Description du projet

CyberLakanani

Solution de lutte contre les arnaques et renforcement de la confiance en ligne.

Nom de l'équipe : CyberVDP

- Ulrich Cédric WANGRAWA

  Contact: +226 06583462 - Email: ulrichcedricwang@gmail.com

- Jacob Evariste TAPSOBA

  Contact: +226 73 63 62 83 - Email: artemis37hacker1@gmail.com

- Jaciel Leonce AYEDJI

  Contact : +226 71 95 62 55 - Email : jacileonayedji@gmail.com

- Romaric NADEMBEGA

  Contact: +226 76 90 01 42 - Email: nadembegaromaric11@gmail.com

Sommaire

1. Contexte

Au Burkina Faso, comme dans les autres pays de l'AES, l'accès à internet et la digitalisation des services s'est largement développé. Cependant, cette transition numérique s'accompagne d'une montée inquiétante des cas d'arnaques en ligne, d'usurpation d'identité et de fraudes sur les plateformes numériques. Par exemple, la Brigade centrale de lutte contre la cybercriminalité (BCLCC) du Burkina Faso a enregistré 4 114 plaintes en 2024, avec un préjudice financier évalué à 1 742 616 173 FCFA selon Africa News. L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI-BF) quant à elle enregistre de plus en plus de cas de signalement de cyberattaques dont les vecteurs d'infection initiaux sont les phishing (liens et messages frauduleux).

Dans toute la région Ouest africaine, le phénomène est encore plus large : selon un rapport de INTERPOL, la cybercriminalité représente désormais plus de 30 % de tous les crimes signalés dans l'Ouest et l'Est de l'Afrique Nairametrics. Des centaines d'entrepreneurs numériques, vendeurs en ligne et utilisateurs honnêtes voient leur réputation ternie à cause du manque de mécanismes fiables pour vérifier la crédibilité des acteurs en ligne.

2. Problèmes identifiés

- Les utilisateurs ne disposent pas d'un outil simple et accessible pour vérifier rapidement si un lien ou un e-mail est fiable ou potentiellement frauduleux.
- Le signalement des arnaques reste fragmenté, peu centralisé et peu exploité pour générer des statistiques ou des alertes communautaires.
- Les plateformes numériques manquent de mécanisme de certification automatique qui permettrait de sécuriser leur réputation et de renforcer la confiance des utilisateurs.
- Le climat de méfiance numérique se généralise avec l'augmentation des utilisateurs qui hésitent à s'engager en ligne, ce qui nuit à l'essor du commerce en ligne et des services digitaux dans la région.
- La croissance rapide de la digitalisation à travers le commerce électronique, le mobile money et les services en ligne se sont développés plus vite que la régulation et la formation des utilisateurs.

- Le manque de maîtrise de la digitalisation accrue : La digitalisation au Burkina Faso et dans la zone AES apparait par moment sans accompagnement structuré.

Cette digitalisation rapide expose les populations de l'AES à des pertes financières importantes, à une baisse de confiance envers les plateformes locales et à une dépendance accrue aux solutions étrangères. D'où l'urgence d'une solution locale.

3. Présentation du projet

- **Nom :** CyberLakanani
- **Type :** Plateforme en ligne pour la prévention des arnaques, la protection des plateformes en ligne et la sensibilisation.
- **Objectif principal :** Renforcer la sécurité des utilisateurs de l'AES via une plateforme accessible et intuitive qui permet de détecter, signaler et prévenir les arnaques numériques, tout en évaluant la fiabilité des applications et services web.

4. Objectifs spécifiques

- Permettre aux utilisateurs de tester des URL et vérifier leur sécurité.
- Permettre aux utilisateurs de tester des adresses e-mail pour détecter des risques de compromission ou d'arnaque.
- Offrir un service de signalement d'arnaques et de compromission, permettant aux utilisateurs de partager leurs expériences et preuves.
- Fournir des statistiques sur les signalements pour identifier les arnaques et les risques de compromissions les plus récurrentes et informer les autorités compétentes.
- Offrir un service d'audit pour applications web ou mobiles : les applications auditées et conformes obtiennent un Badge de Confiance.
- Chatbot WhatsApp proche des utilisateurs, permettant :
    - Signalement d'arnaques
    - Vérification de liens et e-mails
    - Réception de messages de sensibilisation et d'alertes

5. Innovations

- Intégration d'un écosystème complet : analyse automatique, signalement communautaire, audit des plateformes en ligne.
- Proximité utilisateur : chatbot WhatsApp pour interaction directe et sensibilisation.
- Badge de confiance numérique pour la valorisation les applications fiables.
- Tableau de bord analytique pour visualiser les statistiques et tendances des arnaques et compromissions signalées.

6. Fonctionnalités détaillées

- Interactions avec le grand public – Chabot WhatsApp et portail web grand public :
  - Chatbot WhatsApp pour recevoir les demandes des utilisateurs (vérification d'URL, de message, vérification de la fiabilité de site web, vérification de la fiabilité d'application mobile, fiabilité des adresses email, etc.).
  - Soumission d'arnaque ou de compromission avec preuves (captures d'écran, échanges, liens)
  - Réception automatique réguliers de message de sensibilisation.
  - Réception automatique réguliers de signalement d'arnaque ou de compromission avérés.
  - Consultation de statistiques.
- Fonctionnalité de l'application en backend
  - Réception et prise en charge automatique des demandes
  - Test automatique de liens (URL)
  - Vérification automatique de la sécurité des sites web.
  - Détection automatique des sites malveillants ou de phishing.
  - Test automatique d'adresse e-mail
  - Détection automatique de comptes compromis ou liés à des arnaques.
  - Agrégation des données pour analyses statistiques.
  - Audit complet d'applications web ou mobiles.
  - Attribution d'un badge de confiance pour les plateforme
  - Sensibilisation automatisée, envoi de messages de sensibilisation et alertes de sécurité.

7. Technologies utilisées

- Frontend : React.js
- Backend : Python
- Intelligence Artificielle, Automatisation, Chatbot : n8n
- Base de données : PostgreSQL
- APIs externes :
  - Google Safe Browsing (URL scanning)
  - LeakCheck & BreachDirectory (email breach detection)
  - HaveIBeenPwned (email breach)
  - VirusTotal & URLScan.io (analyse URL / fichiers)
  - PhishTank / URLhaus / Abuse feeds
  - Intégration des Indicateurs de compromission de MISP et OpenCTI
  - ZAP API
  - MaxMind GeoIP
- Audit d'application mobile : MobSF

8. Impact attendu

- Réduction des risques liés aux arnaques numériques et fuites de données pour les utilisateurs.
- Renforcement de la confiance numérique entre utilisateurs et entreprises locales.
- Contribution à la maitrise de la digitalisation accrue.
- Soutien à la cyber-souveraineté locale grâce à un système d'audit et de certification des plateformes nationales.

CyberLakanani, c'est un bouclier numérique. Dans un contexte où les arnaques en ligne brisent des vies et freinent la digitalisation de nos pays, notre solution apporte une réponse concrète, endogène et innovante. Notre ambition est claire : faire de l'AES la région la plus sûre du numérique africain.