KAMI LIMU

HunterTrust

Group Members and Roles

1. James Kibuti - Team Lead
2. Sarah Wangari – CyberSecurity Analyst
3. Vivian Nkatha – Lead Designer

ICT Track Mentor - John Kuria

Problem Background

The rise of Business Email Compromise (BEC) attacks, particularly within Kenya's financial sector, is symbolic of the broader issue of phishing and cybercrime. BEC attacks represent a more targeted, sophisticated form of phishing, where fraudsters impersonate trusted individuals within an organization to manipulate executives, finance teams, or senior managers into authorizing fraudulent transactions. The financial damage resulting from these attacks is staggering, with an increase of 42% reported in Kenya in 2023 alone, underscoring the growing vulnerability of the sector. The reliance on digital communication within banking and financial institutions has only exacerbated the situation, with BEC attacks preying on the trust and authority of senior decision-makers, disrupting operations, and causing significant financial losses.

Several key factors contribute to this growing threat. First, the rapid digitization of the banking sector has created an expanded attack surface for cybercriminals, who exploit the relatively underdeveloped cybersecurity defenses in place. Secondly, the human factor remains one of the

greatest vulnerabilities—fraudsters use social engineering to exploit trust relationships and familiarity between employees, often bypassing more technical security barriers. As attackers evolve their tactics, the financial sector struggles to keep pace, with many traditional security solutions failing to address the specific nuances of BEC attacks.

While the overall phishing problem has been well-researched, the issue persists primarily due to gaps in detection tools and employee awareness programs. Current security systems focus on blocking malicious attachments and links, but they struggle with identifying emails that appear legitimate, particularly when the sender's email and domain closely resemble those of trusted entities. Furthermore, employees often lack the training to recognize these more nuanced forms of attack, leaving organizations vulnerable.

Existing solutions, such as anti-spam filters, firewalls, and email authentication tools, have made strides in combating phishing in general. However, they are not specifically tailored to address BEC, where the sender's email domain is typically similar to legitimate ones but includes slight variations, a technique known as domain spoofing. This gap in detection and prevention leaves financial institutions at considerable risk. The absence of a tool that can specifically detect BEC and similar forms of phishing—by analyzing both behavioral indicators in emails and subtle variations in sender domains—further complicates efforts to protect against these attacks.

This project aims to address these gaps by developing a specialized tool that focuses on detecting BEC attacks within Kenya's financial sector. The solution will not only validate sender domains but will also use advanced algorithms to identify spoofed domains and behavioral patterns in emails, providing an extra layer of protection against BEC attacks. This tool will be designed to

integrate seamlessly with existing security infrastructures, offering a scalable solution to enhance both technical defenses and employee awareness.

In addition to addressing these technological gaps, this project will explore several research questions, such as:

i. How might we design a tool that detects spoofed domains, and impersonation attempts in real time?
ii. What algorithms can be implemented to analyze email behavior for signs of BEC?
iii. How can this solution improve employee awareness of BEC attacks in a financial institution?

Market Opportunity

The market opportunity for a specialized Business Email Compromise (BEC) detection tool remains strong despite the existence of current cybersecurity solutions that offer anti-phishing and email security features. However, these solutions primarily focus on general phishing and malware detection, and while effective in combating common cyber threats, they do not adequately address the nuanced tactics employed in BEC attacks, especially those exploiting trust within financial institutions.

Alternative Solutions

Barracuda Sentinel

Barracuda offers a comprehensive email security solution that includes anti-phishing, malware detection, and spam filtering. It utilizes artificial intelligence (AI) to block threats and can detect

some forms of account compromise. However, its focus remains largely on external threats, such as malicious attachments or links, and it struggles to detect subtle BEC attacks where the attacker uses compromised accounts or similar-looking domains to send fraudulent requests. BEC attacks often bypass traditional email security measures by relying on social engineering rather than overtly malicious content.

Avast Antivirus

Avast is another well-known cybersecurity provider that offers endpoint protection and email security through anti-spam and anti-phishing filters. Like Barracuda, Avast is designed to catch malware, phishing links, and other external threats. However, Avast's solutions are more general in scope and not specifically tailored to detect the sophisticated domain manipulation and internal email compromise techniques that BEC attackers use. This makes it less effective in cases where attackers impersonate executives or other trusted employees.

Gaps in Existing Solutions

Although solutions like Barracuda and Avast provide valuable baseline protection, several key gaps persist:

Inadequate Focus on BEC Attacks: While these tools are effective at detecting typical phishing and malware attacks, they are less capable of identifying BEC threats, which often do not include malware or suspicious links. BEC attacks frequently involve emails from compromised accounts or cleverly disguised domain names that bypass traditional filters.

Domain and Sender Spoofing Detection: Current solutions lack advanced analysis of email domains and sender addresses, which is crucial in detecting slight variations used in BEC attacks.

