LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

Ingeniería Social: Exponiendo vulnerabilidades en la red con Estudiantes de la Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo Magdalena.

Social Engineering: Exposing vulnerabilities in the network with Students from the Rural School for Girls in the Isla del Rosario district of the municipality of Pueblo Viejo Magdalena.

Ingeniero Emerson Carbono Carbono
Contacto: ecarbonoc@libertadores.edu.co

Ingeniera Sandra Patricia Lopez Bulla
Contacto: splopezb@libertadores.edu.co

Ingeniera Constanza Puentes Sánchez
Contacto: zcpuentes@libertadores.edu.co

Ingeniero Héctor Manuel Herrera Herrera
Contacto: hmherrerah@libertadores.edu.co

RESUMEN

Este artículo tiene como objetivo realizar un experimento mediante el uso de técnicas de ingeniería social, enfocado específicamente en los estudiantes de la Escuela Rural de Niñas ubicada en el corregimiento Isla del Rosario, perteneciente al municipio de Pueblo Viejo en Magdalena. Esta área se caracteriza por ser una zona rural apartada en Colombia, con un nivel de cultura digital aún en desarrollo. Se destaca la presencia de una brecha significativa en cuanto al acceso a capacitación en temas de ciberseguridad, en comparación con los estudiantes de zonas urbanas en las principales ciudades del país.

La elección de este entorno específico se fundamenta en la necesidad de comprender y abordar las disparidades existentes en la preparación y concienciación sobre ciberseguridad entre las áreas urbanas y rurales. La falta de recursos y oportunidades en regiones remotas como Isla del Rosario puede traducirse en una mayor vulnerabilidad frente a amenazas digitales, por lo que este experimento busca proporcionar datos valiosos para la formulación de estrategias educativas adaptadas a las necesidades particulares de estas comunidades.

El objetivo de este experimento es exponer las vulnerabilidades en la seguridad de los estudiantes de grado 8 y 9 de la Escuela Rural de Niñas, en dispositivos móviles en un entorno rural, donde la conciencia sobre ciberseguridad y las prácticas de protección digital pueden ser menos frecuentes o encontrarse en una fase menos avanzada. Los jóvenes, como usuarios activos de la tecnología, enfrentan riesgos significativos en un contexto en el que la exposición a amenazas en línea podría acarrear consecuencias más graves debido al limitado conocimiento sobre ciberseguridad.

A través del análisis detallado en cada fase del experimento, se logró obtener una comprensión más profunda de las percepciones de seguridad, el nivel de exposición a riesgos cibernéticos y la efectividad de las prácticas de seguridad actuales en el contexto rural específico objeto de estudio. Los resultados y conclusiones derivadas de esta investigación ofrecen una visión valiosa sobre la relevancia de la educación en ciberseguridad en entornos con menor acceso a la información digital, resaltando la necesidad crítica de fortalecer la protección digital en comunidades rurales apartadas.

Es importante destacar que la investigación se llevó a cabo con el máximo respeto a los principios éticos y la privacidad de los estudiantes participantes. El objetivo central es contribuir a cerrar la brecha existente en el acceso a conocimientos esenciales de seguridad digital, promoviendo así un ambiente educativo más equitativo e inclusivo para todos los estudiantes, independientemente de su ubicación geográfica.

PALABRAS CLAVES: Ingeniería social, Ciberseguridad, Vulnerabilidades, Cultura digital, Amenazas cibernéticas, Conciencia de seguridad, Riesgos en línea, Prácticas de protección, Ataques cibernéticos simulados, Credenciales de usuarios, Exposición digital.

ABSTRAC

This article aims to carry out an experiment through the use of social engineering techniques, specifically focused on the students of the Rural Girls' School located in the Isla del Rosario district, belonging to the municipality of Pueblo Viejo in Magdalena. This area is characterized by being a remote rural area in Colombia, with a level of digital culture still developing. The presence of a significant gap in access to training on cybersecurity issues stands out, compared to students from urban areas in the country's main cities.

