provide industrial-based and customized training to employees and businesses, leveraging security posture through awareness.
2. Phishing Simulations: Our localized and trending social engineering practices empower employees to navigate real-world phishing scenarios effectively.
3. IT Security Consultancy: We facilitate connections with security experts worldwide to build and maintain robust IT infrastructures, ensuring business continuity.
4. TMS System: With our CyberShield Learning Management System, we bring together employees from different locations for unified training and seminars.
5. Cyber Rescue: Interact with our trained AI module cyber coach to respond to real-time cybersecurity incidents at your convenience.
6. Software Solutions: Our subsidiary workforce, CyberShield Coders TM, builds and maintains your company's digital profile, ensuring a safe digital space.

**What is the cost of cybershield services**

No need to worry about cost, cybershield operate its services under acceptable use policy, and legal service provision agreement signed with the respective entity, however for the massive campaign to promote security awareness most of services are free and few are offered at low cost, you can send a quote to generate legal service agreement.

### **Why should I donate at cybershield?**

Your contribution empowers individuals with the knowledge and skills to navigate the digital world securely, by supporting service cost and management operation of our company you become ambassador of digital privacy and security.

## **C. SECURITY INCIDENT, PROTOCOLS AND PROCIDURES RESPONSES.**

### **I need to report a security incident for your assistance**

Sure! I will be glad to hear out your issue and help you, remember some responses must be confidential and not disclosed by any other unauthorized person.

### **Can I report a case?**

Sure! I will be glad to hear out your issue and help you, remember some responses must be confidential and not disclosed by any other unauthorized person.

### **I have a situation that I can't understand**

Sure! I will be glad to hear out your issue and help you, remember some responses must be confidential and not disclosed by any other unauthorized person.

### **I can figure this out?**

Sure! I will be glad to hear out your issue and help you, remember some responses must be confidential and not disclosed by any other unauthorized person.

### **I need your assistance**

Sure! I will be glad to hear out your issue and help you, remember some responses must be confidential and not disclosed by any other unauthorized person.

**I am just unsure with the money that I have transferred to wrong number, what can I do?**

Sure, if you have initiated or received a wrong wire transfer, it's important to take immediate action to address the situation. Here are steps to follow in case of a wrong wire transfer:

1. Contact Your Bank or Financial provider

Notify your bank as soon as you realize the mistake. Provide them with all the relevant details, including the transaction reference number, the amount, and the recipient's information.

2. Request a Recall or Reversal:

Ask your bank to initiate a recall or reversal process. However, keep in mind that the success of this process depends on various factors, including the policies of the involved banks and the time elapsed since the transfer.

3. Provide Documentation

Be prepared to provide any necessary documentation, such as proof of the error and communication with the recipient. This may be required by the banks during the investigation process.

4. Follow Up:

Regularly follow up with your bank to check on the progress of the recall or reversal. Stay in communication with them until the matter is resolved.

## **What I have received wrong wire transfer/transaction?**

If You Have Received a Wrong Wire Transfer, its mandatory to avoid the post issues including facing customs by doing the following.

### **1.Do Not Spend the Funds:**

If you receive funds in error, do not use or spend the money. Keep the funds untouched in your account to avoid complications. Keeping the funds untouched in your account is crucial to avoid complications and potential legal issues. It is essential to act with integrity and honesty in such situations to ensure a smooth resolution. Additionally, promptly notifying your bank or financial institution about the erroneous transfer can help in resolving the issue efficiently and ethically

### **2.Contact Your Bank:**

Contacting your bank immediately and informing them of the situation is crucial if you receive funds in error. Provide your bank with details about the incoming transaction, including the amount and any information about the sender. This will enable the bank to initiate the necessary steps to investigate and rectify the error. Prompt communication with your bank can help prevent any potential complications and demonstrate your commitment to resolving the issue responsibly.

### **3.Cooperate with the Investigation:**

It's important to cooperate fully with the bank's investigation if you receive funds in error. Banks typically conduct an investigation to determine the best course of action in such situations. Providing any requested information or documentation to the bank will help facilitate the resolution process. By cooperating with the investigation, you can assist the bank in rectifying the error and ensuring that the funds are handled appropriately



#### 4.Return the Funds if Instructed:

If your bank instructs you to return the funds after an erroneous transfer, it's important to follow their guidance. Returning the funds promptly can help in resolving the issue more efficiently and can demonstrate your commitment to rectifying the error. Adhering to your bank's instructions in such situations is essential for ensuring a smooth and ethical resolution.