For instance, fraudsters may create domains that closely resemble legitimate ones (e.g., "xyzbank.com" vs. "xybank.com"), which can evade detection by traditional email filters.

Contextual and Behavioral Analysis: Existing tools do not fully analyze the context or intent behind emails, which is essential in identifying unusual or suspicious behavior typical of BEC attacks. For example, an urgent request for a large financial transfer from a high-level executive to the finance department would go undetected if it came from a legitimate-looking email address, even if the request was fraudulent.

Opportunities for Improvement

To effectively tackle BEC attacks, a more targeted and specialized solution is needed, one that enhances the capabilities of current offerings. There are several suggestions mentioned below:

Advanced Domain Spoofing Detection - A robust BEC tool would include algorithms to detect subtle variations in domains and alert users when an email address appears to be imitating a trusted source, even if the difference is minimal.

Behavioral and Contextual Analysis - A key improvement would be the introduction of behavioral analysis that can detect suspicious patterns in email content, such as unexpected financial requests, urgency markers, or communication patterns that deviate from the norm.

Integration with Existing Tools - A BEC-focused solution should be designed to work alongside existing platforms like Barracuda and Avast, enhancing their capabilities by adding specialized protection without requiring organizations to overhaul their entire cybersecurity infrastructure.

Leveraging the Gap

The gap in the market presents a clear opportunity for a BEC-specific detection tool. Current email security providers lack the sophisticated domain and sender analysis needed to detect the subtle variations often employed in BEC attacks. By focusing on these weaknesses and developing a solution that integrates seamlessly with popular tools like Barracuda and Avast, this project can bridge the gap between general email security and the specific needs of protecting financial institutions from BEC attacks.

Market Size and Opportunity

The Kenyan banking sector is a significant part of the country's economy, making it a promising market for cybersecurity solutions that address the Business Email Compromise (BEC). Here's an analysis of the market size in terms of revenue, target audience, and economic impact:

1. Revenue Potential

Banking Industry Revenue

Kenya's financial sector, including commercial banks, microfinance institutions, and savings and credit cooperative organizations (SACCOs), generates substantial revenue. As of 2023, the total assets of the sector surged to approximately KES 7.7 trillion, marking a significant 17.6% annual growth, and continues to grow due to increased digital adoption and economic recovery post-pandemic. (Kenya Bankers Association, 2024).

Cybersecurity Spending

Kenya's cybersecurity market is expected to reach US$56.13 million by 2024, with a significant portion of this growth coming from cyber solutions like email security and threat detection, which

are crucial in preventing attacks such as Business Email Compromise (BEC). Cyber solutions alone are forecasted to generate US$31.47 million in revenue by 2024. The sector is projected to grow at a compound annual growth rate (CAGR) of 10.54% between 2024 and 2029, ultimately reaching US$92.64 million by 2029. (Statista, n.d.)

Given these figures, it's clear that the rising threat of cyberattacks, particularly in the financial sector, is driving significant investment in cybersecurity infrastructure. BEC and other phishing attacks frequently target banks that are likely to allocate a considerable portion of their budgets to these solutions. This creates substantial revenue opportunities for cybersecurity providers who offer email security, threat detection, and intelligence-sharing platforms tailored to the banking industry.

Such spending could contribute millions of dollars to the market, especially as banks adopt advanced security measures to protect their assets and sensitive data.

2. Affected Target Audience

Banks and Financial Institutions

Kenya has over 40 commercial banks, including major players such as Equity Bank, KCB Group, and Cooperative Bank, and numerous microfinance institutions and SACCOs. These institutions are increasingly digitizing their services, making them prime targets for email-based threats, especially BEC.

Banks have tens of thousands of employees who are potential victims of phishing and BEC attacks. These employees, especially those in high-risk roles like finance, HR, and procurement, form a critical part of the target audience for awareness training and automated threat detection tools.

3. Contribution to the Economy

Key Economic Driver

The banking sector contributes significantly to Kenya's GDP, with estimates suggesting it contributes around 7% to 8% of the total GDP. By securing this industry against email-based attacks, especially BEC, cybersecurity solutions would help protect the broader economy from potentially devastating financial losses. (Kenya Bankers Association, 2023)

Prevention of Financial Losses

BEC attacks can result in the loss of millions of dollars, both for individual banks and the economy. A robust BEC defense across the sector could save businesses and banks millions annually, safeguarding investor confidence and financial stability (Papathanasiou, n.d.). A study on Africa's financial sector showed that cybercrime, including BEC, could cause losses of up to $3.5 billion if left unchecked.

Fostering Digital Transformation

As Kenya accelerates its digital banking transformation, improving cybersecurity will help ensure that the sector continues to grow and contribute to economic development. Cybersecurity resilience will enable smoother digital transitions, increased customer trust, and further expansion of digital banking services.

References

Kenya Bankers Association. (2023, 3 6). Total Tax Contribution of the Kenya Banking Sector 2022. Total-Tax-Contribution-Report-2022.pdf. https://www.kba.co.ke/wp-content/uploads/2023/08/Total-Tax-Contribution-Report-2022.pdf

Kenya Bankers Association. (2024, AUGUST 5). STATE OF THE BANKING INDUSTRY REPORT 2024. State-of-the-Banking-Industry-Report-2024.pdf. https://www.kba.co.ke/wp-content/uploads/2024/08/State-of-the-Banking-Industry-Report-2024.pdf

Papathanasiou, A. (n.d.). Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures—A Perspective on the Greek Landscape. MDPI. Retrieved September 9, 2024, from https://www.mdpi.com/2624-800X/3/3/29

Statista. (n.d.). Cybersecurity - Kenya | Statista Market Forecast. https://www.statista.com/outlook/tmo/cybersecurity/kenya

Solution Idea

Target User

The target users for this project are financial institutions, particularly executives, finance departments, and IT security teams in Kenya's banking sector. These users were identified through research into the specific vulnerabilities associated with Business Email Compromise (BEC) attacks, which typically exploit employees with authority over financial transactions, such as senior management and finance officers. In Kenya, these users have been disproportionately affected, as financial institutions rely heavily on email communication for authorizing large transactions and conducting sensitive operations.

Additionally, IT security teams within these organizations are also key stakeholders. They are tasked with implementing cybersecurity protocols and protecting their institution's digital assets. These teams are often overwhelmed by the evolving nature of phishing and BEC attacks, highlighting their need for a specialized tool that focuses on detecting sophisticated email fraud techniques.

Why this target group?

This group was chosen because of the significant financial impact BEC attacks have had on the sector, which saw a 42% increase in BEC cases in recent years. The high volume of financial transactions and sensitive data processed via email within these institutions makes them prime targets for attackers. While other sectors such as healthcare or education also face phishing attacks, BEC is most prevalent and damaging in finance, where even a single successful attack can result in multi-million-dollar losses.

The problem directly affects this target group, though it indirectly impacts other users such as customers and regulatory bodies who rely on the stability and security of financial institutions. However, the primary focus is on executives and finance teams due to their critical role in authorizing transactions that BEC attackers seek to exploit.

Solution Prototype

The proposed solution is a BEC-specific detection tool that uses advanced sender domain analysis, contextual behavioral analysis, and AI-driven anomaly detection to identify and prevent fraudulent emails. Unlike traditional phishing filters, this solution focuses on the subtle manipulation of email domains and behavior patterns commonly used in BEC attacks, such as impersonation of trusted figures and urgent financial requests.

Technology Choice: The solution uses a combination of:

i. Natural Language Processing (NLP) to analyze email content for context and intent.
ii. Domain and Sender Verification algorithms to identify subtle domain manipulations (e.g., lookalike domains). These technologies were chosen for their ability to go beyond surface-level email filtering, targeting the specific tactics used in BEC attacks that often evade standard cybersecurity measures.

Process Overview

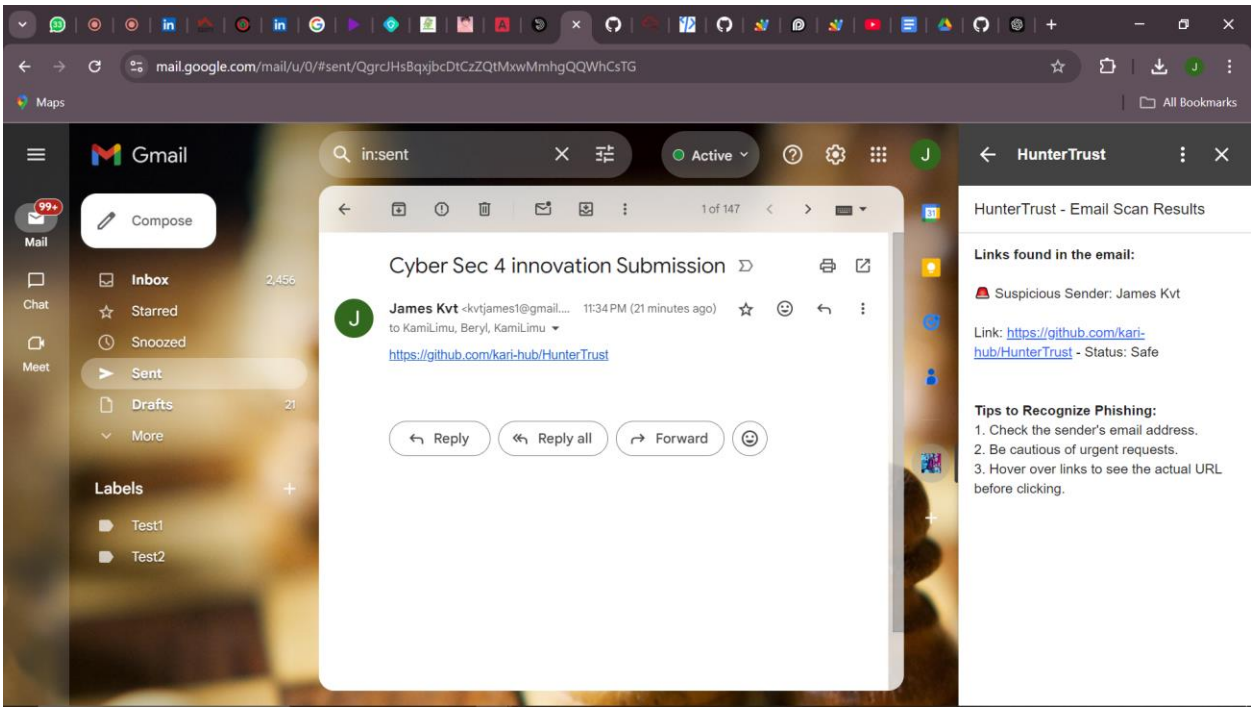
The solution follows a multi-step process designed to analyze incoming emails in real time:

i. **Email Receipt & Initial Scanning**: When an email arrives, the system first checks the sender's domain and compares it to a list of trusted and frequently used domains within the organization. If there is any variation (e.g., “xyzbank.com” vs. “xybank.co”), an alert is generated.
ii. **Content Analysis**: The email body is then passed through a natural language processing (NLP) engine, which analyzes the language for urgency, tone, and financial-related keywords that are typical in BEC attacks. Requests for wire transfers, invoice payments, or sensitive information are flagged for further review.

iii. **Behavioral Anomaly Detection**: The email's behavior is compared against normal email patterns for both the sender and recipient. For example, if an executive typically sends requests to the finance team during office hours but an urgent request for a financial transfer comes through at an unusual time, this deviation from the norm would raise suspicion.

iv. **Risk Scoring**: A risk score is generated based on the domain check, content analysis, and behavior analysis. If the score exceeds a certain threshold, the email is flagged as suspicious and either quarantined or marked for review by the IT security team.

v. **User Notification & Escalation**: If the tool detects a high-risk email, it alerts the relevant user (finance department, IT security team) and suggests next steps. This may include blocking the email, notifying the impersonated user (e.g., the CEO), or launching an internal investigation.



This process ensures that emails are not just scanned for malware or phishing links but are deeply analyzed for the subtle red flags characteristic of BEC attacks, directly addressing the problem outlined in the previous section.

Prototyping

We have built a basic prototype using VirusTotal API and Google Workspace APIs for email integration. Early testing of the prototype has shown promising results, detecting several simulated BEC attempts based on real-world case studies.

How the Solution Directly Solves the Problem

This solution directly addresses the problem of BEC by focusing on the specific attack vectors used in these scams:

i. Domain Spoofing: The tool detects small, hard-to-spot variations in email domains that are often used to trick employees into believing a request is legitimate.
ii. Behavioral Analysis: By analyzing typical email behaviors, the solution can detect abnormal patterns that often indicate BEC attempts, such as unusual timing, urgency, or language used in requests.
iii. Contextual Content Review: Through NLP, the solution can understand the intent behind the email, flagging high-risk requests for financial transfers or sensitive information.

By providing real-time risk scoring and alerting, the tool significantly reduces the likelihood of a successful BEC attack, protecting the organization's financial assets and operations.

Assumptions

Several assumptions were made in developing this solution:

i. Executives and finance teams will continue to rely on email for financial transactions and sensitive communications, making them primary targets for BEC attacks.
ii. Phishing and BEC attacks will remain a persistent threat, requiring organizations to adopt specialized tools rather than relying solely on traditional cybersecurity solutions.
iii. Organizations will have IT security teams in place to manage and act on the alerts generated by the tool.

iv. Kenyan financial institutions will prioritize investment in specialized cybersecurity tools to prevent significant financial losses caused by BEC attacks.

HunterTrust Value Proposition:

HunterTrust empowers Kenyan financial institutions by providing real-time, AI-driven protection against Business Email Compromise (BEC) and phishing attacks. With advanced threat detection tailored to local cybersecurity challenges, we help organizations safeguard their sensitive financial communications and transactions.

