

SIMULACIÓN DE CAMPAÑAS DE **PHISHING**



Alejandro Delgado
PROYECTO FINAL BOOTCAMP
CIBERSEGURIDAD

2023/2024
KEEP CODING



1. Índice

1. Índice	1
2. Introducción	2
2.1. Contexto y Justificación	2
2.2. Objetivos del Proyecto	3
3. Marco Teórico	4
3.1. Phishing: Definición y Tipos	4
3.2. Educación sobre Ciberseguridad	6
3.3. Simulaciones de Phishing	10
4. Metodología	14
4.1. Análisis de Requerimientos	14
4.2. Diseño del Sistema	15
4.3. Tecnologías Utilizadas	17
4.4. Desarrollo y Pruebas	18
5. Desarrollo	19
5.1. Configuración del Entorno de Desarrollo	19
5.2. Implementación del Sistema	20
5.3. Desafíos y Soluciones	22
6. Resultados	23
6.1. Funcionalidades Implementadas	23
6.2. Evaluación del Sistema	23
6.3. Puntos de Mejora del Proyecto	24
7. Conclusiones	25
8. Bibliografía	26

2. Introducción

2.1. Contexto y Justificación

En el mundo digital en el que vivimos, la ciberseguridad ha emergido como una de las preocupaciones más importantes para individuos y organizaciones por igual. Entre todas las amenazas que encontramos en la web, el phishing representa una de las tácticas predominantes utilizada por los ciberdelincuentes para poder engañar a los usuarios y poder acceder a información confidencial.

Esta técnica de ingeniería social está basada en el engaño para persuadir a las víctimas de revelar sus datos personales, credenciales financieras o información de seguridad mediante el uso de comunicaciones electrónicas engañosas, siempre aparentando ser fuentes fiables para el usuario.

El crecimiento sufrido en la sofisticación de los ataques de phishing nos da un indicativo de la importancia de la concienciación y la educación sobre la seguridad cibernética como herramientas esenciales en la prevención de dichas amenazas. A pesar del crecimiento en la conciencia en términos de ciberseguridad, muchas personas y organizaciones siguen siendo vulnerables a los ataques de phishing debido a la falta de conocimiento práctico y experiencia a la hora de identificar los intentos de phishing.

En este contexto, desarrollaré un sistema de simulación de phishing como una idea innovadora en este apartado para poder educar y entrenar a los diferentes usuarios en el reconocimiento y el manejo de correos electrónicos de phishing de manera segura y controlada. A través de la simulación de ataques de phishing realistas, los usuarios pueden experimentar de primera mano las tácticas empleadas por los ciberdelincuentes, mejorando de esta forma su habilidad para identificar y poder evitar estas amenazas en situaciones reales.

2.2. *Objetivos del Proyecto*

El proyecto tiene como objetivo general el diseño e implementación de un sistema de simulación de phishing que proporcione una plataforma educativa interactiva y accesible para aquellas empresas concienciadas en términos de ciberseguridad. Los objetivos específicos incluyen:

- **Desarrollar una Interfaz de Usuario Intuitiva:** Crear una interfaz de usuario amigable y accesible que permita a los usuarios interactuar fácilmente con el sistema, realizar simulaciones de phishing y recibir feedback inmediato.
- **Simular Escenarios de Phishing Realistas:** Implementar una variedad de escenarios de phishing que reflejen las técnicas y métodos más comunes utilizados por los ciberdelincuentes, proporcionando así una experiencia de aprendizaje real a los usuarios que reciban este tipo de campañas.
- **Proporcionar Retroalimentación Educativa:** Ofrecer a los usuarios retroalimentación detallada y recursos educativos después de cada simulación para mejorar su comprensión y capacidad para identificar intentos de phishing.
- **Garantizar la Seguridad y Privacidad:** Asegurar que el sistema opere de manera segura y mantenga la privacidad de los usuarios, evitando cualquier riesgo de exposición de datos durante las simulaciones.

3. Marco Teórico

3.1. Phishing: Definición y Tipos

El phishing está considerado, dentro del ámbito de las amenazas de la ciberseguridad, como una de las más prevalentes y efectivas, aprovechando la ingeniería social para engañar a los usuarios y obtener información confidencial.

El phishing (o suplantación de identidad) es bastante conocido, pero si profundizamos en sus variantes podremos identificar y prevenir ataques mucho más específicos.

Durante los siguientes apartados, profundizaremos en diferentes tipos de phishing, explorando sus características, métodos de ataques y aportaré consejos para la detección y prevención de los mismos.

3.1.1. Phishing General

El phishing general es la forma más básica de phishing, donde los atacantes envían correos electrónicos masivos a un gran número de destinatarios. Estos correos suelen ser genéricos y no están personalizados para el receptor.

A menudo, imitan comunicaciones de entidades bien conocidas, como bancos, servicios de correo electrónico o plataformas sociales, con el objetivo de capturar credenciales de acceso, números de tarjetas de crédito o información personal.

Para el proyecto, partiremos desde este punto como base para mostrar cómo se realizan este tipo de campañas de phishing.

Prevención

- Verificar siempre la autenticidad del remitente antes de responder a correos electrónicos sospechosos.
- Evitar hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos no solicitados.

- Utilizar soluciones de seguridad cibernética, como software antivirus y filtros de spam.

3.1.2. Spear Phishing

El spear phishing es una forma más dirigida de phishing, donde los correos electrónicos están personalizados para sus víctimas. Utilizando información específica sobre el individuo o la empresa, estos ataques crean la ilusión de una comunicación legítima mucho más creíble. La personalización puede incluir el nombre del destinatario, detalles de su empleo, o referencias a eventos recientes.