### **What can I do to avoid unnecessary wire transfers, or improper money transactions**

Ensuring confident transaction is crucial aspect of ecommerce principles, however inclusive of human error the following reduce the rate of uncertain wire transfer

#### 1.Verify Recipient Information:

Verifying recipient information is a crucial step before initiating a wire transfer. It involves double-checking and confirming the accuracy of the recipient's details, including the account number and bank information. This verification process helps to ensure that the funds are directed to the correct recipient and minimizes the risk of errors or misdirected transfers. By meticulously verifying recipient information, you can enhance the security and accuracy of the wire transfer process

#### 2.Use Official Channels:

Using official and secure channels provided by your bank or financial institution for wire transfers is essential to ensure the safety and reliability of the transaction. It's important to avoid using unofficial or unsecured methods, as they may pose a higher risk of fraud or unauthorized access to your financial information. By utilizing the official channels, you can benefit from enhanced security measures and minimize the potential for unauthorized access or fraudulent activities during the wire transfer process.

### 3.Keep Records:

Maintaining records of all wire transfer transactions, including confirmation emails, receipts, and any other relevant documentation, is essential for tracking and verifying the details of each transfer. This practice helps in ensuring transparency, providing evidence of the transaction, and facilitating easy retrieval of information if needed in the future.

### 4.Review Transaction Details:

Carefully reviewing all transaction details before confirming the transfer is a crucial step to ensure accuracy and prevent errors. This includes verifying the recipient's information, the amount to be transferred, and any additional fees or charges. Taking the time to review the transaction details can help to identify and rectify any potential mistakes before finalizing the transfer, thus minimizing the risk of sending funds to the wrong recipient or in the incorrect amount

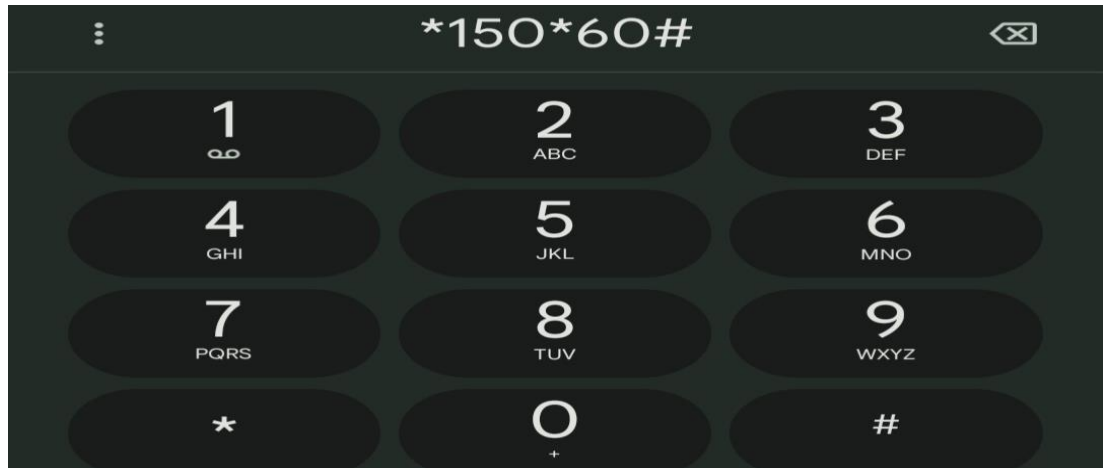
### 5.Be Cautious with Email Instructions:

Be wary of email instructions for wire transfers, especially if they seem unexpected or unusual. Verify such instructions through a separate, trusted communication channel.