Designed Solution

Technologies Used

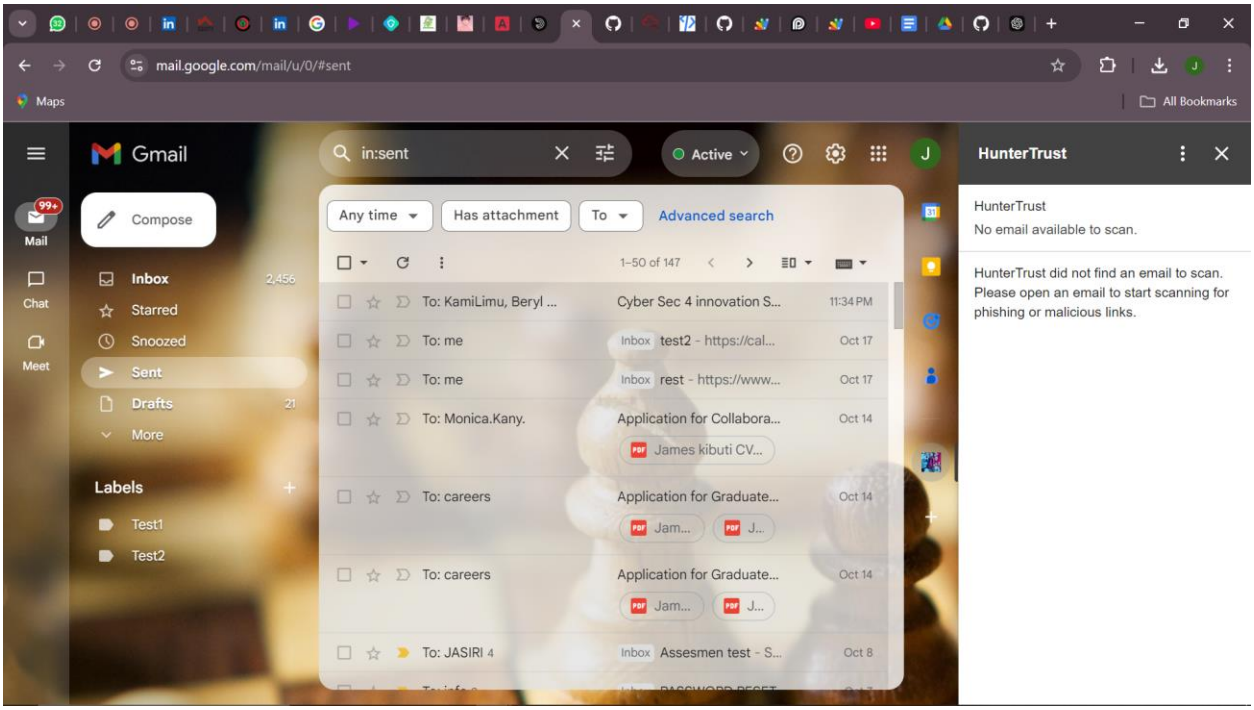
We have chosen specific technologies to ensure our email security solution addresses BEC (Business Email Compromise) threats effectively and efficiently:

1. Google Apps Script -This platform was chosen for its seamless integration with Gmail, enabling us to monitor and analyze incoming emails in real time. By leveraging the Google Workspace APIs, we can easily access and process email metadata while maintaining security and scalability.
2. VirusTotal API - The VirusTotal platform is renowned for its ability to scan files and URLs for malware. Integrating its API allows us to extend our phishing detection capabilities by cross-referencing suspicious links or attachments found in emails against VirusTotal's extensive database.
3. Natural Language Processing (NLP) - We use NLP models to scan the content of emails, analyzing their context and identifying high-risk language patterns. This is especially critical in detecting BEC attempts, where attackers craft messages tailored to individuals within an organization.
4. Cloud Infrastructure (Google Cloud) - Hosting on Google Cloud allows us to leverage secure, scalable infrastructure for real-time threat detection. Using cloud services enables us to scale with increasing traffic, ensuring low-latency responses during email analysis.

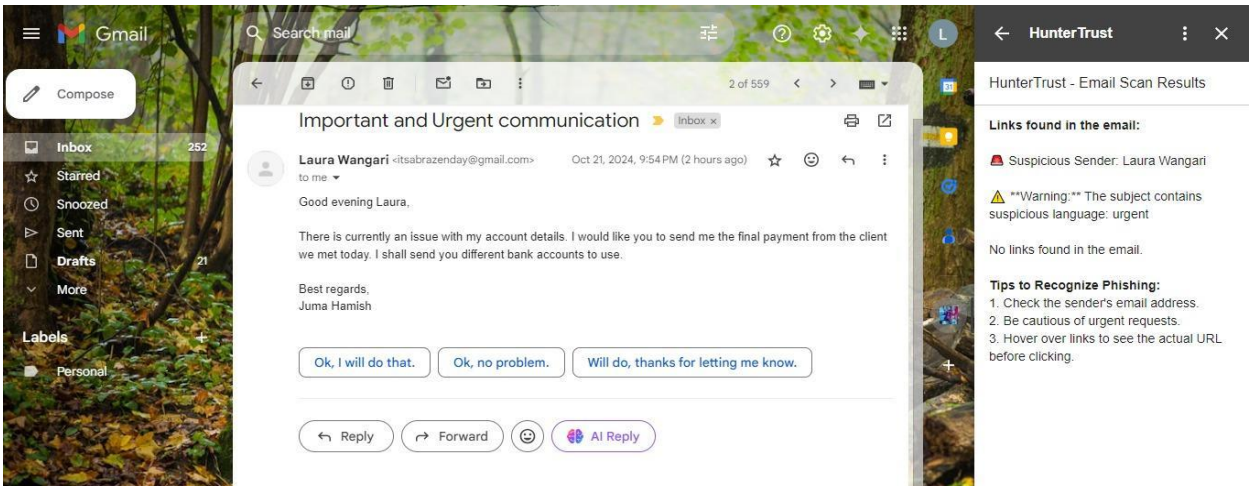
5. GitHub – This is a web-based version control and collaboration platform for software developers that we used for collaboration and version control for this project.