The choice of this specific environment is based on the need to understand and address existing disparities in cybersecurity preparedness and awareness between urban and rural areas. The lack of resources and opportunities in remote regions such as Isla del Rosario can translate into greater vulnerability to digital threats, which is why this experiment seeks to provide valuable data for the formulation of educational strategies adapted to the particular needs of these communities.

The goal of this experiment is to expose security vulnerabilities for 8th and 9th grade students at the Rural Girls' School on mobile devices in a rural environment, where

cybersecurity awareness and digital protection practices may be less prevalent. or be in a less advanced phase. Young people, as active users of technology, face significant risks in a context where exposure to online threats could lead to more serious consequences due to limited knowledge about cybersecurity.

Through detailed analysis of each phase of the experiment, a deeper understanding of security perceptions, the level of exposure to cyber risks, and the effectiveness of current security practices in the specific rural context under study was obtained. The results and conclusions derived from this research offer valuable insight into the relevance of cybersecurity education in environments with less access to digital information, highlighting the critical need to strengthen digital protection in remote rural communities.

It is important to highlight that the research was carried out with the utmost respect for the ethical principles and privacy of the participating students. The central objective is to contribute to closing the existing gap in access to essential digital security knowledge, thus promoting a more equitable and inclusive educational environment for all students, regardless of their geographical location.

KEYWORDS: Social engineering, Cybersecurity, Vulnerabilities, Digital culture, Cyber threats, Security awareness, Online risks, Protective practices, Simulated cyber attacks, User credentials, Digital exposure.

INTRODUCCIÒN

En un mundo cada vez más interconectado, la seguridad en línea se vuelve crucial, especialmente en entornos donde el acceso a la información y la comprensión de las amenazas cibernéticas pueden ser limitados. Este proyecto se enfoca en un experimento social realizado en una zona rural apartada de Colombia, Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo Magdalena, donde los estudiantes están expuestos a mayores riesgos cibernéticos por un nivel de cultura digital aún en desarrollo.

El propósito de este experimento es explorar las vulnerabilidades en la seguridad de los dispositivos móviles en un contexto rural, donde la conciencia sobre ciberseguridad y las prácticas de protección digital pueden ser menos comunes o estar subdesarrolladas. Los jóvenes, como usuarios activos de la tecnología, enfrentan riesgos significativos en un entorno donde la exposición a amenazas en línea podría tener consecuencias más graves debido al nivel de conocimiento limitado sobre ciberseguridad.

El experimento se diseñó meticulosamente para simular situaciones comunes de ataques cibernéticos en este entorno, incluyendo la creación de amenazas como aplicaciones maliciosas, la configuración de redes wifi-engañosas y el uso de tácticas de ingeniería social. Este enfoque permitió no solo evaluar las debilidades en la seguridad

digital, sino también comprender cómo los jóvenes reaccionan y se protegen en un entorno con un nivel de cultura digital menos accesible.

Con el análisis detallado de cada fase del experimento, se espera conocer las percepciones de seguridad, el nivel de exposición a riesgos cibernéticos y la efectividad de las prácticas de seguridad actuales en este contexto rural específico. Los resultados y conclusiones derivadas de este estudio ofrecen una visión valiosa sobre la importancia de la educación en ciberseguridad en entornos con menor acceso a la información digital, destacando la necesidad crítica de fortalecer la protección digital en comunidades rurales apartadas.

OBJETIVO GENERAL:

Evaluar los riesgos en el uso de las redes sociales a los que están expuestos los estudiantes de los grados 8° y 9º de la Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo Magdalena, sobre las vulnerabilidades en redes sociales y las trampas asociadas al uso de dispositivos en estas plataformas.

OBJETIVOS ESPECÍFICOS:

1. Determinar el nivel actual de conocimiento en los estudiantes de los grados 8° y 9º de la Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo Magdalena, sobre las vulnerabilidades en redes sociales.

2. Identificar por medio de una encuesta las principales amenazas y trampas a las que están expuestos los estudiantes en el entorno de las redes sociales.