Prevención:

- Educar a los empleados sobre la importancia de proteger la información personal y profesional en línea.
- Implementar políticas de seguridad que requieran la verificación de solicitudes inusuales a través de canales alternativos.
- Utilizar tecnología de detección de phishing que analice el contenido del correo electrónico en busca de señales de alerta.

3.1.3. Whaling

El whaling se centra en los "peces grandes", es decir, altos ejecutivos o personas con acceso a información financiera crítica. Los correos electrónicos utilizados en el whaling son altamente sofisticados, a menudo imitando comunicaciones internas de la empresa y solicitando transferencias de fondos o información confidencial.

Prevención:

- Implementar procedimientos de autenticación de dos factores para transacciones financieras importantes.
- Capacitar a los ejecutivos sobre las tácticas específicas de whaling y cómo identificarlas.

- Asegurar que haya controles internos fuertes y procesos de verificación para solicitudes de información sensible.

3.1.4. *Phishing a través de SMS (Smishing) y Phishing a través de Llamadas telefónicas (Vishing)*

Tanto el smishing como el vishing se apartan de los correos electrónicos y utilizan mensajes de texto y llamadas telefónicas, respectivamente. Estos métodos pueden ser particularmente efectivos porque las personas tienden a confiar más en los mensajes de texto y las llamadas telefónicas que en los correos electrónicos.

Los atacantes pueden pretender ser instituciones financieras, agencias gubernamentales, o proveedores de servicios, solicitando que la víctima revele información personal o realice acciones específicas.

Prevención:

- Ser escéptico con respecto a mensajes de texto o llamadas que solicitan información personal o financiera.
- No responder directamente a estos mensajes o llamadas. En su lugar, contactar a la entidad supuestamente emisora a través de un número de teléfono o un sitio web oficial.
- Informar a las autoridades o a las entidades afectadas sobre intentos de smishing o vishing.

3.2. *Educación sobre Ciberseguridad*

La educación sobre ciberseguridad es una piedra angular en la estrategia de defensa contra ataques de phishing y otras amenazas en línea. Al capacitar a los usuarios en cómo reconocer, responder y reportar intentos de fraude, se fortalece el eslabón más débil en la cadena de seguridad: el factor humano.

Profundizaremos en los aspectos clave de la educación sobre ciberseguridad y cómo estos pueden ser implementados eficazmente.

3.2.1. *Identificación de Señales de Advertencia en Correos Electrónicos y Comunicaciones Sospechosas*

Los correos electrónicos de phishing son un método común utilizado por los atacantes para intentar engañar a las personas y obtener información confidencial.

Sin embargo, hay varias señales de advertencia que pueden ayudarnos a identificar estos intentos fraudulentos si prestamos suficiente atención. Por ejemplo, es bastante común encontrar errores gramaticales y ortográficos en estos correos. Aunque algunos ataques de phishing pueden ser muy sofisticados, muchos muestran errores que, con un poco de cuidado, son fáciles de detectar.

Otro aspecto a tener en cuenta es la dirección de correo electrónico del remitente. A primera vista, puede parecer legítima, pero si miramos más de cerca, podemos notar discrepancias sutiles o dominios que no coinciden con los oficiales de la entidad que supuestamente nos está escribiendo. Esta es una señal clara de que algo no está bien.

Además, debemos ser escépticos con los correos electrónicos que solicitan información personal de manera no solicitada. Los atacantes a menudo se hacen pasar por organizaciones legítimas para pedir datos sensibles, pero es importante recordar que las empresas reales raramente, si es que lo hacen alguna vez, solicitarán este tipo de información por correo electrónico.

Por último, la creación de un sentido de urgencia es una táctica común en los ataques de phishing. Los atacantes intentan presionarnos para que actuemos rápidamente, con la esperanza de que la prisa nos impida verificar la autenticidad de la solicitud. Siempre es mejor tomarse un momento para reflexionar y comprobar antes de responder a este tipo de correos.

Estar atentos a estas señales puede ayudarnos a protegernos de caer en las trampas de los phishers y mantener segura nuestra información personal.

3.2.2. *Prácticas Seguras para Manejar Enlaces y Adjuntos en Correos Electrónicos*

Para mantener nuestra seguridad en línea, es esencial ser precavidos con cómo manejamos los enlaces y documentos adjuntos que recibimos por correo electrónico. A menudo, los atacantes intentan engañarnos para que hagamos clic en enlaces que nos llevan a ejecutar software malicioso o a visitar páginas de phishing.

Una regla de oro es evitar hacer clic en enlaces de correos electrónicos no solicitados. Incluso si el correo parece ser de una fuente de confianza, es más seguro teclear la URL directamente en el navegador o usar un marcador que hayamos guardado previamente. Esta simple acción puede protegernos de caer en muchas trampas ciberneticas.

Además, siempre es una buena práctica verificar los enlaces antes de decidir hacer clic en ellos. Al pasar el cursor sobre el enlace, sin hacer clic, la mayoría de los navegadores nos mostrarán la URL real a la que apunta. Este pequeño paso nos permite detectar discrepancias o dominios sospechosos que podrían indicarnos que el enlace no es seguro.

Cuando se trata de adjuntos, la precaución es igualmente crucial. Los adjuntos en correos electrónicos no solicitados o que parezcan sospechosos nunca deben abrirse sin una verificación previa de su legitimidad. Los atacantes a menudo disfrazan el malware como documentos adjuntos inofensivos, esperando que los destinatarios los abran sin pensar. Verificar siempre la fuente y, si hay alguna duda, es mejor errar en el lado de la cautela y no abrir el adjunto.

