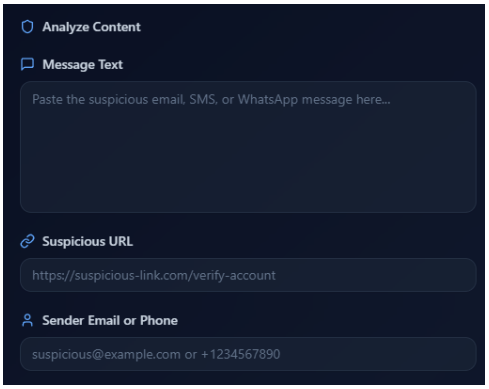
¿Crees que no dejas huella?

CPR SANTIAGO APÓSTOL

Álvaro Casado Campos y Antonio García Piñeiro

RESUMEN DEL PROYECTO

Este proyecto propone el diseño conceptual de dos aplicaciones en una de ciberseguridad desarrolladas con la plataforma Base 44 para mejorar la protección digital de usuarios no expertos. Las aplicaciones son: Anti- Phish Guardian y Privacidad 360. Cada una aborda un riesgo frecuente en Internet: filtraciones de cuentas, fraudes por phishing y exposición de datos personales. El sistema se centra en interfaces simples, alertas comprensibles y recomendaciones educativas que permitan a cualquier persona gestionar su seguridad digital. El objetivo es demostrar cómo la tecnología puede convertir la ciberseguridad en algo accesible para familias, niños y personas mayores.



INTRODUCCIÓN

La vida cotidiana depende cada vez más de servicios digitales, lo que aumenta la exposición a amenazas como el robo de cuentas, el phishing o la filtración de datos. Más del 90 % de los adolescentes tiene al menos un perfil en redes sociales[1], lo que amplía su huella digital pública. Además, según el Federal Bureau of Investigation, el phishing es uno de los ciberdelitos más comunes[2], con más de 298.000 denuncias en un solo año. Muchos usuarios carecen de conocimientos técnicos para protegerse. Este proyecto explora cómo aplicaciones sencillas pueden ayudar a mejorar la seguridad digital

PROPÓSITO DEL TRABAJO

El objetivo del proyecto es diseñar un conjunto de aplicaciones de ciberseguridad accesibles que permitan a cualquier usuario comprender y mejorar su seguridad digital. Se busca crear herramientas que identifiquen amenazas comunes, expliquen los riesgos de forma clara y ofrezcan acciones concretas para prevenir fraudes, robo de identidad o exposición de datos personales.

ESTUDIO DEL ESTADO DEL ARTE

Existen varias herramientas relacionadas con la ciberseguridad y el análisis de huella digital, como Have I Been Pwned, que permite comprobar si un correo aparece en filtraciones de datos; Maltego, utilizado para investigar información pública en internet; o VirusTotal, que analiza enlaces sospechosos y posibles amenazas. Aunque existen muchas aplicaciones de este tipo, en este proyecto decidimos desarrollar nuestra propia herramienta utilizando Base44, con el objetivo de explicar cómo funciona este tipo de tecnología y crear una interfaz sencilla e intuitiva que facilite su uso a cualquier persona.

HIPÓTESIS

Si se desarrollan aplicaciones de ciberseguridad con interfaces simples, análisis automático de riesgos y explicaciones educativas, los usuarios sin conocimientos técnicos podrán identificar amenazas digitales y tomar decisiones más seguras al navegar por Internet.

MATERIAL Y MÉTODOS

El proyecto se basa en el diseño conceptual de dos aplicaciones desarrolladas con Base 44. Se analizaron riesgos digitales comunes y se diseñaron funcionalidades orientadas a prevenirlos. Se definieron flujos de usuario, paneles visuales de riesgo y sistemas de alerta comprensibles. Cada aplicación se enfoca en un área específica: detección de phishing y control de huella digital.

RESULTADOS

El resultado del proyecto es el diseño de dos soluciones digitales complementarias: Anti-Phish Guardian, para detectar estafas en mensajes y enlaces, y Privacidad 360, para analizar la exposición de datos personales en Internet. En conjunto, forman un ecosistema que facilita la protección digital de los usuarios. Actualmente, el sistema se encuentra en desarrollo y, por limitaciones técnicas de la plataforma y de las herramientas utilizadas, todavía no es posible realizar búsquedas ilimitadas, aunque se plantea como una mejora futura para ampliar las capacidades de análisis.

CONCLUSIONES

Las herramientas de ciberseguridad pueden ser más efectivas cuando se diseñan pensando en usuarios sin conocimientos técnicos. Aplicaciones con lenguaje claro, indicadores visuales y recomendaciones simples pueden mejorar la prevención de fraudes y riesgos digitales. Este proyecto demuestra que la combinación de tecnología, educación y diseño accesible puede fortalecer la seguridad digital.

BIBLIOGRAFÍA

- Hadnagy, C. (2015). Ingeniería social: El arte del hacking personal. Anaya Multimedia.
- Caballero, J. (2019). Ciberseguridad para todos: Cómo proteger tu vida digital. Anaya Multimedia.
- López, J. (2020). Ciberseguridad: Curso práctico. Ra-Ma Editorial.
- Stallings, W., & Brown, L. (2018). Seguridad informática: Principios y práctica. Pearson.
- Kaspersky Lab. (2021). Ciberseguridad para principiantes: Protege tu identidad y tus datos. Kaspersky Lab.
- Europa Press. (2019). Más del 90 % de los adolescentes españoles tiene perfil en redes sociales. Disponible en: https://www.europapress.es/epsocial/igualdad/noticia-mas-90-adolescentes-espanoles-tiene-perfil-propio-redes-sociales-usan-sentirse-integrados-20190122121310.html
- Internet Crime Complaint Center – Federal Bureau of Investigation. (2023). Internet Crime Report. Disponible en: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf