CYBERSHIELD

“Where Awareness unlock security”

CODERS

CYBERSHIELD INC TZ

HYBRID CYBER INNOVATION HACKETHON

ORGANIZER: BROKEN TECHNOLOGIES

TEAM:

1. *GODWIN S. ARUGA- Cyber security/ethical hacking/computer networks/developer*
2. *DAVIS DOL – PROGRAMMING (desktop & embedded systems, still and motion graphics, mechatronics).*
3. *DINALES MDOLLO – UI/UX and FRONT-END DEVELOPER*
4. *EMMANUEL RWEYENDERA – FULL STACK DEVELOPER*
5. *ZAPHANIA JAMES- FULL STACK DEVELOPER*

GENERAL PROBLEM: Social engineering attacks among the society has been growing daily due to increasingly sophisticated techniques, tools and tactics that is a subject to human weakness hence results to breach of information such us credential, user accounts, sensitive information that provide a room for successful cyber attack by the cyber criminals.

TARGETED INDUSTRIES:

Ecommerce, Mobile banking, Health care, Personal safety, social media platforms (accounts), Education organizations, Government institutes.

PROPOSED SOLUTION: a user interactive web-based platform, that is dedicated to providing methodologies, tools and techniques through the following services as the methods to combat social engineering

1. Customized Larger scale security awareness training through online and offline self-paced training, interactive sessions, and guided training by the facilitator in all aspects of cyber security that relay social engineering and personal protection (security culture).
2. Phishing simulator to assess the realistic common phishing and social engineering attacks such as baiting, pretexting, email spoofing, spear phishing and social fraud, scenarios and provide a recommendable solution to each simulated scenario hence prevents the social engineering attack.
3. Incident response plans for various security incident in cross cutting cyberspace, for enterprise, individual and company, using the generated response templates, AI chatbot to provide feedback basing on the customized scenarios and emergency contact for father assistance, Localized protocols to follow on response to security incidents, governance and compliance, and recovery procedures.
4. IT cyber tools and modules that include, technical advice to internet devices security settings and configuration, password strengths test tools, antivirus directories, tools for spam email check, and URL check.

GENERAL SITE FUNCTIONALITY AND FEATURES

1. User interactive design and role-based authentication (subscriber, learner, facilitator, and admins)
2. Language localization- Swahili language for content delivery of non-technical- awareness training) purposes and English language for technical learning experience
3. API integration for specific purpose functionality, e.g. SARUFI, CHATGPT, VIRUSTOOL API, Google RECAPTCHA, depending on license condition-free tools are first priority.
4. Inclusion of quick links to most pages of the enter site.
5. Motion pictures to the homepage relating cyber security issues (language: Swahili).
6. Blog page of the website on the current cyber threats and new social engineering techniques. -unlimited from access
7. Active DB to enable upload and download of various material, contain user information etc., *(design condition are granted to developer decision)*

SPECIFIC FUNCTIONALITIES AND FEATURES- To be implemented.

1. TRAINING MODULE- that have the following capabilities
    i. User login as facilitator/learner
    ii. User have access to the learning materials in terms of webpage blog, quiz, or drop cards etc., download depends on the policy to be discussed.
    iii. A student can take assessment from the facilitator and submit for ranking.
    iv. A facilitator user can create class, upload material and receives students feedback in his/her feedback page.
    v. A facilitator to examine the learner progress, disable or unable learner access to the account depending on time frame for learning, assessment criteria etc.
    vi. Chatbot available for the student to answer question relating to site operation and contact for help (this is general function that work on this category)
    vii. A page to allow partner company to initiate training of their employees (customized classes)

viii. A page that allows stakeholders such as researchers, academicians and cyber security experts to upload specific papers on training or awareness building purpose, and posts- must be reviewed by the admin before posted. *(note: upload restricted to pdf file only)*

2. INCIDENT RESPONSE PLAN MODULE: - *this part should appear as a heading with its relevant sub menu listed below.*

The content of this module is likely to be uploaded to the DB by the content creator, as the UI/UX designer you should provide quick links interface to the following document below and the attached link to the repository by the backend developer.