Al adoptar estas prácticas seguras, podemos ayudar a proteger nuestras computadoras y nuestra información personal de los riesgos que acechan en los correos electrónicos no deseados y potencialmente peligrosos.

3.2.3. Importancia de la Verificación de Fuentes y la Comunicación Segura

Para asegurarnos de que no caemos víctimas de intentos de phishing, es crucial verificar siempre la fuente de cualquier comunicación que recibamos. Si alguna vez tenemos dudas sobre la legitimidad de un correo electrónico, lo más seguro es tomar la iniciativa de contactar directamente a la organización o persona que supuestamente nos ha enviado el mensaje.

Es importante hacerlo usando información de contacto que hayamos obtenido de fuentes independientes y confiables, en lugar de la proporcionada en el correo electrónico sospechoso. Esta medida nos puede ayudar a confirmar si la comunicación es legítima o un intento de engaño.

Además, para proteger nuestra información personal y financiera, siempre deberíamos optar por utilizar canales de comunicación seguros. Esto significa preferir sitios web que utilicen HTTPS, lo cual asegura que la información que enviamos y recibimos está cifrada y protegida de los cibercriminales.

De igual manera, cuando usamos aplicaciones de mensajería, es prudente elegir aquellas que ofrezcan cifrado de extremo a extremo para nuestras conversaciones. Tomando estas precauciones, podemos reducir significativamente el riesgo de exponer nuestra información sensible y caer en trampas de phishing.

3.2.4. Implementación de Programas de Concienciación sobre Seguridad Cibernética

Para que los programas de concienciación sobre seguridad cibernética sean realmente efectivos, es esencial que se implementen de manera continua, adaptativa y participativa. Esto implica organizar sesiones de capacitación de manera regular, las cuales no solo deben abarcar los principios básicos de la seguridad cibernética, sino también mantenerse al día con las últimas estrategias y

tácticas empleadas en los ataques de phishing. De esta manera, los usuarios estarán siempre informados y preparados para enfrentar nuevas amenazas.

Además, la realización de simulaciones de phishing de forma periódica es una herramienta que aporta mucho valor a la hora de evaluar y mejorar la capacidad de detección de fraudes por parte de los usuarios. Estas simulaciones proporcionan una experiencia práctica que es difícil de replicar en otros formatos de capacitación, poniendo a prueba a los usuarios en situaciones que simulan ataques reales sin los riesgos asociados.

Otro componente crítico de un programa efectivo es la retroalimentación y el análisis posterior a las simulaciones o a incidentes reales de phishing. Proporcionar comentarios constructivos sobre lo que se hizo bien y lo que se puede mejorar es fundamental para el aprendizaje y el desarrollo de habilidades. Este proceso de revisión permite a los usuarios entender mejor sus errores y cómo pueden evitarlos en el futuro.

Finalmente, es vital fomentar una cultura de seguridad dentro de la organización, donde la seguridad sea vista como una responsabilidad compartida por todos. Esto significa alentar a los empleados no solo a estar atentos y reportar cualquier intento de phishing que encuentren, sino también a compartir prácticas y consejos de seguridad entre ellos. Crear un entorno en el que la seguridad es prioritaria y valorada por todos contribuye significativamente a fortalecer las defensas generales contra las amenazas del entorno digital.

3.3. Simulaciones de Phishing

Las simulaciones de phishing representan una herramienta educativa que aporta mucho valor en el ámbito de la ciberseguridad. Al simular ataques de phishing de manera controlada, estas actividades ofrecen a los usuarios y organizaciones la oportunidad de enfrentarse a escenarios realistas sin los riesgos asociados a los ataques reales.

A continuación, profundizaremos en cómo se estructuran estas simulaciones, sus beneficios clave y mejores prácticas para su implementación.

3.3.1. Estructura de las Simulaciones de Phishing

Una simulación de phishing efectiva se desarrolla en varias etapas clave:

1. **Planificación:** Seleccionar los objetivos de la simulación, incluyendo el público objetivo y los tipos específicos de ataques de phishing a simular.
2. **Diseño:** Crear los contenidos de la simulación, tales como correos electrónicos de phishing, páginas web falsas y otros materiales que imiten las tácticas empleadas por los atacantes reales.
3. **Lanzamiento:** Enviar los materiales de phishing a los usuarios objetivo dentro de un marco temporal definido, asegurando que el proceso sea transparente para los participantes.
4. **Seguimiento y Análisis:** Recolectar datos sobre las interacciones de los usuarios con la simulación, incluyendo clics en enlaces, ingreso de información en páginas falsas, y otras respuestas a los intentos de phishing.
5. **Retroalimentación y Educación:** Proporcionar feedback inmediato y constructivo a los participantes, enfocándose en las lecciones aprendidas y ofreciendo recursos educativos para mejorar su capacidad de detección.

3.3.2. Beneficios de las Simulaciones de Phishing

Las simulaciones de phishing ofrecen numerosos beneficios que son fundamentales para mejorar la seguridad cibernética de una organización o de individuos.

Uno de los principales beneficios es la experiencia práctica que proporcionan. Al participar en estas simulaciones, los usuarios tienen la oportunidad de enfrentarse a la sutileza y complejidad de los ataques de phishing en un entorno controlado y seguro.

Esto no solo fortalece su capacidad para reconocer estos intentos de fraude, sino que también mejora su habilidad para responder de manera adecuada, aumentando así su confianza y preparación ante amenazas reales.