3. Diseñar un experimento social para exponer a los estudiantes a situaciones simuladas de riesgo en redes sociales.

4. Evaluar el impacto del experimento en la percepción y el conocimiento de los estudiantes sobre las vulnerabilidades en redes sociales.

Pregunta problema:

¿Cómo a partir del uso de herramientas y metodologías se pude llegar minimizar los riesgos o vulnerabilidades en los dispositivos móviles de los estudiantes de la Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo del Magdalena?

ESTADO DEL ARTE

La seguridad en línea es una cuestión de creciente importancia en la sociedad contemporánea, y los adolescentes, en particular, enfrentan riesgos significativos en el ciberespacio. Esta revisión del estado del arte se centra en la vulnerabilidad de los

adolescentes en línea y la utilización de experimentos de ingeniería social como un enfoque de investigación para abordar estas vulnerabilidades. El estudio se desarrolla en el contexto del Colegio Sagrado Corazón de Jesús, en Mompox, Bolívar, con Vulnerabilidad de los Adolescentes en Línea.

Numerosos estudios han documentado la vulnerabilidad de los adolescentes en línea. La literatura destaca que los adolescentes a menudo carecen de la experiencia y la conciencia necesaria para lidiar con las amenazas cibernéticas, lo que los hace susceptibles a diversas formas de ataques. Estos riesgos incluyen el ciberacoso, la exposición a contenido inapropiado, el robo de identidad y la comunicación con desconocidos en línea. (https://www.unicef.org/, 2022)

Experimentos de Ingeniería Social en Investigación Previas**.** Varios estudios han aplicado experimentos de ingeniería social para evaluar la ciberseguridad, aunque la mayoría se ha centrado en adultos. Estas investigaciones han demostrado la efectividad de las tácticas de ingeniería social utilizadas por los ciberdelincuentes y la susceptibilidad de las personas a caer en trampas en línea Sin embargo, se ha prestado una atención limitada. (INCIBE (INCIBE), 2019)

Educación en Seguridad en Línea para Adolescentes**:** La educación en seguridad en línea es una estrategia prometedora para abordar la vulnerabilidad de los adolescentes. Programas de concienciación en seguridad en línea han demostrado mejorar la conciencia y las prácticas de seguridad entre los adolescentes (Francisco Labrador Encinas, 2015)

La vulnerabilidad de los adolescentes en la investigación y en la práctica clínica: “Los adolescentes son considerados como grupo vulnerable y expuesto a diferentes amenazas en el ámbito de la salud, por lo cual es necesario que exista un debate sobre los aspectos éticos relacionados con su participación en la investigación y en la práctica clínica. Por medio de una revisión integradora de la literatura, se seleccionaron estudios que abordaban aspectos bioéticos relacionados con la vulnerabilidad de los adolescentes en los últimos quince años. Después del análisis de los estudios seleccionados, se verificó que no es posible llegar a un consenso válido para todas las situaciones que involucran adolescentes en la investigación y en la práctica clínica. Palabras clave: Vulnerabilidad. Adolescencia. Bioética”. (de Oliveira Santos, y otros, 2017)

En TIC Confío es el programa del Ministerio TIC que promueve el uso seguro y responsable de las TIC entre niños, niñas, adolescentes, padres, madres y cuidadores. Durante 2019, esta iniciativa sensibilizó a más de 800.000 personas y para el 2020 se espera llegar a un millón de beneficiarios. Encuentre más información y recomendaciones sobre el uso seguro de las TIC en ((TIC´s, 2021).