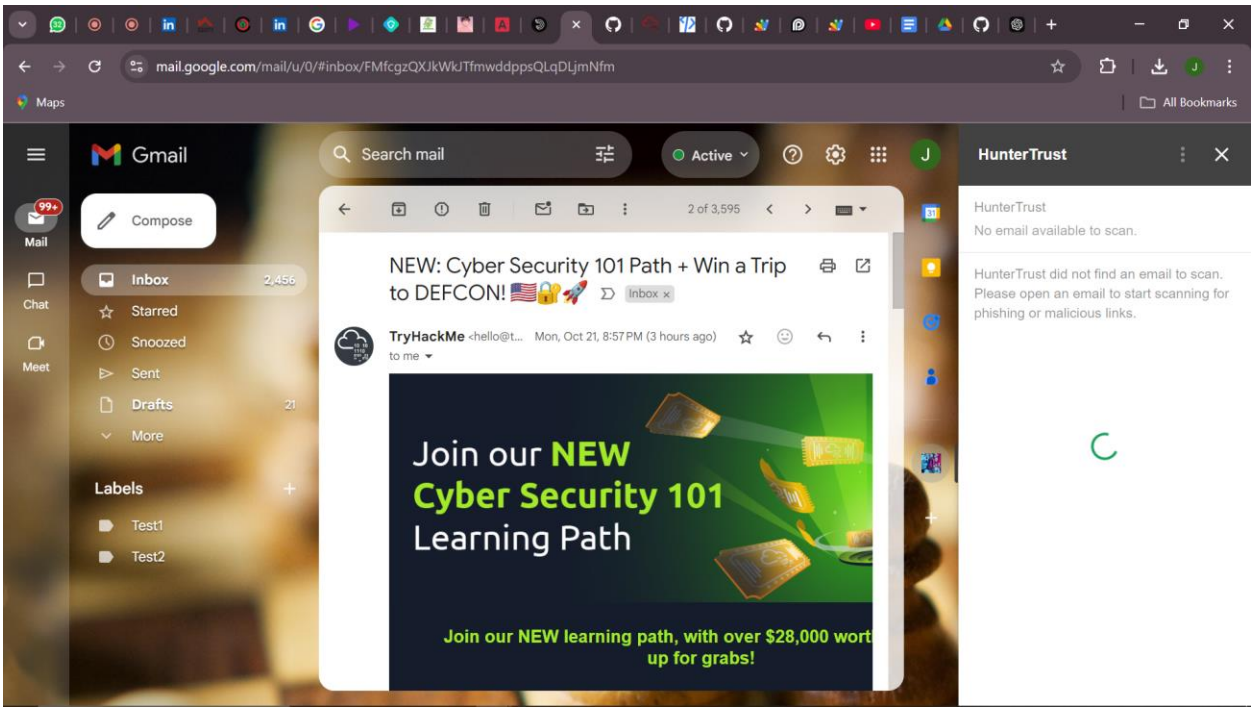
Screenshots of Main Modules

i. **Dashboard Overview**: The dashboard provides users with an overview of the current email security status, highlighting detected threats, flagged emails, and overall risk score.



ii. **Email Analysis Module**: This module shows how emails are scanned in real-time, illustrating the risk score assigned based on content analysis, domain verification, and behavioral patterns.