Otro aspecto valioso de las simulaciones de phishing es la evaluación de vulnerabilidades que permiten realizar. A través de estas actividades, es posible identificar a los usuarios o departamentos que son más susceptibles a ciertos tipos de ataques de phishing. Esta información es crucial para poder enfocar los esfuerzos de capacitación y recursos de seguridad en las áreas que más lo necesitan, asegurando así una distribución más eficiente de los recursos de seguridad.

Además, las simulaciones de phishing actúan como catalizadores para la mejora continua en materia de seguridad. Al revelar áreas específicas de mejora, tanto en el comportamiento individual de los usuarios como en las políticas y prácticas de seguridad organizacional, estas simulaciones impulsan cambios proactivos. La retroalimentación obtenida a partir de las simulaciones puede ser utilizada para ajustar y fortalecer las estrategias de seguridad, promoviendo un ciclo de aprendizaje y mejora constante.

3.3.3. Mejores Prácticas en las Simulaciones de Phishing

Para que las simulaciones de phishing sean realmente efectivas y bien recibidas, es esencial adoptar un enfoque bien planificado y considerado. Una parte crucial de este enfoque es la comunicación transparente. Es importante informar a los empleados sobre la realización de estas simulaciones, destacando especialmente su finalidad educativa y cómo contribuyen a la seguridad global de la organización.

Hacerlo no solo ayuda a evitar malentendidos, sino que también puede aumentar la participación y el apoyo de los empleados al entender que estas actividades están diseñadas para su beneficio.

La personalización de las simulaciones también juega un papel importante. Adaptar los escenarios de phishing a las características y situaciones específicas de la organización y sus empleados puede aumentar significativamente la relevancia y la efectividad de los ejercicios. Al reflejar situaciones que los empleados podrían encontrarse en su día a día, las simulaciones se convierten en una herramienta de aprendizaje más impactante y memorable.

Otro aspecto a considerar es la frecuencia de las simulaciones. Es vital encontrar un equilibrio que permita mantener alta la conciencia sobre el phishing y garantizar que los empleados estén siempre preparados, sin llegar a saturarlos o causarles fatiga de alerta. La clave está en programar estas simulaciones regularmente, pero dándole el suficiente espacio de manera que se mantenga el interés y la efectividad.

Integrar las simulaciones de phishing dentro de los departamentos de seguridad existentes en dicha empresa puede fortalecer aún más la eficacia de ambos enfoques. Complementar las simulaciones con formación adicional y recursos educativos asegura que los empleados no solo aprendan a identificar intentos de phishing, sino que también comprendan las prácticas de ciberseguridad necesarias para protegerse.

Por último, el análisis y la mejora continua son fundamentales para el éxito a largo plazo de cualquier programa de simulación de phishing. Evaluar los resultados de cada simulación ayuda a identificar tendencias y áreas de mejora, permitiendo ajustar las estrategias de simulación y capacitación con el tiempo.

Este proceso de revisión continua asegura que el programa se mantenga relevante y efectivo, adaptándose a las nuevas tácticas de phishing y a los cambios en el comportamiento de los empleados.

En conjunto, estos elementos forman un marco sólido para implementar simulaciones de phishing de manera efectiva, pudiendo crear un entorno donde los empleados estén bien preparados para enfrentar las amenazas de phishing, fortaleciendo así la seguridad de la empresa en el entorno digital.

4. Metodología

4.1. Análisis de Requerimientos

Para empezar con el proyecto, primero se realizó un análisis de los requerimientos para el desarrollo del sistema que estaba implementando. Durante este proyecto, el proceso fue el siguiente:

- **Identificación de Usuarios Objetivo:** Determinar quiénes utilizarán el sistema, incluyendo organizaciones que buscan entrenar a sus empleados y personas interesadas en que sus personas conocidas pudieran identificar este tipo de estafas en el entorno digital.
- **Recolección de Requerimientos:** Se realizó una búsqueda sobre los patrones habituales de este tipo de atacantes, además de contactar con gente cercana para saber qué esperaba de este tipo de aplicación y cómo se podría fomentar la concienciación en este ámbito.
- **Especificación de Requerimientos:** Una vez tenía toda la información necesaria, empecé a documentar los requerimientos básicos para que esta aplicación fuese aplicable en entornos laborales, entre los que podemos encontrar:
 - Interfaz amigable para el usuario promedio.
 - Personalización de campañas para hacerlas más creíbles en entornos internos de la empresa (datos que un externo no pudiera recabar).
 - Maquetación de correos con campañas comunes, para enseñar al usuario como debe crear este tipo de campañas y acelerar su uso.
 - Subida del logo para enviar un correo aún más creíble.

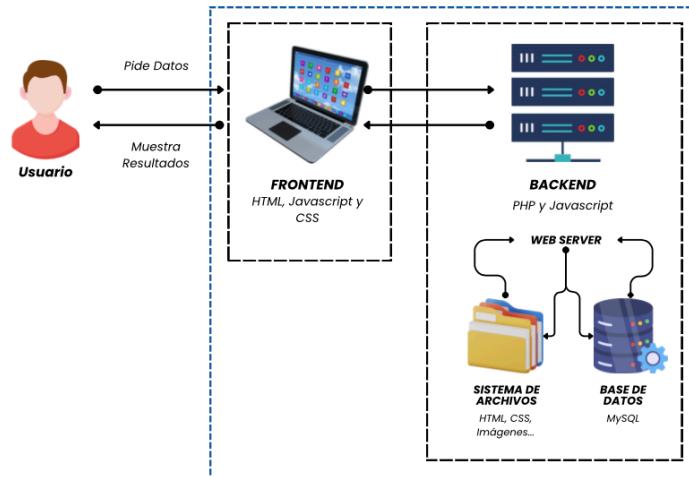
- Subir correos de los destinatarios, ya sea manualmente o mediante un volcado de un archivo. Es fundamental, por ejemplo, en entornos empresariales con 100 empleados, para que no tuvieran que subirlo a mano.
- Mecanismos de seguimiento para saber aquellos usuarios que son vulnerables en este tipo de ataques y poder ofrecerle una formación adecuada.
- Retroalimentación educativa instantánea, haciendo que el usuario vea que ha caído en una campaña de phishing y que sepa cómo actuar una vez haya pasado esto.

