Cohort 8 Group Members and Roles

1. Jean Wanjira - Project Lead
2. Dorcas Nkirote- Frontend Developer
3. Collins Kubu - Backend Developer

John Kuria - ICT Track Mentor

TikTactics

Problem Background

According to the Federal Bureau of Investigation (Miller, 2020), global cyberattacks were up as much as 400% during the height of the COVID-19 pandemic and after, with phishing as one of the most common cyber attacks. For example, a Kaspersky report (Kaspersky, 2022) shows that phishing attacks increased in Kenya by 438% in 2022. Further, in a 2024 study by Interpol among African member states (Interpol, 2024), phishing was identified as the most commonly occurring online threat, expanding its socioeconomic effect across the continent.

Social media is one of the online spaces where phishing is predominant, with attackers expanding their target from emails to social media scams such as fake social media pages, messages and links. For instance, social media phishing on Facebook and Instagram increased by 74.7% at the start of 2019 (Barker, 2019). With the top three social media sites used in Africa being Facebook, TikTok, and Instagram (Adika, 2023), it is evident that this reach provides a broad target for hackers and scammers.

A segment of social media users are social media influencers who significantly impact the online choices made by social media users. For example, a study carried out among over 100 university students in Nairobi showed that influencer marketing was the most effective mode of marketing on the brands that they consume (Ntoiti et al, 2021). Further, a study among 100 SMEs in Nairobi County showed that celebrity influencers positively correlated with brand loyalty (Matwetwe, 2023). These social media influencers utilize platforms such as Tiktok that have seen a significant rise in use among Kenyans partly due to its short and quick video format, such that in 2023, the country led in global use of the platform, with 54% of Kenyan tiktok users actively engaging with the platform (Ranjan, 2023), the highest user engagement in the world. Thus, Tiktok will be the choice of platform for this study.

However, the rise of digital influencer marketing has attracted phishing attackers to target social media influencers due to the size of their following and how much information influencers share on their accounts, thus making information gathering easier. For instance, according to Promoty data, the top ten Kenyan influencers on Tiktok have between 1.8 million and 4.2 million followers each, meaning that these influencers share information with millions of followers leading to their information susceptible to attackers due to this expansive visibility. One of the Kenyan influencers is Kevin Maina, who lost half a million followers after a TikTok email phishing attack (Njoroge, 2024) leading to the hackers hijacking his account and posting content that led to his account being banned. These attacks not only result in significant financial losses but also erode trust between influencers and their followers, causing immense psychological distress. Phishing attacks often exploit social engineering tactics to deceive victims into divulging personal information, highlighting the need for heightened security measures in the influencer industry.

Market Opportunity

In today's landscape, TikTok influencers face a significant security challenge when it comes to phishing attacks. Two common solutions currently in use—Two-Factor Authentication (2FA) and browser-based anti-phishing tools—address certain aspects of account security, but both fall short of fully protecting users from sophisticated phishing schemes.

Two-Factor Authentication (2FA) is widely used by TikTok influencers to secure their accounts. However, it primarily protects against unauthorized access after login, offering little to no defense against phishing attacks that lure users into clicking malicious links or divulging personal information. This reactive measure does not address phishing before it can occur, leaving influencers vulnerable to email-based scams or fake verification messages designed to mimic TikTok notifications.

Additionally, **browser extensions**, such as anti-phishing toolbars, offer generic protection by blocking known malicious websites. However, these solutions are not tailored to specific platforms like TikTok, where phishing techniques often involve platform-specific elements such as fake emails or misleading in-app notifications targeting influencers. Current extensions lack the ability to proactively detect and block phishing attempts designed specifically to exploit the trust TikTok users place in the platform.

TikTactics addresses this gap by offering a platform-specific, proactive phishing prevention solution designed to protect influencers from targeted phishing schemes. By monitoring incoming emails, TikTactics validates email authenticity through domain checks, email header analysis, and content matching against known TikTok standards. Additionally, it automatically blocks access to malicious links before the user has a chance to interact with them, providing a defense mechanism that goes beyond the capabilities of traditional 2FA or browser extensions.