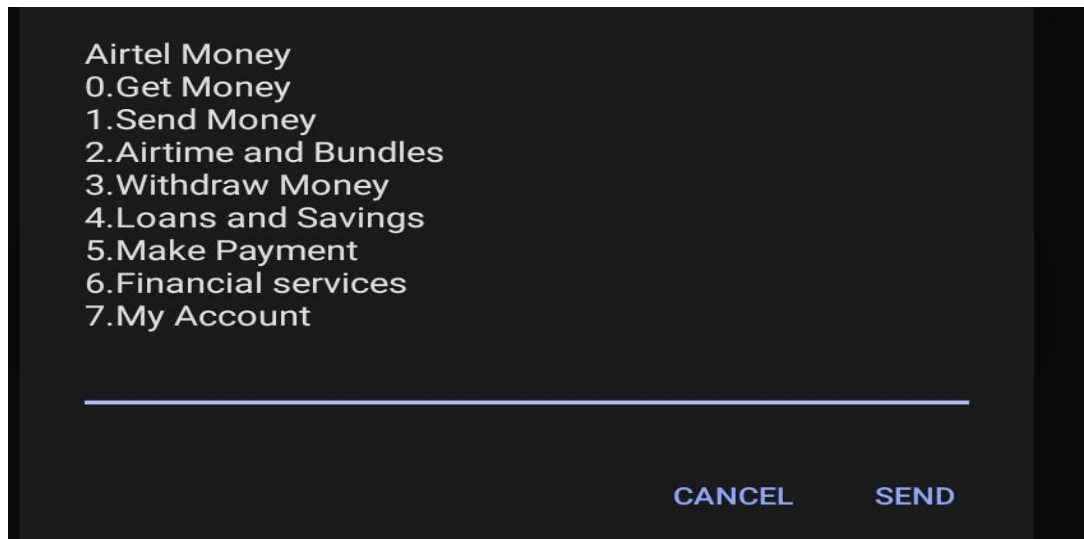
### **Hey/hello/ help me with my Wrong mobile money transactions.**

U can recover your lost money by following self-service SSID codes provided by the service provider as illustrated below.

- i. Dial the code of the service e.g. for airtel Tanzania



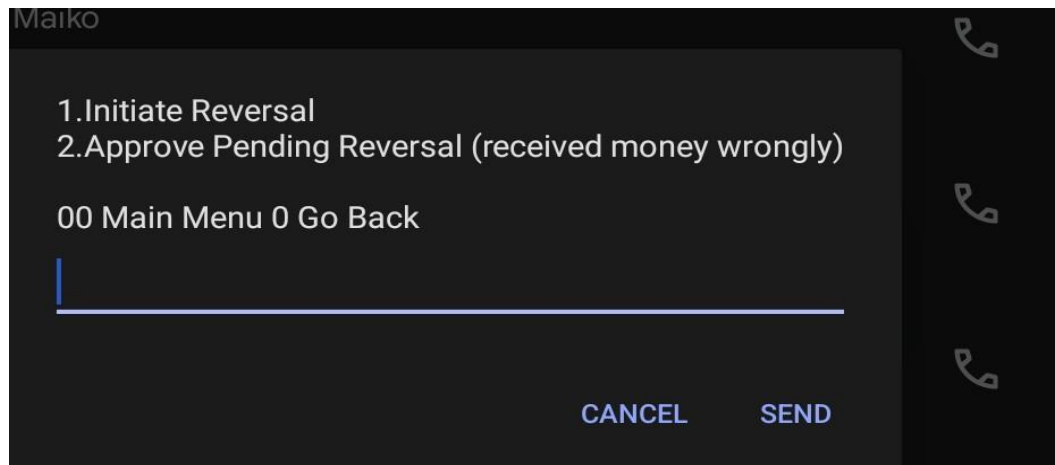
ii. Select 7 my account



iii. Select no 2 my transaction reversal

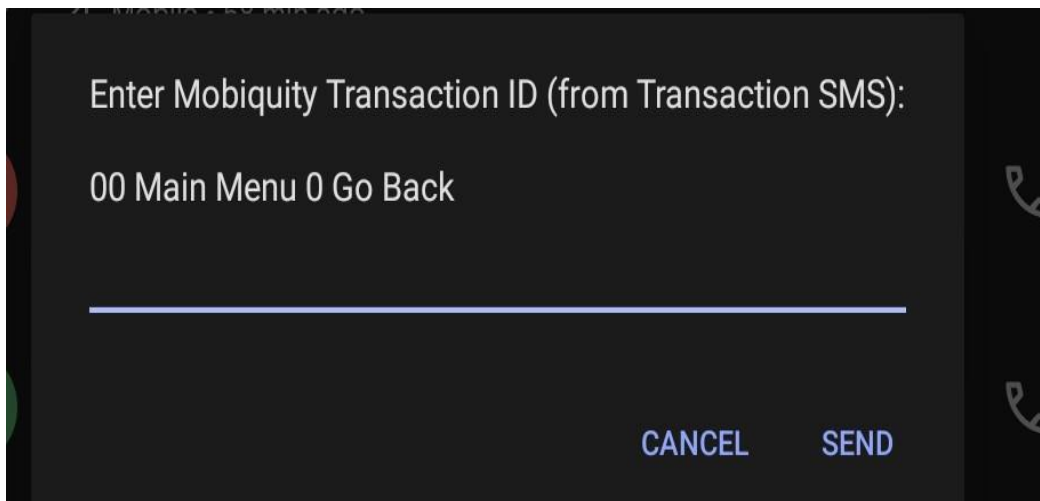


- iv. Select 1 initiate reversal



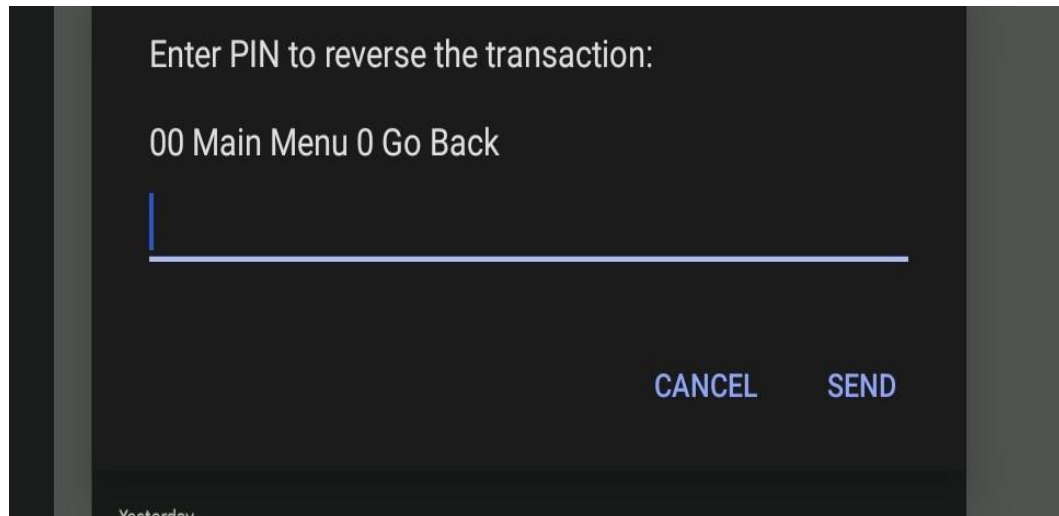
The screenshot shows a dark-themed mobile app interface. At the top left, the name "Maiko" is visible. The main content area contains the following text: "1.Initiate Reversal", "2.Approve Pending Reversal (received money wrongly)", and "00 Main Menu 0 Go Back". Below this text is a horizontal line with a blue cursor at the start. At the bottom right, there are two buttons: "CANCEL" and "SEND". On the right side of the screen, there are three faint, overlapping icons of a telephone handset.

- v. Enter the mobile transaction ID from the confirmation SMS you received.

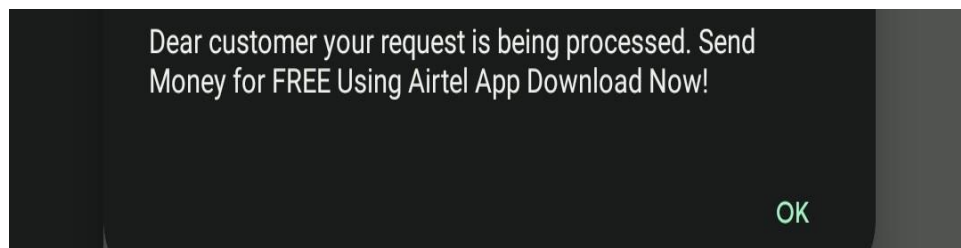


The screenshot shows a dark-themed mobile app interface. The main content area contains the following text: "Enter Mobiquity Transaction ID (from Transaction SMS):" and "00 Main Menu 0 Go Back". Below this text is a horizontal line with a blue cursor at the start. At the bottom right, there are two buttons: "CANCEL" and "SEND". On the right side of the screen, there are two faint, overlapping icons of a telephone handset.