4.2. Diseño del Sistema

Una vez tenía los requerimientos necesarios para la construcción del proyecto, se comenzó con el diseño del sistema que transformará estos requerimientos anteriormente descritos en una arquitectura que guiará en la implementación de los mismos. Este proceso incluyó:

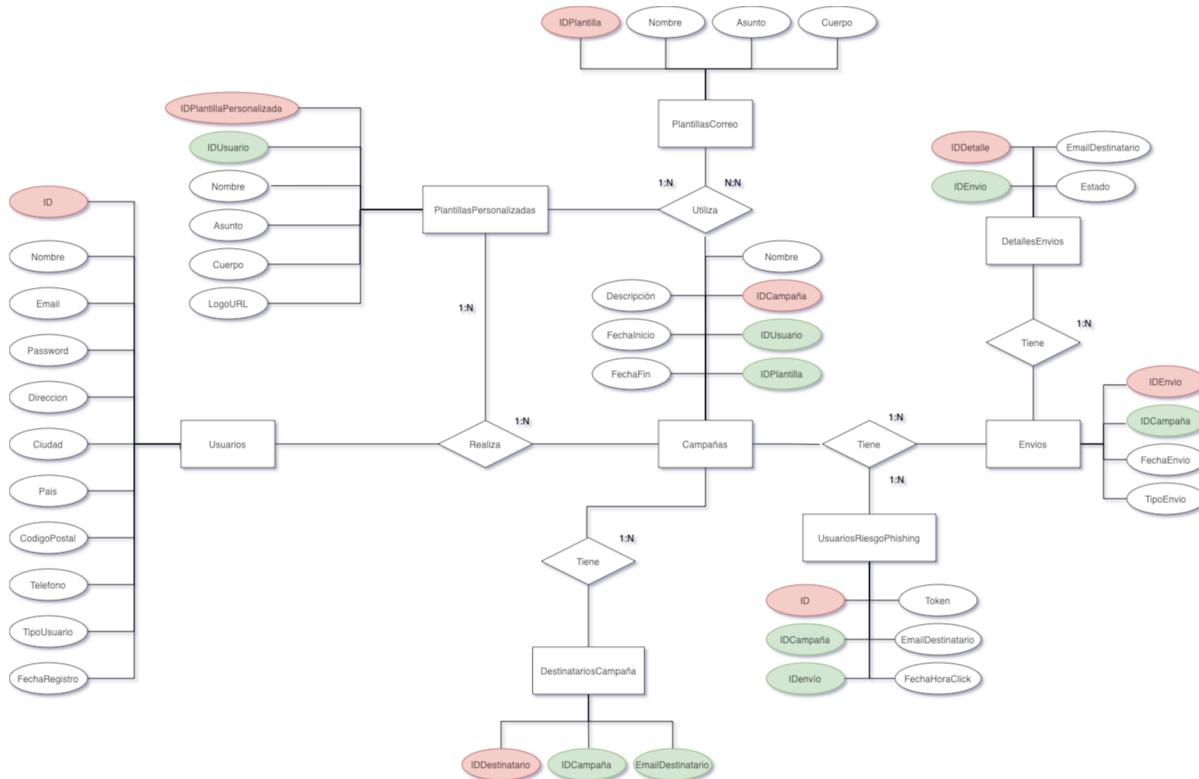
- **Arquitectura del Sistema:**

Definir la estructura general del sistema, incluyendo el front-end para la interacción del usuario, el back-end para el procesamiento de datos, y la base de datos para el almacenamiento de información.

