

## 1. Greeting & Purpose

**Bot:**

Hello 🙋, I'm your AI Cybersecurity Assistant. I help SMEs identify, prevent, and respond to cyber threats.

What do you need help with today?

**Options:**

- ☐ I think my business is under attack
  - ☐ I want to learn about threats & prevention
  - ☐ I need to report an incident to CAK
- 

## 2. If User Selects "Under Attack"

### Step 1 – Identify Threat

**Bot:**

Let's figure out the type of threat you're facing:

- a) Phishing email or suspicious link
- b) Ransomware (files locked with a payment demand)
- c) Hacked email or account
- d) Website down (possible DDoS)
- e) Other / Not sure

### Step 2 – Give Immediate Actions

- **Phishing:** Do not click links, delete email, report to IT.
- **Ransomware:** Disconnect from the internet, don't pay ransom, call CAK.
- **Hacked Account:** Change passwords immediately, enable MFA.
- **DDoS:** Contact hosting provider, enable DDoS protection.

### Step 3 – Provide CAK Contact Info

**Bot:**

Please **report the incident immediately** to the Communications Authority of Kenya:

☎ +254 703 042 700

✉ [incidents@ca.go.ke](mailto:incidents@ca.go.ke)

🌐 [www.ca.go.ke](http://www.ca.go.ke)

---

### 3. If User Selects "Learn About Threats & Prevention"

**Bot:**

Here are the most common SME cyber threats:

- Phishing
- Ransomware
- Business Email Compromise
- Malware & Viruses
- Insider Threats
- DDoS Attacks

Which one do you want to learn about?


**When User Selects a Threat** → Bot explains:

- **What it is**
  - **Risks to your business**
  - **How to prevent it**
  - **What to do if attacked**
- 

### 4. If User Selects "Report Incident to CAK"

**Bot:**

Here's how to contact the **Communications Authority of Kenya (CAK) Cybersecurity Unit:**

 **+254 703 042 700**

 **incidents@ca.go.ke**

 **www.ca.go.ke**

Make sure to have the following ready:

- Description of the incident
  - Evidence (emails, screenshots, logs)
  - Time & date it occurred
- 

### 5. End of Conversation

**Bot:**

Stay safe   — remember to:

- Keep software updated

- Use strong passwords & MFA
- Train your team on cyber awareness