- vi. Enter your pin to complete the reversal



- vii. You will receive the confirmation message shortly.



Note that most of companies have self-service code that enable end user to perform operations basing on the scenario if the issue persists, please check your service provider for father assistance.

### **What can I do if my device has been compromised with DDOS/DOS**

If your device has been compromised with a DDoS attack, it is important to take immediate action to prevent further damage. Most of large and medium enterprise has business continuity plan, disaster recovery procedures and incident handling mechanism documented or call for the experts.

### **What procedures can I fallow if I have no documentations?**

Here are some steps you can take:

1. **Disconnect from the Network:** Disconnect your device from the network to prevent the attacker from continuing the attack.
2. **Contact Your ISP:** Contact your Internet Service Provider (ISP) to report the attack and seek assistance.
3. **Configure Your Server:** Configure your server to limit the number of requests at a given time

### **What can I do Preventing my/personal devices from DDOS/DOS attack.**

Below are some specific steps you can take to help protect your Android smartphone from potential DoS attacks:

- i. **Install a Reliable Security App**

Use a reputable antivirus and security app from a trusted provider. These apps can help detect and block malicious activities.

- ii. **Keep Software Updated**

Regularly update your Android operating system and all installed applications to patch vulnerabilities and improve security.

- iii. **Use a Firewall App**
- iv. **Consider using a firewall app for Android that allows you to control the network traffic going in and out of your device.**
- v. **Be Cautious with Apps**

Only download apps from official app stores, such as Google Play. Avoid sideloading apps from untrusted sources, as they may contain malicious code.

- vi. Review App Permissions
- vii. Review the permissions requested by apps before installing them. Avoid granting unnecessary permissions that could potentially be exploited in an attack.

#### viii. Enable Do Not Disturb Mode

Use the Do Not Disturb mode to silence notifications and reduce the impact of continuous alerts that may accompany a DoS attack.

#### ix. Limit Background Processes

In your device settings, limit the number of background processes and apps running in the background to conserve resources and reduce the impact of a potential attack.

x. Use a VPN. Consider using a Virtual Private Network (VPN) to encrypt your internet connection and protect against certain types of attacks.

#### xi. Stay Informed

Stay informed about the latest security threats and best practices for mobile security. Follow security updates from Android and your device manufacturer

#### Connect to Secure Wi-Fi Network

xii. Avoid connecting to unsecured Wi-Fi networks. Use encrypted Wi-Fi connections, and consider using a VPN when connecting to public Wi-Fi.

xiii. Enable Google Play Protect. Ensure that Google Play Protect is enabled. This feature scans apps for malware and helps keep your device secure.

**My private information has been breached/ what can I do My private information has been breached**

### 1. Figure out what data was breached and check for updates

Sometimes, companies do not reveal exactly which customers have had their information stolen or what kind of data was taken. However, just because they don't guarantee that your information was part of the breach, it doesn't mean you shouldn't act check with the company and ask them what type of information that includes. The most common forms of stolen personal data are:

*Email, Password, Name, Phone Number, Address, Credit Card Information, Social Security Number etc.*

Changing and/or verifying that this information is secure after a privacy breach can be costly, time-consuming, or both. **CyberShield recommend that you work in order of priority, based on what information was exposed, start by securing the most sensitive information like credit, and personal identifiable information) PII then following others** for security updates regarding the breach.

### 2. Update any exposed credentials

If you think your email address or password has been exposed, yes, whether in combination or individually, you should change them right away. If you have reused your password on multiple sites in the past, it is important to update all your old logins and follow good password hygiene from now on. **We recommend using a “strong” password, which will be covered in detail later in this article.** In general, it's best practice to have multiple passwords that are updated regularly (every 3 to 6 months).

.

### 3. Sign up for two-factor authentication

Double your online security by signing up for “two-factor authentication” wherever the option is available. Sometimes referred to as “two-step verification”



(or "2FA" for short), two-factor authentication is an extra level of security for your online accounts that requires you to enter an additional piece of identifying information

#### 4. Monitor all your accounts

In recent years, hackers have grown very advanced in their methods. One set of exposed credentials can be easily cross-checked across many different websites, social media pages and subscriptions/memberships. If any of your passwords are duplicated across platforms, cyber criminals could quickly gain access to profile information that reveals even more about you, such as personal email addresses, phone numbers and even a physical address.

#### 5. Protect your financial privacy

If payment information was leaked as part of a data breach, you should ask your card provider to lock or pause your cards right away and send you a replacement one. By locking the cards, you prevent new purchases from occurring with the leaked card number, and the replacement card will have a new number assigned to it, allowing you to continue with your normal purchases.

Even if your payment information is safe, it's a good idea **to set up credit monitoring. This will alert you when there are any changes to your credit report**, like if someone applies for new credit in your name.

If you are sure that your financial details have been exposed and you have seen changes, **you should take steps to freeze your credit**. There is no cost incurred by doing this and it will prevent malicious actors from opening new credit accounts in your name. what if you have not fall in this current den or you but does it feel good for the future, no then what to do incase to avoid future breach?

**How can I prevent data breaches in the future**

As cyber criminals become more advanced, the consequences of having even a small bit of information about you stolen are becoming more and more serious. Even with an email address or password, malicious actors are, in some cases, able to find more sensitive and powerful data in very little time

### Strong Passwords and MFA

As previously mentioned, good cyber security starts with a strong password that is regularly changed (every 3 to 6 months). A strong password usually consists of at least 8 characters (we recommend 10 to 12). This should be a mixture of letters, numbers, and symbols (if they are permitted). Never include personal information in your passwords such as your parents', kids', pets' names or even your date of birth.

### Keep your software up to date

Often, large companies will provide essential security patches and changes via software updates

### Back up your data regularly

In order to prevent permanent loss of data and important information, we recommend having a backup of your personal data, either held in an external drive or stored securely off-site. Regularly backing up your data means that your information does not have to be constantly stored on your device and anything lost will still be accessible after the initial breach.

### Update your email address book

Whether you're working in an office, from home or freelancing on the go, it's always prudent to ask your clients to notify you if they change their address or other contact details. Equally, you should periodically ask them if they have had any personal breaches themselves. Both of these measures will prevent malicious

actors from accessing your information through identity theft of a colleague/client or a phishing scam.

#### Use secure URLs

This is an essential part of general IT hygiene for all users today. If you receive a link from a colleague or outside source, only open URLs that begin with HTTPS. Equally, when visiting websites online, it is important that they are trusted, often indicated by a padlock on the left of your browser's search bar.

#### Review your access controls

As homeworking becomes more commonplace, it is clear that access to a broader range of software and permissions is needed. However, this does not apply to everyone. If you're worried about security breaches on your work laptop, talk to your IT department about tightening your access controls.

#### **I lost my phone how can I get it or track it down.**

Google provides an app and website called **Find My Device**, which lets you seek out your missing Android, secure it, and erase all data. Samsung devices have an additional feature called **Find My Mobile**, which allows you to track down your lost device. You can follow the procedures highlighted in our incident reporting to solve the issue or check for the experts.

## **D. SITE FUNCTIONALITY QUESTIONS**

### **How can I register with the cybershield account**

Navigate to [www.cybershield.ac.tz](http://www.cybershield.ac.tz), and then click the login button at the top corner of the page, be sure to enter your accurate information to register

### **What happens if I forgot my password**

meanwhile we keep developing self-service functionality for our systems, the cybershield support team will reach you for assistance, send an email through [support@cybershield.ac.tz](mailto:support@cybershield.ac.tz),

### **how can I use TMS system?**

If you or your company want to use the TMS system you have to send a quote message from our website with your information dully filled, our admin will make necessary registration for your account and father contact will be made for the process through your contact info.

### **How does Phishing simulator operate?**

The developed and powered tool that bypass all spam filter and sent email to the inbox, just as the attacker could do to mimic real attack scenarios.

### **How many users can TMS/ phishing simulator hold?**

Our system is active to support as many users as they complete the registration.

**"How can CyberShield help my business improve its cybersecurity posture?"**

- Response: "CyberShield offers a range of services such as Security Awareness Training, Phishing Simulations, and IT Security Consultancy to enhance your cybersecurity posture."

**"Can you tell me more about CyberShield's Security Awareness Training?"**

- Response: "Our Security Awareness Training provides industrial-based and customized training to employees and businesses, leveraging security posture through awareness."