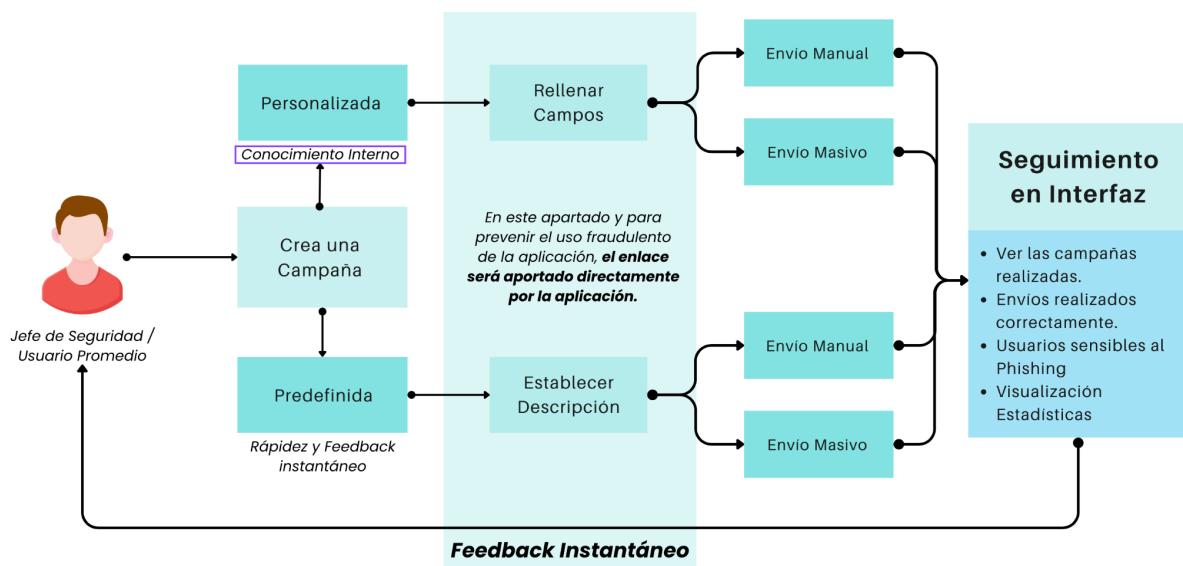


Memoria del Proyecto

- **Diseño de Base de Datos:** Especificar la estructura de la base de datos para almacenar detalles de usuarios, simulaciones, y resultados de evaluaciones.



- **Diseño de la Lógica de Negocio:** una vez hemos elaborado la estructura de la base de datos, realizaremos el diseño de la lógica que debe seguir el usuario.



4.3. *Tecnologías Utilizadas*

La selección de tecnologías es fundamental para el éxito del desarrollo e implementación del sistema. Para este proyecto, elegí las siguientes herramientas y lenguajes de programación:

- **Front-End:** En el ámbito del front-end, he elegido HTML, CSS y JavaScript como los pilares fundamentales para la creación de la interfaz de usuario. Estos lenguajes de programación son fundamentales para estructurar el contenido, diseñar la presentación visual y añadir interactividad al sitio web.

Para complementar estas tecnologías, se ha incorporado Swiper, un slider que enriquece la experiencia del usuario al navegar por el contenido de manera interactiva y visualmente atractiva.

Bootstrap me facilitó mucho el trabajo, ya que este framework de diseño web responsive asegura que la interfaz de usuario sea accesible y estéticamente agradable en todos los dispositivos y tamaños de pantalla, promoviendo una experiencia de usuario coherente.

- **Back-End:** En el lado del servidor, he seleccionado PHP por su robustez y versatilidad para manejar la lógica de negocio y el procesamiento de datos. Esta elección permite un desarrollo dinámico y flexible de aplicaciones web.

Para la gestión de envíos de correo electrónico de forma segura y eficiente, se utiliza PHPMailer, una biblioteca de envío de correos para PHP que es conocida por su fiabilidad.

Además, Composer, un sistema de gestión de paquetes para PHP, ha sido empleado para manejar las dependencias del proyecto, facilitando la instalación y actualización de librerías externas de manera eficiente y manteniendo el proyecto organizado y actualizado.

- **Base de Datos:** Para la gestión de la base de datos, se ha optado por MySQL, dada su eficiencia, escalabilidad y soporte amplio. MySQL es ideal para almacenar y gestionar los datos de usuarios, simulaciones y resultados, ofreciendo un rendimiento óptimo y garantizando la integridad de los datos a través de esquemas de base de datos normalizados.
- **Entorno de Desarrollo y Control de Versiones:** En este ámbito, mi selección fue MAMP, ya que proporciona un entorno de desarrollo local que facilita el desarrollo y pruebas de aplicaciones PHP y MySQL en un ambiente controlado, acelerando el proceso de desarrollo y permitiendo pruebas exhaustivas antes de la implementación.

Para el control de versiones he utilizado Git & GitHub, herramientas esenciales que promueven un flujo de trabajo organizado, permitiendo el seguimiento de cambios en el código.

Finalmente, he utilizado Visual Studio Code como el editor de código para este proyecto, gracias a su interfaz de usuario intuitiva, soporte extenso para diferentes lenguajes de programación y una amplia gama de extensiones disponibles.

4.4. Desarrollo y Pruebas

El desarrollo se llevó a cabo en iteraciones, permitiendo la incorporación de feedback temprano y ajustes en el diseño. Entre las pruebas que realicé se incluyen:

- **Pruebas Unitarias:** Verificar la correcta ejecución de funciones individuales y componentes.
- **Pruebas de Integración:** Asegurar que los distintos componentes del sistema trabajen correctamente juntos.
- **Pruebas de Usuario:** Recoger feedback de usuarios reales para identificar problemas de usabilidad y comprensión.

5. Desarrollo

5.1. *Configuración del Entorno de Desarrollo*

La configuración del entorno de desarrollo es un paso crucial que prepara el camino para un proceso de desarrollo eficiente. Incluye:

- **Instalación de Software:** Para el desarrollo local, se optó por MAMP por su capacidad de facilitar un entorno controlado para aplicaciones PHP y MySQL, eliminando la necesidad de configurar servidores locales como XAMPP.

Visual Studio Code se seleccionó como el IDE principal debido a su interfaz intuitiva y soporte extensivo para HTML, CSS, JavaScript, y PHP, complementado con una amplia gama de extensiones útiles.
- **Configuración de la Base de Datos:** La base de datos MySQL se configuró según los requisitos del proyecto, aprovechando su eficiencia y escalabilidad para gestionar los datos de usuarios y simulaciones. Se diseñaron esquemas de base de datos normalizados para optimizar el rendimiento y garantizar la integridad de los datos, siguiendo las mejores prácticas de diseño de bases de datos.
- **Preparación del Entorno de Trabajo:** Se estableció un flujo de trabajo de desarrollo robusto utilizando Git, con la creación de ramas específicas para el desarrollo, pruebas y producción, facilitando la integración continua y el despliegue continuo (CI/CD). Esto permite automatizar las pruebas y despliegues, asegurando que el código sea de alta calidad y esté listo para producción en cualquier momento.

En el front-end, la elección de HTML, CSS, y JavaScript como pilares fundamentales, complementados con Swiper para la interactividad y Bootstrap para el diseño responsive, asegura la creación de una interfaz de usuario atractiva y funcional en todos los dispositivos.

En el back-end, PHP, junto con PHPMailer para el manejo de correos electrónicos y Composer para la gestión de dependencias, proporciona una base sólida para el procesamiento del lado del servidor y la lógica de la aplicación.

5.2. *Implementación del Sistema*

La implementación del sistema se divide en varias fases, cada una enfocada en diferentes componentes del sistema:

Front-End:

La creación de la interfaz de usuario se realiza mediante la utilización de HTML, CSS y JavaScript, estableciendo así los cimientos para una experiencia de usuario interactiva y visualmente atractiva.

HTML estructura el contenido básico, mientras que CSS se encarga del diseño y la presentación visual, garantizando que la interfaz sea estéticamente agradable y coherente en diferentes dispositivos. JavaScript, por su parte, añade una capa de interactividad esencial, permitiendo una experiencia de usuario dinámica.

Para complementar estas tecnologías y facilitar un diseño responsive, se emplea Bootstrap, un framework que agiliza el desarrollo de interfaces que se adaptan perfectamente a cualquier tamaño de pantalla.

Además, se integra Swiper, un slider interactivo, para enriquecer la navegación y visualización de contenido, mejorando la experiencia del usuario al interactuar con el sitio web.

Back-End:

En el servidor, PHP se elige por su capacidad para manejar eficientemente la lógica de negocio y el procesamiento de datos. Este lenguaje de programación facilita el desarrollo de aplicaciones web dinámicas, permitiendo la autenticación de usuarios, la generación y gestión de simulaciones de phishing, y la recopilación y análisis de los resultados obtenidos.

La implementación de la lógica para enviar correos electrónicos simulados y registrar las interacciones de los usuarios con estos se realiza a través de PHPMailer, asegurando una gestión segura y eficaz de las comunicaciones por correo electrónico. Para una estructura de código más organizada y segura, se considera el uso de Composer, facilitando la gestión de dependencias y la integración de librerías externas necesarias para el proyecto.

Base de Datos:

La gestión de datos juega un papel crucial en el sistema, utilizando MySQL para almacenar y manejar eficazmente los datos de usuarios, simulaciones y resultados.

Se implementan operaciones CRUD (Crear, Leer, Actualizar, Eliminar) para una administración eficiente de la información, mientras se asegura la integridad y seguridad de los datos mediante el uso de consultas preparadas, evitando así vulnerabilidades como la inyección SQL.

Entorno de Desarrollo y Control de Versiones

MAMP provee un entorno de desarrollo local óptimo para el desarrollo y prueba de aplicaciones PHP y MySQL, agilizando significativamente el ciclo de desarrollo. Para el control de versiones y una colaboración eficiente, se utiliza Git & GitHub, promoviendo un flujo de trabajo organizado y facilitando el seguimiento de todas las modificaciones en el código.

Visual Studio Code se selecciona como el editor de código predilecto para el proyecto, gracias a su interfaz amigable, amplio soporte para diversos lenguajes de

programación y la disponibilidad de numerosas extensiones. Esto mejora la productividad del desarrollo al ofrecer funcionalidades avanzadas como resaltado de sintaxis, autocompletado de código, y depuración integrada.

5.3. Desafíos y Soluciones

Durante el desarrollo del sistema, se enfrentaron varios desafíos técnicos y de diseño, entre lo que podemos contar:

- **Simulación Realista de Phishing:** Crear escenarios de phishing creíbles sin comprometer la seguridad del usuario. En este apartado, y al ser un proyecto estudiantil, estaba bastante limitado a la hora de recrear una campaña de phishing real, donde se debería ofrecer enlaces parecidos a los que se está suplantando y otros elementos complicados de realizar.

En esta situación, y debido al escaso tiempo de desarrollo, se optó por lo básico que tiene que contar el proyecto de manera fiable, que es la construcción de correos simulando campañas de phishing actuales. Además, se oculta el enlace para un mayor realismo y se provee al usuario de un feedback instantáneo una vez pulsa sobre el mismo.

- **Educación y Retroalimentación:** Proporcionar retroalimentación educativa efectiva post-simulación. En este apartado, se ha creado una página de alerta para los usuarios que han caído en la campaña que proporciona una visión clara al usuario de que debe concienciarse en este ámbito, proveyendo a su vez de un documento PDF que recoge de forma extensa todo lo básico que debe conocerse sobre el phishing, su prevención y pasos post caída en este apartado.
- **Seguimiento del usuario:** Realizar un seguimiento del click en el enlace del usuario en riesgo de phishing. Para ello, creamos un token basado en la fecha y un número random para facilitar el uso individual por cada usuario.

6. Resultados

6.1. Funcionalidades Implementadas

A continuación detallaré las principales funcionalidades del sistema y cómo estas han contribuido a cumplir los objetivos marcados en el proyecto:

- **Simulaciones Realistas de Phishing:** El sistema permite a los usuarios experimentar ataques de phishing en un entorno controlado y seguro, utilizando escenarios basados en tácticas comunes de phishing, como es el envío de correo suplantando a entidades conocidas o dando posibilidad al usuario interesado en este ámbito de profundizar en dichos detalles y hacerlo mucho más real para los empleados de su empresa o familiares.
- **Retroalimentación Educativa Inmediata:** Después de cada simulación, el sistema proporciona a los usuarios retroalimentación inmediata, destacando los indicadores de phishing que podrían haberse pasado por alto y ofreciendo consejos para mejorar su capacidad de detección, además de un documento PDF educativo con todo lo que debe saber sobre el phishing.
- **Análisis de Resultados y Seguimiento:** El sistema recopila datos sobre las interacciones de los usuarios con las simulaciones, permitiendo a los administradores saber aquellos usuarios que tienen más posibilidades de caer en este tipo de campañas y poner en peligro la información sensible de la empresa.