Gmail
Search mail
Compose
Inbox 252
Starred
Snoozed
Sent
Drafts 21
More
Labels
Personal
2 of 559
Important and Urgent communication
Inbox ×
Laura Wangari <itsabrazenday@gmail.com> Oct 21, 2024, 9:54 PM (2 hours ago)
to me
Good evening Laura,
There is currently an issue with my account details. I would like you to send me the final payment from the client we met today. I shall send you different bank accounts to use.
Best regards,
Juma Hamish
Ok, I will do that.
Ok, no problem.
Will do, thanks for letting me know.
Reply
Forward
AI Reply
HunterTrust
HunterTrust - Email Scan Results
Links found in the email:
Suspicious Sender: Laura Wangari
⚠ **Warning:** The subject contains suspicious language: urgent
No links found in the email.
Tips to Recognize Phishing:
1. Check the sender's email address.
2. Be cautious of urgent requests.
3. Hover over links to see the actual URL before clicking.


mail.google.com/mail/u/0/#inbox/FMfcgzQXJkWkJTfmwddppsQLqDLjmNfm
Maps
All Bookmarks
Gmail
Search mail
Active
Compose
Mail
Chat
Meet
Inbox 2,456
Starred
Snoozed
Sent
Drafts 21
More
Labels
Test1
Test2
2 of 3,595
NEW: Cyber Security 101 Path + Win a Trip to DEFCON! 🇺🇸🔐🚀
Inbox ×
TryHackMe <hello@t... Mon, Oct 21, 8:57 PM (3 hours ago)
to me
Join our NEW
Cyber Security 101
Learning Path
Join our NEW learning path, with over $28,000 wort
up for grabs!
HunterTrust
HunterTrust
No email available to scan.
HunterTrust did not find an email to scan. Please open an email to start scanning for phishing or malicious links.

iii. **Alert Management System**: Screenshot of the alert system where users are notified of potentially dangerous emails, allowing for prompt actions such as quarantining the email or notifying the security team.
https://github.com/kari-hub/HunterTrust

Business Model

Revenue Streams:

1. Subscription-Based Model:
    - Tiered Plans: Offer different subscription tiers based on the size of the organization and the level of security features required. For instance:
        - Basic Plan: Includes core features like email filtering and basic behavioral monitoring. Suitable for small businesses.
        - Pro Plan: Adds advanced features such as real-time alerts, comprehensive threat analysis, and quarantine options. Targeted at medium-sized organizations.
        - Enterprise Plan: Includes all features, with enhanced support, customizable options, and priority updates. Geared towards large corporations and financial institutions.
    - Annual and Monthly Subscriptions: Customers can choose between monthly or discounted annual plans, ensuring predictable revenue flow.
2. Licensing Partnerships:
    - White-Label Solutions: Partner with IT service providers and other cybersecurity firms to offer HunterTrust's technology as part of their solutions, with licensing fees generating revenue.
    - API Integrations: Provide API access to other platforms looking to integrate our email security features, with charges based on usage.

3. Consultancy Services:
    - Offer expert consultancy for organizations that require assistance in setting up and maintaining secure email communication channels. This could include integration, training, and regular assessments.

Ensuring Financial Sustainability:

1. Scalability and Cost Efficiency:
    - Leverage cloud-based infrastructure to keep operational costs low and scale easily as demand grows.
    - Utilize AI and automation to reduce the need for large-scale manual monitoring, ensuring efficient operations.
2. Partnerships and Collaborations:
    - Collaborate with local banks, insurance firms, and industry associations to increase adoption and build trust within the financial sector.
    - Develop alliances with cybersecurity firms for mutual referrals and bundled offerings.
3. Continuous Improvement and Innovation:
    - Regularly update the platform to stay ahead of evolving threats, ensuring continued relevance and effectiveness.
    - Implement feedback loops with clients to identify areas for improvement, thus increasing customer satisfaction and retention.
4. Trial and Freemium Models:
    - Offer a limited-time free trial or a freemium version with basic features, allowing organizations to test the product before committing to a paid plan. This can help drive adoption and conversion rates.

Responsible Computing in HunterTrust

HunterTrust adheres to responsible computing principles by ensuring that user data is handled with care, security, and privacy. Our solution is designed to scan emails for malicious content, suspicious patterns, and Business Email Compromise (BEC) indicators without saving or storing any email content in a database. This approach respects user privacy by ensuring that sensitive information is only analyzed for security purposes and not archived, keeping the integrity of email communications intact.

Additionally, HunterTrust incorporates the following responsible computing principles:

1. Data Privacy: We implement strict data privacy measures, ensuring that no sensitive information is stored or shared without consent. All scans are conducted in real-time, and the results are immediately communicated to users without retaining any data.
2. Transparency: Users are fully informed about what data is being scanned and how the tool operates. This fosters trust and ensures ethical handling of sensitive information.
3. Security: The platform employs strong encryption and secure APIs to ensure that email communications remain protected from unauthorized access during scanning, further enhancing trust.
4. Sustainability: Our solution is designed to be scalable, efficient, and minimizes resource usage, contributing to environmental sustainability by reducing the computational load and energy required for email security operations.

HunterTrust meets high standards of responsible computing while providing effective protection against cyber threats by focusing on these core aspects.