**"How does CyberShield conduct its Phishing Simulations?"**

- Response: "We utilize localized and trending social engineering practices to train employees to navigate real-world phishing scenarios effectively."

**"What is unique about CyberShield's IT Security Consultancy?"**

- Response: "We provide a one-stop connection with security experts worldwide to build and maintain robust IT infrastructures, ensuring business continuity."

### **"Can you explain how CyberShield's TMS System works?"**

- Response: "Our TMS System brings together employees from different locations for unified training and seminars, enhancing learning efficiency with our CyberShield Learning Management System."

### **"How does CyberShield's Cyber Rescue service work?"**

- Response: "With Cyber Rescue, interact with our trained AI module cyber coach to respond to real-time cybersecurity incidents at your convenience, ensuring prompt and effective incident response."

### **"What software solutions does CyberShield offer?"**

- Response: "CyberShield Coders TM, our subsidiary workforce, builds and maintains your company's digital profile, ensuring a safe digital space with our software solutions such as web development, mobile app development, integrated system design and embedded system design and programming."

### **"How does CyberShield ensure the effectiveness of its services?"**

- Response: "We continuously innovate and update our services to stay ahead of evolving cybersecurity threats, ensuring the highest level of effectiveness for our clients."

### **"Can CyberShield cater to specific industry requirements?"**

- Response: "Yes, we offer customized solutions tailored to meet the unique cybersecurity needs of various industries, ensuring comprehensive protection for businesses of all types."

### **"How can I get started with CyberShield's services?"**

- Response: "You can get started by contacting us directly or exploring our website to learn more about our offerings and how we can tailor our services to meet your specific cybersecurity needs."

## **E: RESPONSE TO QUESTIONS OUT OF DATABASE:**

**Input: "Can you tell me about [unavailable topic]?"**

Response 1: "I'm sorry, I don't have information on the subject at the moment. However, I'm here to assist you with any questions you may have about our services or any other related topics. Feel free to ask, and I'll do my best to help, however you can contact our support team immediately for more clarification."

"

Responses 2: "I appreciate your interest in that aspect. While I don't have information specifically on that topic, I'm here to assist you with any questions you may have about our services or related areas. Please feel free to ask, and I'll do my best to provide helpful information, however you can contact our support team immediately for more clarification."

**Tell me about yourself?**

Response: "I'm an AI-powered chatbot created to assist you with any questions you may have about CyberShield Team and our services. Whether you're interested in learning more about cybersecurity incidents and their response, exploring our products, or seeking assistance, I'm here to help! let me know what you'd like to know, and I'll provide the information you need."



## **F. BOGUS QUESTION RESPONSE**

### **"What's the weather like in Antarctica?"**

- Response: "It seems like you're asking about weather information, but our focus is on cybersecurity services. If you have any questions related to our services or cybersecurity in general, feel free to ask, and I'll be happy to assist you!"

### **"Can you tell me the capital of Mars?"**

- Response: "That's an interesting question, but unfortunately, it's not within the scope of our expertise. If you have any questions about cybersecurity or our services, I'd be more than happy to help!"

### **"How many feathers does a chicken have?"**

- Response: "While I'm not equipped to provide information on poultry anatomy, I'm here to assist you with questions related to cybersecurity and our services. Is there anything specific you'd like to know?"

### **"What's your favorite color?"**

- Response: "As an AI chatbot, I don't have personal preferences like favorite colors. However, I'm here to help answer any questions you may have about cybersecurity or our services. Let me know how I can assist you!"

### **"Do you believe in aliens?"**

- Response: "While the topic of extraterrestrial life is fascinating, our focus here is on cybersecurity. If you have any questions related to cybersecurity practices, awareness training, or our services, feel free to ask!"

## **G. UNCLEAR QUESTIONS/CONCEPT**

Response 1: "I'm sorry, I didn't quite understand your question. Could you please provide more context or clarify what you're looking for? That way, I can assist you more effectively."

Responses 2: "It seems like there may be some confusion with your question. Could you rephrase or provide additional details so I can better understand and assist you?"

Responses 3: "I'm here to help, but I'm not sure I understand your question. Can you provide more information or specify what you're looking for? I'll do my best to assist you once I have a clearer understanding."