1. Protocols and reporting procedures to follow in response to specific security incident-shall be named -UTARATIBU/RIPOTI TUKIO
2. Guidance on how to respond to attacks or security issues depending on industry-named TUKIO and should have the following sub menu.
    - i. Kuibiwa simu
    - ii. Hali ya taharuki- mawasiliano yasiyo salama
    - iii. Kutuma pesa kimakosa
    - iv. Kupoteza umiliki wa akaunti
    - v. Ripoti mwalifu
    - vi. Mengineyo
3. Templates witch security checklist for compliance for various small and medium industries. - named MIONGOZO

4. Chatbot to provide customized incident advisor, that request a user to describe the situation and then provide guidelines, provided the above tools haven't help-named MSHAURI

3. PHISING SIMULATION MODULE: -***Decision on what methodology to use is a point to discussion.***

Methodology 1. The use of APIs

The algorithmic sketch and design that collect information from the end user about the scenario and then *provide the general view on the impact*, *possible exposed details or information and how to mitigate it* as a result. The implementation of this methodology will depend on integration of this site with various opensource tools (API) To enable functionality *(due to limited time to develop these modules from scratch. The deep study on the available API is going to be considered after discussions along the implementation phase.*

Methodology 2. Psychological playbook

A complete design of scenarios that mimic the real threat, presented inform of videos, animations, drop cards and other suitable and presentable ways, the user has to what on

i. *How the attack is initiated*
ii. *How does it spoof him/her*
iii. *The impact of the situation*
iv. *How to mitigate it*

Methodology 3. Local phisher

A Localized playbook presented inform of podcast (for phone call phishing, text quotes (SMS) and email aiming to provide a sample of common attack techniques.

This is a form of content created and does not depend on user inputs,

4. IT TOOLS

This will cover several tools APIs attached to the platform not limited to (attention to patent rights and APIs policy.

i. *Weak password test*
ii. *URL analysis tool*
iii. *Fraud email identifier*
iv. *SMS semantic analysis*
v. *Social media security culture toolkit.*

UI/UX DESIGN COMPONETS

Please visit the following below attached sites and learn experience on how such platforms look like and interact users.

1. https://www.knowbe4.com/
2. http://www.phishme.com

upon making that survey features inclusive to the following should be included. Your decision to design is fully granted.

Sitename: CYBERSHIELD

Motto: "Where Awareness unlock security"

Note: both name and motto should appear as a site logo

TOP MENU

1. *About us*
2. *Support*
3. *Login tab*
4. *Donate tab*
5. *Home page*
6. *Contact us (email form for enquiry)*

BELOW TOP MENU

7. *Training program*
8. *Incident response plan*
9. *Phishing simulator*
10. *IT tools*

FOOTER: necessary information and quick links to navigate through out the site.

NOTE: Each of the major pages contains sub menus example IT TOOLS have *weak password test, URL analysis tools, fraud email identifier, SMS semantic analysis, social media security culture toolkit*

etc.,

HENCE ITS ADVICED TO GO THORUGH THE DOCUMENT TO RECOGNIZE THE SUB MENU IN EACH CATEGORY TO INCLUDE IN YOUR DESIGN.

SITE DEVELOPMENT TEAM:

COORDINATOR: EMMANUEL

FRONT END TEAM LEAD: DINNAH

GRAPHICS (motion-GUI): DAVIS &DINNA

BACKEND DEVELOPERS, EMMANUEL, ZEPHANIA, DAVIS

CONTENT CREATOR-GODWIN

QUALITY ASSURENCE; GODWIN

CHANGE CONTROL; ALL TEAM

TMELINE; ZEPHANIA

COMMUNICATION MODEL:

WEEKLY UPDATE ON PROGRESS-Saturday 0830 PM- google meeting (formal update)

BASIC ADVISORY FROM TEAM MEMBERS -GENERAL – WhatsApp group, phone call or SMS individual, - ANYTIME NEEDED.

CRITICAL ISSUES: immediate consultation individual responsible, team leader, via normal call or SMS. -ANYTIME

Technical advice; if the issue cannot be solved within a group consulting expert outside the group and thorough use of internet is necessary.

NOTE: OFFICIAL DEVELOPMENT BEGAN: 02 JAN 2024

Phase one: 02 Jan- 14 Jan 2024

1. *UI/UX*
2. *collection of common training content to be included in testing phase*

Phase 2: Jan 15 – feb 20 2024

1. *backend design and implementation*
2. *implementation of available training content to be included in testing phase (11 February 2024)*

phase 3: APIs integration feb 21- march 12

phase 4: final setup and windups march 13-17 actual testing 16 march

phase 5: hosting and quality assurance. 18-23 march.

Note:

1. ***The role Assigned to team member is a subject of close examination during implementation phase however full team cooperation in all aspect of implementation is required.***
2. ***This paper is a guideline to what best we can do and possible techniques, implementation mechanisms however ability to do so is retained for changes and capacity of the person responsible.***

"Let's focus to show who we are, and how capable we are"

Yours

Godwin s. Aruga (0686969536).