Traction

Our project has made significant strides in its early stages, moving from concept to active engagement with potential users. Below are the key milestones we have achieved so far:

i. User Engagement & Feedback

We have spoken with several potential users, including cybersecurity professionals and stakeholders from local financial institutions. Our professional mentor, John Kuria, has been instrumental in guiding our development and validating the relevance of our solution within the industry. His expertise in cybersecurity has helped us shape the secure email gateway to meet real-world security challenges in financial institutions.

To date, twenty users from financial institutions have tested our secure email gateway prototype. Their feedback has been invaluable in identifying areas for improvement, particularly in threat intelligence integration and user experience. This initial user feedback gives us confidence that our solution addresses critical pain points in email security, such as phishing and BEC (Business Email Compromise). Below is a picture with our mentor, John Kuria, during a feedback session.

ii. Revenue Generation & Impact

While we have not yet generated revenue from the product, we are in the early stages of discussing potential partnerships and future deployments with financial institutions. We anticipate generating revenue as we move from the pilot phase into full-scale implementation.

Our most significant impact so far comes from users reporting a higher level of confidence in the security of their email communications after testing the product. One of our early users shared how the real-time threat detection feature helped them avoid a phishing attempt, which reaffirmed the

effectiveness of our solution. We are encouraged by these early results and are motivated to continue refining the product to enhance its value to more institutions.

Funding/Support Need

To implement and scale the project over the next three years, we estimate a total funding requirement of KES 15 million. This budget will cover both the pilot phase and the expansion post-pilot. Below is a detailed breakdown of our funding needs:

Pilot Stage (6 Months)

For the pilot phase, focused on building and testing the secure email gateway, we require KES 3 million. This funding will be allocated as follows:

i. Software Development: KES 1 million to develop the secure email gateway using JavaScript for core functionality, threat detection, and integration of real-time threat intelligence.
ii. Infrastructure & Security Tools: KES 800,000 for server hosting, cloud infrastructure, and access to necessary security tools.
iii. Personnel: KES 600,000 to compensate developers, security analysts, and the technical team overseeing development and testing.
iv. Phishing Simulations & Employee Training: KES 400,000 to run training sessions, simulations, and ongoing security awareness programs for users in financial institutions.
v. Operational Costs: KES 200,000 for administrative expenses, project management, and contingencies.

Post-Pilot Stage (Year 1 to Year 3)

After the pilot phase, the project will scale to more financial institutions and introduce advanced features, including AI. The budget for the post-pilot phase totals KES 12 million and will be distributed as follows:

i. Platform Scaling & Security Enhancements: KES 4 million to integrate AI into the platform for advanced threat detection, including AI-driven behavioral analysis and NLP for BEC detection. This will ensure the solution can handle growing traffic and evolving security challenges.
ii. Threat Intelligence & Research: KES 3 million to enhance real-time threat intelligence sharing across the sector and invest in research for localized threats, especially within Kenya's banking sector.
iii. Personnel: KES 3.5 million to expand the team, bringing on additional cybersecurity experts, AI specialists, and technical staff to maintain and improve the solution.
iv. Marketing & Client Onboarding: KES 1 million for promoting the solution, onboarding new clients, and partnering with financial institutions.
v. Operational & Administrative Costs: KES 500,000 for ongoing project management, legal support, and other operational needs.

Total Funding Required:

Pilot Stage: KES 3 million
Post-Pilot Stage: KES 12 million
Total for 3 Years: **KES 15 million**

This funding structure ensures that the pilot is sufficiently resourced to deliver a working secure email gateway using JavaScript, while the scaling phase brings in AI to enhance security through

advanced threat detection. The attached graph illustrates the phased allocation of funds, with AI development beginning in the post-pilot stage to ensure sustainable growth and effectiveness.

Our team

Meet the HunterTrust team, a dedicated group of cybersecurity professionals with a shared vision of revolutionizing email security in Kenya's financial sector.

James Kibuti, the team lead and security analyst, is in charge. James combines strategic leadership with expertise in analyzing and mitigating cybersecurity risks. His ability to develop comprehensive solutions and guide his team through complex challenges makes him an ideal leader for the project.

Sarah Wangari, the Threat Intelligence Specialist, works alongside him, who brings her sharp analytical skills to identify emerging cyber threats. With a deep understanding of threat landscapes, Sarah ensures the team remains proactive and well-informed on the latest attack vectors.

Vivian Nkatha, the team's Vulnerability Assessment Specialist, complements their efforts with her detailed approach to security testing. She excels at identifying potential weak points in systems and ensuring they are fortified against attacks.

Together, James, Sarah, and Vivian form a well-rounded team capable of delivering a secure, AI-driven email protection solution. Their combined skills in security analysis, real-time threat detection, and system hardening make them uniquely positioned to tackle the rising threat of Business Email Compromise in Kenya.