This proactive approach gives TikTactics a unique edge, allowing it to leverage the gap in the market for platform-specific phishing protection. While existing tools focus on general online threats or securing account access after a breach, TikTactics directly targets phishing scams aimed at TikTok users, providing a level of defense currently missing from the influencer security toolkit.

The market potential for TikTactics is substantial. TikTok has over **1.2 billion global users**, and in Kenya alone, **54%** of social media users are active on the platform (Ranjan, 2023). With influencer culture rapidly growing (Ntoiti et al, 2021), especially in regions like Kenya, the need for specialized protection against phishing attacks becomes even more critical. Influencer marketing is projected to reach **$15 billion** globally by 2025, making the security of influencer accounts a high-stakes concern both for individual creators and the broader social media economy. By focusing on phishing prevention for this high-value group, TikTactics positions itself to tap into a lucrative market segment, offering essential protection for TikTok influencers in an increasingly digital economy.

Solution Idea

The primary target users of **TikTactics** are **TikTok influencers**. These users have garnered a substantial following on the platform and frequently interact with their audience through various forms of content. They are particularly **prone to phishing attacks** due to their accounts' value, **extensive reach**, and the **financial opportunities** tied to their online presence. Brands and businesses also engage with these influencers, often through email communication, creating a ripe environment for phishing attempts disguised as **partnership offers** or **verification requests.**

The target users were identified through research on cybersecurity threats faced by social media influencers, with **phishing attacks** emerging as a common issue. TikTok influencers, in particular, were highlighted as vulnerable due to the platform's fast growth, unique content-creation environment, and a user base that often includes younger, tech-savvy individuals who may not be as aware of sophisticated phishing tactics. The increasing number of phishing attempts mimicking official communication from TikTok led to the identification of this group as a priority.

TikTok influencers were chosen because they represent a **high-risk** and **high-visibility** group within the platform. Unlike general users, influencers have more at stake if their accounts are compromised, as their **income and brand partnerships** can be severely impacted. While phishing affects many social media platforms, TikTok's rising prominence, the rapid influx of new influencers, and a **lack of dedicated security tools** for this platform make it a priority. The project focuses on addressing their specific needs rather than targeting broader social media users or influencers on other platforms, which are better served by existing solutions.

While **TikTactics** is designed to protect TikTok influencers, phishing is a widespread problem affecting all users on the platform. However, influencers face unique risks due to their **high follower counts**, the **financial transactions** they manage, and their public-facing personas. These influencers are specifically targeted because compromising their accounts can lead to broader damage, including access to a **large audience** and potential revenue from fraudulent activities.

The decision to focus on TikTok influencers was made because phishing attacks on influencers can lead to far-reaching consequences, including **reputational damage**, **financial loss**, and disruption of partnerships. Unlike general users, influencers' accounts are high-value assets, which makes them prime targets. Addressing their needs ensures that **TikTactics** delivers the most impact where the stakes are highest, and where phishing attempts are more **frequent**.

Solution Prototype

The solution, **TikTactics**, is an app designed to monitor and protect TikTok influencers from phishing attacks by identifying malicious emails posing as legitimate TikTok communications. The **Phishing Detection System** aims to identify and mitigate phishing attempts targeting TikTok users. It relies on various technologies to ensure efficient detection and secure handling of data and authentication processes.

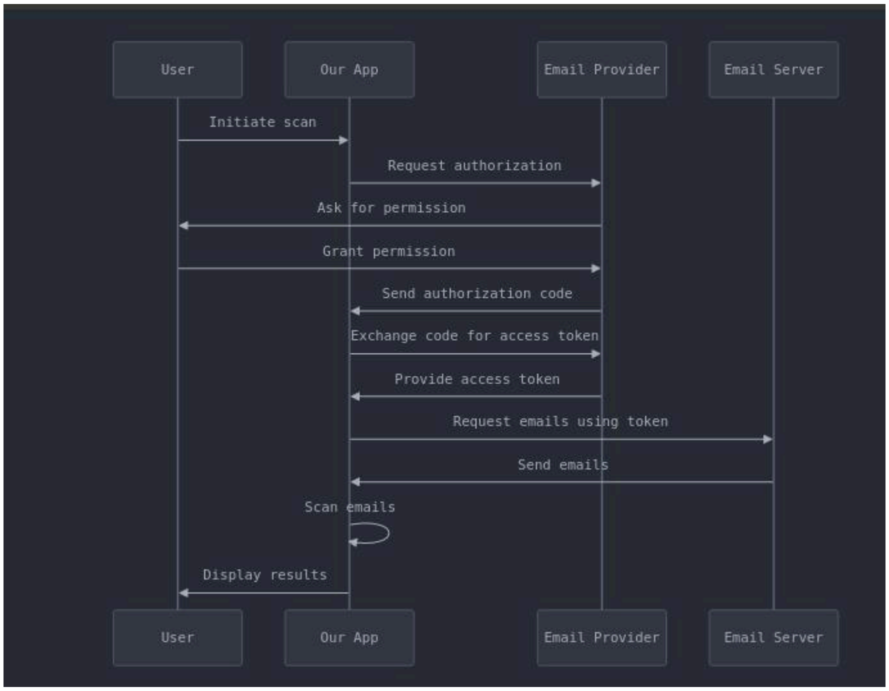
Technology Choices and Justifications:

1. **Backend Development:**
   - **Technology choice:** Python, Django, Django Rest Framework, Kotlin.
   - **Justification:** Python offers simplicity and flexibility in handling various tasks, while Django provides a robust framework for backend development, allowing for rapid growth and scalability. The Django Rest Framework simplifies the creation of APIs for external communication. Additionally, Kotlin will be utilized for Android app development, ensuring mobile users' modern and efficient experience.
2. **Phishing Detection Mechanism:**
   - **Technology choice:** Regular Expressions (Regex).
   - **Justification:** Regex is used to identify suspicious patterns in email subjects and bodies, focusing on phishing language, credential theft indicators, and fake domains. It accurately

detects specific text patterns and allows for flexible updates as phishing tactics evolve. A whitelist is implemented to avoid false positives by validating emails from legitimate TikTok sources.

3. **Database Management:**
    - **Technology choice:** PostgreSQL.
    - **Justification:** PostgreSQL is chosen for its reliability and performance, particularly in handling large volumes of structured phishing-related data. Its advanced query capabilities and support for ACID compliance ensure data integrity and efficient data management.
4. **Authentication:**
    - **Technology choice:** JSON Web Tokens (JWT).
    - **Justification:** JWT offers stateless authentication, which enhances performance by eliminating the need for server-side session storage. This ensures secure and scalable user authentication by embedding claims within the token itself, protecting the system from tampering.

Solution Process



The solution follows a multi-step process to detect and manage phishing attempts effectively. It begins with scanning incoming emails using predefined regex patterns to identify phishing indicators. If a suspicious email is detected, it is flagged, but before that, the sender is cross-checked against a whitelist of legitimate TikTok email sources to ensure that genuine emails are not mistakenly flagged.

Flagged emails are then stored in a PostgreSQL database, along with metadata such as the sender's address, subject, and body, for further analysis. To ensure security, only authorized users can access the system, protected through JWT-based authentication for secure and efficient session handling. This approach ensures that phishing threats are handled efficiently while maintaining security and data integrity.

This solution directly solves the problem of phishing attacks targeting TikTok influencers by proactively identifying and flagging suspicious emails before they can harm users. By leveraging regex patterns designed to detect phishing indicators and cross-referencing the sender with a whitelist of verified TikTok sources, the system prevents phishing emails from reaching influencers' inboxes. This approach minimizes the risk of influencers falling victim to phishing schemes, such as credential theft or account takeover.

Assumptions Made

In designing **TikTactics**, several key assumptions were made to guide the development of the phishing detection solution, which focuses on protecting TikTok influencers from phishing attacks. These assumptions provide the foundational understanding necessary for ideating and implementing the solution:

1. **Phishing is a Persistent Threat for TikTok Influencers**
   The solution assumes that TikTok influencers are a prime target for phishing attacks due to their large follower bases and influential presence on the platform. Attackers are increasingly using social engineering techniques and fake communication to gain access to their accounts. Therefore, a proactive phishing detection system is essential.
2. **TikTok Users are Vulnerable to Social Engineering**
   We assume that many TikTok users, especially influencers, may not have strong technical knowledge about phishing attempts or how to identify malicious communication. This necessitates a user-friendly solution that automatically detects phishing attempts with minimal user intervention.
3. **Email is a Common Phishing Vector for TikTok Attacks**
   The system is designed with the assumption that most phishing attempts targeting TikTok influencers are delivered through email. The solution is therefore focused on monitoring email communications, detecting fake domains, and analyzing phishing language that impersonates TikTok's official communication.
4. **Legitimate TikTok Communications Can be Accurately Whitelisted**
   One key assumption is that TikTok's legitimate communication sources (e.g., official email domains like "tiktok.com") can be effectively whitelisted, allowing the system to focus on detecting emails from suspicious or unrecognized domains. This is based on the understanding that TikTok maintains consistent domains for official interactions.
5. **Regex Patterns Are Reliable for Phishing Detection**
   The solution assumes that regular expressions (regex) are an effective method for detecting phishing emails based on specific patterns in the subject line, body, and sender information. We assume that a well-maintained library of regex patterns can adapt to new phishing tactics as they emerge.

6. **Influencers Will Use TikTactics for Early Phishing Detection**
   We assume that TikTok influencers will adopt **TikTactics** as a proactive tool to safeguard their accounts, relying on the system to detect phishing attempts before they fall victim to account hijacking. The system assumes that influencers are vested in securing their online identity and brand.
7. **PostgreSQL Database Can Efficiently Handle Email Data**
   We assume that PostgreSQL's ability to manage relational data and large volumes of emails will be sufficient for **TikTactics** to store and retrieve phishing email information efficiently. The database's ACID compliance and structured data storage ensure data integrity during transactions.
8. **TikTok Will Not Implement Similar In-House Solutions**
   It is assumed that TikTok does not currently offer a fully-fledged phishing detection solution for its users, particularly influencers and that external tools like **TikTactics** are necessary to fill this gap.
9. **Phishing Tactics Will Evolve, and TikTactics Will Adapt**
   Lastly, we assume that phishing tactics targeting TikTok users will continue to evolve. **TikTactics** will be designed with flexibility in mind, allowing for the regular update of regex patterns and phishing detection methodologies to keep up with the latest threats.

Value proposition

TikTactics is an application that offers TikTok influencers real-time phishing detection to protect their accounts and personal brands from cyber threats.

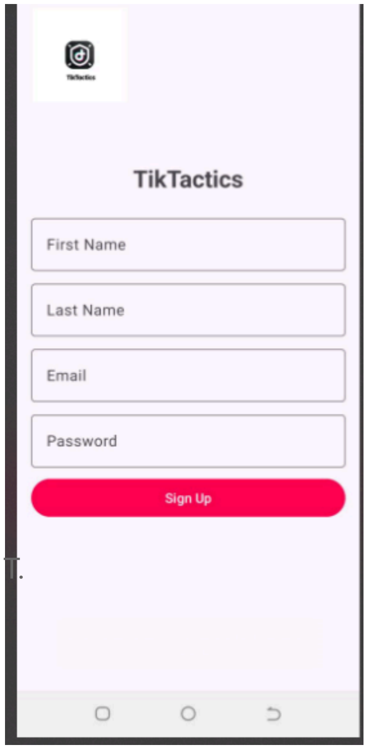
Designed Solution

Technologies Used

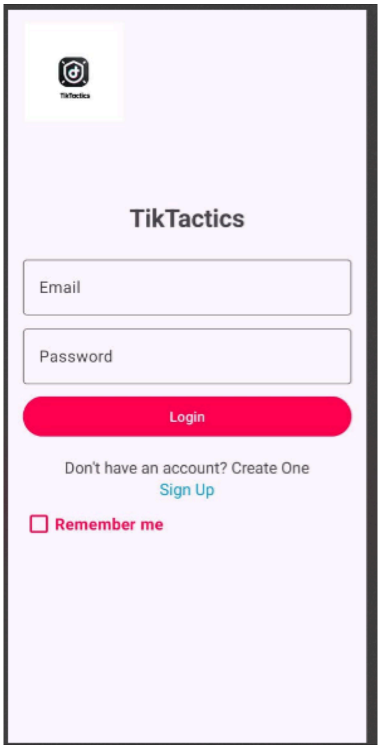
We used **Python** for its simplicity and flexibility in handling diverse tasks, combined with **Django** and **Django Rest Framework,** to provide a robust, scalable framework for backend development and API creation. For phishing detection, we utilized **Regular Expressions (Regex)** due to their precision in identifying phishing patterns, such as fake domains and suspicious language. **PostgreSQL** was chosen for database management because of its reliability and performance in handling large volumes of structured data, ensuring data integrity. Lastly, **JSON Web Tokens (JWT)** were employed for secure, stateless user authentication, enhancing performance and scalability without needing server-side session storage.