6.2. Evaluación del Sistema

Para la evaluación del sistema realice propiamente el feedback de la misma, contando además con diferentes personas tanto cercanas como externas sobre puntos de mejora de la aplicación.

Durante la propia evaluación del sistema puedo decir que cumple de forma básica lo que promete y se cumplen los objetivos que establecí para el proyecto así como ofrece una interfaz sencilla para el usuario promedio que acceda a la aplicación.

Por otro lado, el feedback externo ha sido favorable debido a su facilidad de uso y la inmediatez con la que pueden crear campañas y ayudar a aquellas personas que creen que pueden caer en este tipo de estafas.

6.3. *Puntos de Mejora del Proyecto*

Aunque se han cumplido las expectativas puestas en el proyecto, a pesar de las limitaciones de tiempo sufridas, he considerado las próximas mejoras que podría tener el proyecto si decidido continuar con él y profundizar en este ámbito:

- **Mejora de la Interfaz:** Uno de los próximos pasos a realizar en la aplicación es la mejora de la interfaz, ofreciendo un diseño más avanzado y profesional de la aplicación para su futuro uso en empresas o a nivel usuario.
- **Ver detalles de las Campañas:** La idea sería abrir cada una de las campañas realizadas y comprobar directamente los envíos que se han realizado en dicha campaña, los clicks que se realizaron y poder ver cada una de ellas de forma individual.
- **Personalizar aún más los correos:** En este punto, para mejorar este tipo de simulaciones podríamos optar por maquetas predefinidas más avanzadas, mencionando los nombres de los usuarios a los que se les está enviando el correo. Además, se podría dar un formulario más específico al usuario para ayudar en este enfoque a que la campaña sea lo más realista posible.
- **Otros tipos de simulaciones:** Además de mejorar lo que hay actualmente, podríamos configurar diferentes tipos de campañas de phishing, ya sea por SMS o por voz, por ejemplo.
- **Añadir adjuntos:** Otro elemento a añadir podrían ser adjuntos maliciosos.

7. Conclusiones

El hecho de haber desarrollado este proyecto de simulación de campañas de phishing es debido básicamente a la creciente preocupación en las empresas de este apartado de la ciberseguridad a nivel global, donde se ataca normalmente al eslabón más débil y que puede revelar información sensible de diferentes ámbitos.

La herramienta que he proporcionado al finalizar este proyecto espero que suponga una ayuda significativa frente a los abusos de los cibercriminales en este ámbito, en el que la suplantación de identidad se ha consagrado como una de las amenazas más significativas en el entorno digital, además de fomentar la concienciación y proporcionar una ayuda educativa en este ámbito.

A través de la simulación de ataques de phishing realistas y el feedback educativo proporcionado he buscado darle una herramienta al usuario promedio que le ayude a evitar este tipo de campañas fraudulentas fomentando la educación en este concepto a los eslabones más débiles de la cadena, que mejore su conocimiento sobre este tipo de amenazas y sepan cómo contrarrestar de forma inmediata.

Uno de los logros más significativos del proyecto es la creación de un ambiente seguro en el que los usuarios pueden experimentar la dinámica de los ataques de phishing sin los riesgos asociados a los encuentros reales. Esta experiencia práctica es complementada con retroalimentación instantánea y recursos educativos que refuerzan el aprendizaje y fomentan una cultura de seguridad proactiva.

Finalmente, con el desarrollo de este proyecto, mi aprendizaje en el ámbito de la ciberseguridad ha avanzado mucho, recabando diferentes campañas realizadas a través de los años y estudiando cómo prevenir este tipo de ataques.

Ha sido un proyecto gratificante, en el que lamento no haber profundizado más por la limitación en el tiempo, pero que me ha ayudado a comprender la importancia de la ciberseguridad y que me ha permitido elaborar un proyecto que pueda ayudar a otras personas en contra de estas amenazas.

8. Bibliografía

González, P. (2023, October 16). *Los 8 tipos de ataque phishing más utilizados*. Sello Legal Abogados. Retrieved February 21, 2024, from

<https://sellolegal.com/blog/los-8-tipos-de-ataque-phishing-mas-utilizados/>

La guía definitiva del phishing. (n.d.). MetaCompliance. Retrieved February 21, 2024, from <https://www.metacompliance.com/es/lp/ultimate-guide-phishing>

Phishing. (n.d.). Wikipedia. Retrieved February 21, 2024, from

<https://es.wikipedia.org/wiki/Phishing>

¿Qué es el phishing? | Cómo protegerse de los ataques de phishing. (n.d.).

Malwarebytes. Retrieved February 21, 2024, from

<https://es.malwarebytes.com/phishing/>

Rashid, S. (n.d.). *Reconocer los ataques de phishing en 2023*. MetaCompliance.

Retrieved February 21, 2024, from

<https://www.metacompliance.com/es/blog/cyber-security-awareness/recognition-phishing-attacks>

Recomendaciones para evitar ser víctima del phishing. (n.d.). FCE UNLP. Retrieved February 21, 2024, from <https://www.econo.unlp.edu.ar/detise/phishing-3923>