Alumnos: Silvia Fernández Mon y Rodrigo Álvarez Fernández

Docente supervisora: Remedios Durán Pernas

Colegio Pablo VI-Fátima, A Rúa, Ourense

CIBER – SEMÁFORO: SACANDO EL RIESGO DIGITAL DE LA PANTALLA AL MUNDO REAL

ÍNDICE

RESUMEN

Este proyecto presenta una solución híbrida de ciberseguridad que combina software y hardware para combatir el *phishing* y la gestión de contraseñas inseguras. Hemos desarrollado una aplicación multiplataforma utilizando tecnología de prototipado rápido que analiza correos electrónicos sospechosos, (ya sea adjuntando el archivo o copiando y pegando el contenido del correo) y evalúa la robustez de las credenciales del usuario. La innovación principal reside en la "tangibilización del riesgo": la aplicación se conecta a un semáforo físico, diseñado y fabricado mediante impresión 3D, que traduce las alertas digitales en señales visuales y auditivas, dando lugar a una simulación de hackeo en caso de alto riesgo.

INTRODUCCIÓN

En la era digital, la ciberdelincuencia ha evolucionado más rápido que la concienciación de los usuarios. A pesar de existir numerosos antivirus y herramientas de verificación online, el factor humano sigue siendo el eslabón más débil: se estima que la mayoría de las brechas de seguridad ocurren por errores de usuario, como hacer clic en enlaces de *phishing* o usar contraseñas débiles.

Este proyecto propone un cambio de paradigma: sacar la alerta de la pantalla y llevarla al mundo físico. Mediante la integración de un dispositivo externo (un semáforo inteligente), buscamos generar una reacción inmediata e ineludible en el usuario, utilizando la psicología del color y el sonido para reforzar hábitos de navegación seguros.

PROPÓSITO DEL TRABAJO

El objetivo principal es desarrollar un sistema accesible y educativo que permita a cualquier persona, independientemente de sus conocimientos técnicos, visualizar el nivel de riesgo de sus acciones digitales en tiempo real.

Pretendemos crear una herramienta intuitiva para detectar correos fraudulentos y demostrar que los estímulos físicos aumentan la atención, concienciación y la respuesta ante amenazas digitales, probando que la retroalimentación física es más eficaz que la digital para captar la atención de cualquier tipo de usuario.

Por ello, con este proyecto también queremos demostrar que el problema de la ciberseguridad hoy en día no es la falta de tecnología: es la " ceguera " o fatiga de alertas. Los usuarios ignoran habitualmente las ventanas emergentes y los avisos de seguridad en pantalla por saturación.

Asimismo, buscamos implementar este proyecto como una solución de bajo coste y código eficiente (No – Code + Imprensión 3D) que pueda ser replicada principalmente en entornos empresariales o educativos

ESTUDIO DEL ARTE

El proyecto innova aplicando principios de “ Internet de las Cosas “(IoT) Y “Computación Tangible”, trasladando la información digital a un objeto físico. El diseño se fundamenta en estudios de Interacción Humano-Computadora (HCI) y psicología del color, que demuestran la superioridad de los estímulos físicos para captar la atención. La lógica de evaluación se basa en los estándares de ”OWASP”, mientras que la necesidad del proyecto está validada por informes de “INCIBE “sobre concienciación ciudadana.

HIPÓTESIS

Se plantea que la implementación de estímulos físicos externos (señales lumínicas y sonoras) vinculados a la evaluación de riesgos digitales aumenta significativamente la percepción de peligro del usuario en comparación con las alertas puramente digitales.

Prevemos que el uso de un semáforo tangible reducirá la "fatiga de alertas", mejorando la retención de consejos de seguridad y fomentando hábitos de creación de contraseñas robustas al trasladar la amenaza invisible del ciberespacio a un entorno físico ineludible.

MATERIALES

- Hardware: Impresora 3D (para la fabricación de la carcasa en PLA), placa microcontroladora (cerebro del sistema), LEDs de alta luminosidad (Verde, Amarillo, Rojo), zumbador activo y cableado de conexión.
- Software: Entorno de desarrollo Base 44 (para la lógica de la App y la interfaz de usuario), Google Forms (para la recopilación de datos estadísticos y conexión en la nube) y software de laminado (Slicer) para la preparación de las piezas 3D.

MÉTODOS

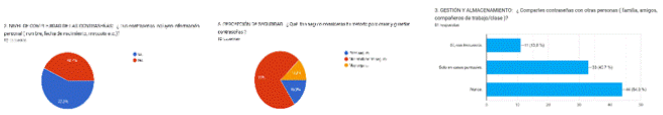
1: Diseño Lógico y Algorítmico (Software): Se programó la lógica de decisión utilizando Base 44. Se establecieron condicionales para evaluar las contraseñas (longitud, variedad de caracteres, etc.) y asignarles un valor de riesgo. Paralelamente, se diseñó la interfaz de la App para que fuera limpia y fácil de usar, priorizando la experiencia del usuario.

2. Prototipado Físico (Hardware)**:** Se modeló la estructura del semáforo en 3D para albergar la electrónica de forma compacta. La impresión se realizó en PLA, un material biodegradable. Se integró el circuito electrónico para que los LEDs y el zumbador respondieran a señales externas.

3. Integración del Sistema Híbrido**:** Se conectó la salida de datos de la App con el dispositivo físico. Cuando el usuario completa la encuesta de seguridad, el sistema procesa la información y envía una señal de disparo (trigger) al semáforo, encendiendo la luz correspondiente y emitiendo un sonido de alerta si el riesgo es alto.

RESULTADOS

Las pruebas de funcionamiento han validado la conectividad entre la aplicación y el semáforo físico. El dispositivo reacciona en tiempo real a las respuestas del usuario, encendiendo la luz roja y emitiendo la alarma sonora ante patrones de contraseñas vulnerables, tal y como se diseñó. Además, realizamos una encuesta previa sobre hábitos de ciberseguridad para establecer la necesidad del proyecto. (Se adjuntan muestras de algunos resultados)



CONCLUSIONEES Y PROYECCIÓN DEL PROYECTO

El “ Ciber – Semáforo “ demuestra que es posible mejorar la concienciación digital mediante la integración de elementos físicos. Hemos comprobado que el semáforo actúa como un refuerzo positivo mucho más potente que un simple aviso de texto en pantalla.

Este sistema es escalable para entornos corporativos (alerta global de virus) y educativos (gamificación para niños). Asimismo, la utilización de herramientas de desarrollo ágil junto con la impresión 3D ha permitido crear un prototipo funcional, económico y escalable.

BLIOGRAFÍA

- Instituto Nacional de Ciberseguridad
- OWASP Fundation
- Norman D.A
- Mark Weiser (1991). - The Computer for the 21st Century. *Scientific American, 265*(3), 94-104.
- Blythe & Sasse - (2007). *The Crying Wolf Problem: The Effect of False Alarms on User Behavior*. Proceedings of the Human-Computer Interaction Conference (INTERACT). Springer

IMÁGENES