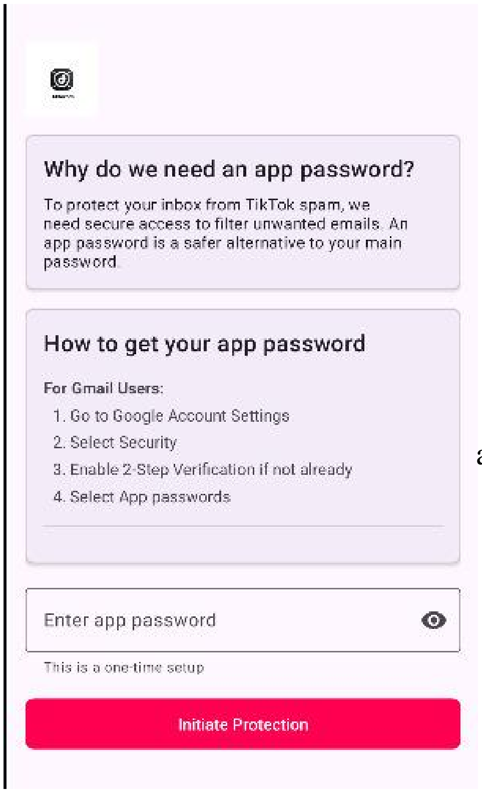
Screenshots of Main Modules

The user creates his/her account.



The user then logs in to the app.





Why do we need an app password?

To protect your inbox from TikTok spam, we need secure access to filter unwanted emails. An app password is a safer alternative to your main password.

How to get your app password

For Gmail Users:

1. Go to Google Account Settings
2. Select Security
3. Enable 2-Step Verification if not already
4. Select App passwords

This page allows users to input their securely app-specific passwords to start phishing detection process.

By entering the password, the app gains authorized access to scan the user’s email for potential phishing attempts while ensuring that all transmitted data is encrypted to protect user privacy. Additionally, this page provides clear user guidance on generating app-specific passwords and includes error-handling mechanisms for incorrect entries, enhancing user experience and enabling seamless phishing detection activation.

Link to the solution

https://github.com/dorcasnkirote/Tiktactics

Business Model

TikTactics will adopt a subscription-based revenue model, offering users tiered pricing options based on the level of phishing protection and features they need. Premium services, such as advanced threat detection, educational resources on safe social media practices. and personalized security audits, will be available for higher-tier subscribers. To ensure financial sustainability, we will explore strategic collaborations with established cybersecurity firms and digital marketing agencies. These partnerships will enable us to enhance our platform's security features and provide expert insights into influencer marketing best practices.

Revenue generated from these collaborations and user subscriptions will be reinvested into continuous platform improvements, including the development of innovative security tools and user-friendly features. Furthermore, funds will be allocated to targeted marketing campaigns aimed at attracting TikTok influencers and users interested in safeguarding their accounts, thereby expanding our user base and ensuring long-term financial stability.

Responsible Computing

1. **User Privacy and Data Protection**: Our solution prioritizes user privacy by implementing robust data encryption protocols and minimizing data collection to only what is necessary for functionality. We will ensure that users have full control over their data, including the ability to delete their accounts and associated information at any time.

2. **Security Awareness and Education**: We recognize the importance of educating users about cybersecurity risks, particularly in the context of social media. Our platform will include comprehensive educational resources, such as tutorials and interactive guides, aimed at enhancing users' understanding of safe online practices, thus empowering them to protect themselves.
3. **Inclusivity and Accessibility**: To ensure that our solution is accessible to a diverse range of users, we will adhere to accessibility standards in our platform design. This includes offering features that accommodate users with disabilities, such as screen reader compatibility and alternative text for images, making our cybersecurity resources available to everyone.
4. **Transparency**: We commit to transparency in our operations by clearly communicating our data collection practices and how user information is utilized. Users will receive regular updates regarding any changes to our privacy policy, ensuring they are informed about their rights and our responsibilities.
5. **Ethical Use of Technology**: We are dedicated to ensuring our technology is used ethically. Our platform will actively promote responsible online behavior among users, discouraging malicious activities such as harassment and misinformation. We will also collaborate with cybersecurity experts to continuously evaluate and enhance the ethical implications of our features.

Traction

User Engagement and Feedback:

- We have conducted preliminary surveys with over 10 potential users, primarily TikTok influencers and users concerned about cybersecurity. Their feedback has been invaluable in shaping our platform's features and functionality (with 90% for example voicing how important this solution will be in ensuring their accounts are protected).

Prototype Testing:

- While we have not yet launched a fully functional product, we developed a prototype shared with a select group of users for initial testing. Two users have interacted with this prototype, providing critical insights for improvements.

Preliminary Revenue:

- We have not yet generated significant revenue, as we are still in development. However, we have explored potential pricing models and have received interest from six users willing to subscribe once we launch.

User Impact:

- Although users have not yet actively utilized our product in a significant way, we have gathered testimonials from potential users who expressed excitement about our concept and how it could enhance their security on TikTok. This indicates a strong market interest that we aim to capitalize on as we refine our offering.

Funding/Support Need

For the first six months of our phishing detection app's development, we have allocated a total budget of **KES 6,444,000**. This budget is strategically distributed to cover essential roles and operational needs associated with our chosen technologies. Specifically, **KES 2,127,000** (26%) is dedicated to hiring a backend Developer, who will leverage Python and Django to develop algorithms that enhance our phishing detection capabilities through accurate data analysis. **KES 1,800,000** (27.9%) is earmarked for the front-end Android Developer, responsible for creating a seamless user experience with the app's interface built using Kotlin.

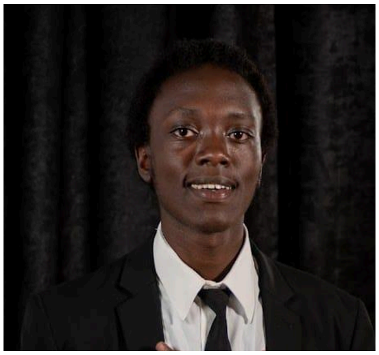
Furthermore, **KES 837,720** (26%) will be allocated for a Security Analyst, who will conduct security assessments and implement protective measures for user data, ensuring compliance with best practices in cybersecurity. To maintain high standards of quality, the Quality Assurance Specialist will receive **KES 837,720** (13%) to carry out extensive testing, and another **KES 837,720** (13%) is designated for UI/UX Design to create an engaging and user-friendly interface. For marketing efforts aimed at promoting the app and attracting users, **KES 837,720** (13%) is reserved, while an additional **KES 837,720** (20%) will be dedicated to infrastructure and hosting costs using PostgreSQL to manage our data efficiently.

As we plan for the next three years, the total budget will increase to **KES 12,888,000**. This expanded budget will allow us to enhance our capabilities significantly over time. We will allocate **KES 4,252,000** (33%) for the Backend developer and **KES 3,600,000** (27.9%) for the Android Developer to ensure their continued involvement in critical development phases, utilizing the Django framework effectively. The budgets for the Security Analyst, Quality Assurance, UI/UX Design, marketing, and infrastructure and hosting will each receive **KES 1,674,000** (13%) to maintain essential operations.

Our team

Our team is exceptionally qualified to develop this phishing detection app, leveraging the latest technologies to ensure a robust solution. Dorcas combines her front-end development skills with advanced security engineering, enabling us to create a secure and visually appealing interface using Kotlin and xml. Collins offers his expertise in backend solutions utilizing Python and the Django Rest Framework to build a scalable and efficient system for handling phishing detection. Meanwhile, Jean's specialized UI/UX design knowledge allows us to craft an intuitive user experience that engages our audience. Together, our diverse skill set and proficiency in these technologies empower us to build an effective solution tailored to combat phishing threats effectively

Dorcas Nkirote



Collins Kubu

Jean Wanjira