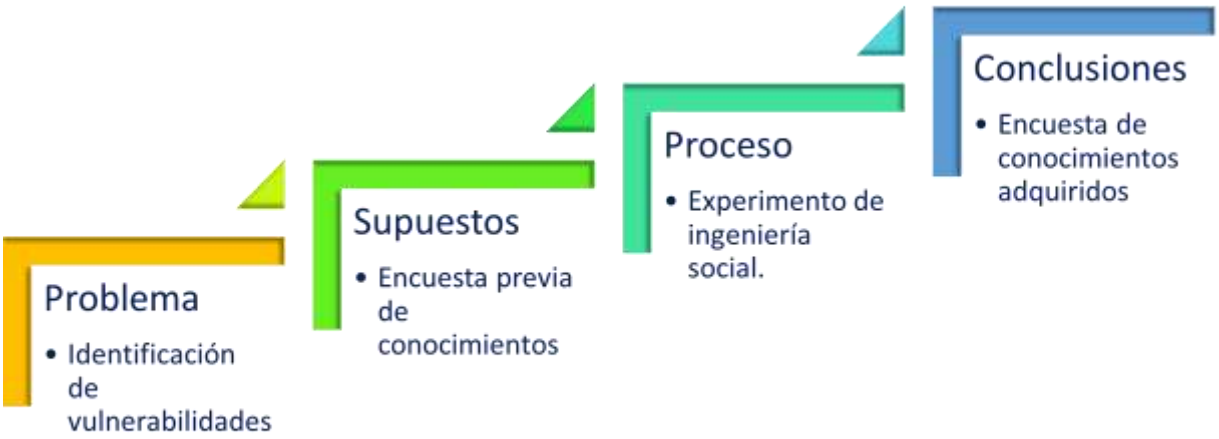
Esta investigación se sustenta en el diseño e implementación de una experiencia de innovación educativa en la cual hemos trabajado con menores en riesgo de exclusión social, sus educadores y referentes educativos y familiares. Todo ello llevado a cabo

desde el anonimizado, desde el cual se lucha contra la pobreza infantil a través de diferentes subprogramas y, entre ellos, el de refuerzo educativo, un subprograma en el que se ha desarrollado la experiencia de uso de aplicaciones y tecnología móvil que pasamos a describir. (Gil Oliver & Prendes espinosa, 2019).

Gestión del riesgo y evaluación de impacto en tratamientos de datos personales: El presente documento es una guía para la gestión de riesgos para los derechos y libertades de los interesados aplicable a cualquier tratamiento, independientemente de su nivel de riesgo. Además, y para los casos de tratamientos de alto riesgo, incorpora las orientaciones necesarias para realizar la Evaluación de Impacto para la Protección de Datos (EIPD) (Datos, 2021):

METODOLOGIA

Con la aplicación de una encuesta en línea, se establecen objetivos como identificar el nivel de conciencia de seguridad en línea, evaluar las prácticas de seguridad en línea, conceptos básicos de ciberseguridad, mediante el análisis cuantitativo de la información recopilada, se puede evidenciar que los estudiantes tienen un conocimiento básico y carecen de comprensión sobre las amenazas, no poseen conocimientos claros y precisos de los temas de seguridad y ciberseguridad, ni son conscientes de los peligros a los que se exponen al compartir información personal, ubicación, estados de ánimo, relaciones de pareja, imágenes o fotografías.



A través del análisis cuantitativo, determinamos las áreas específicas en las cuales centramos nuestro experimento social, identificamos en qué medida comprenden los estudiantes de los grados 8º Y 9º las vulnerabilidades en las redes sociales, esto nos permitió generar una actividad de concientización que nos ayudó a reforzar los conocimientos para que dichos estudiantes puedan identificar los peligros a los que

están expuestos y su vez establecer buenas prácticas de seguridad al momento de compartir información y dejarla pública.

El experimento realizado comprende la ejecución y distribución de una amenaza informática con el objetivo de obtener de forma ilegal las credenciales de los usuarios. A continuación, se detallan las etapas del procedimiento:

1. Creación de una APK maliciosa en Kali Linux: Diseñada para dispositivos Android, esta aplicación tenía la intención de acceder a diversos servicios del dispositivo móvil, incluyendo mensajes de texto, contactos, historial de llamadas, control de notificaciones, cámaras, entre otros, con propósitos no autorizados.
2. Configuración de una red wifi trampa: Con el fin de proporcionar acceso gratuito a internet, se estableció una red wifi diseñada para atraer a los usuarios.
3. Web spoofing a la página de la billetera virtual Nequi: Un proveedor de servicios financieros, donde se llevó a cabo la suplantación de la página con el propósito de engañar a los usuarios y obtener sus credenciales.
4. Desarrollo de una base de datos en Microsoft SQL Server: Se creó para almacenar las credenciales proporcionadas por los usuarios en el formulario de inicio de sesión de Nequi.
5. Envío de un mensaje de texto con una URL acortada: Solicitando la actualización de las credenciales de Nequi. Este enlace redirigió a los usuarios a la página falsa donde se capturaron las credenciales de la cuenta. Posteriormente, se re direccionó al usuario a la página legítima.
6. Realización de una transacción desde la plataforma PSE: Utilizando los datos de la cuenta "Nequi" de la víctima hacia la cuenta del atacante en "Daviplata". Además, a través de la APK, se interceptó y obtuvo el código de seguridad enviado por SMS al número registrado.

Este proceso describe de forma detallada cada una de las fases del experimento, mostrando la secuencia y el desarrolló para obtener las credenciales de los usuarios de manera ilícita.

> Utilizando la herramienta MSFVenom en Kali Linux, se generó una APK maliciosa, La APK maliciosa se envió mediante un mensaje vía WhatsApp a un dispositivo móvil con sistema operativo Android, utilizando el mensaje "actualizacion.apk para la billetera digital Nequi".

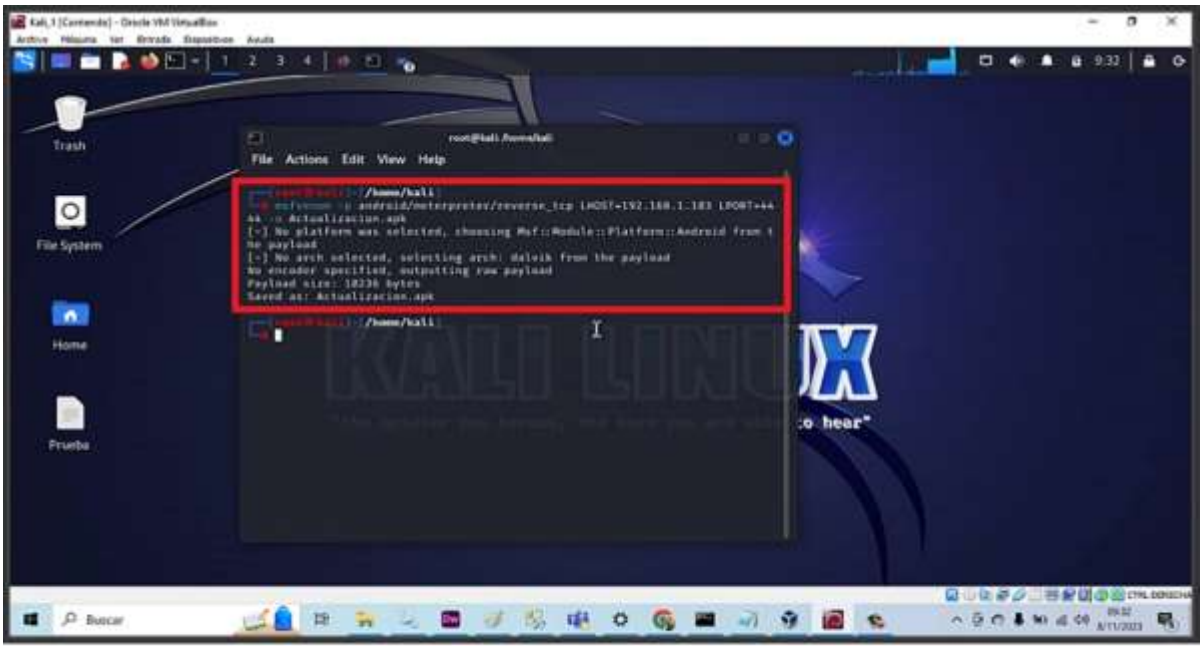


Imagen 1. Creación APK

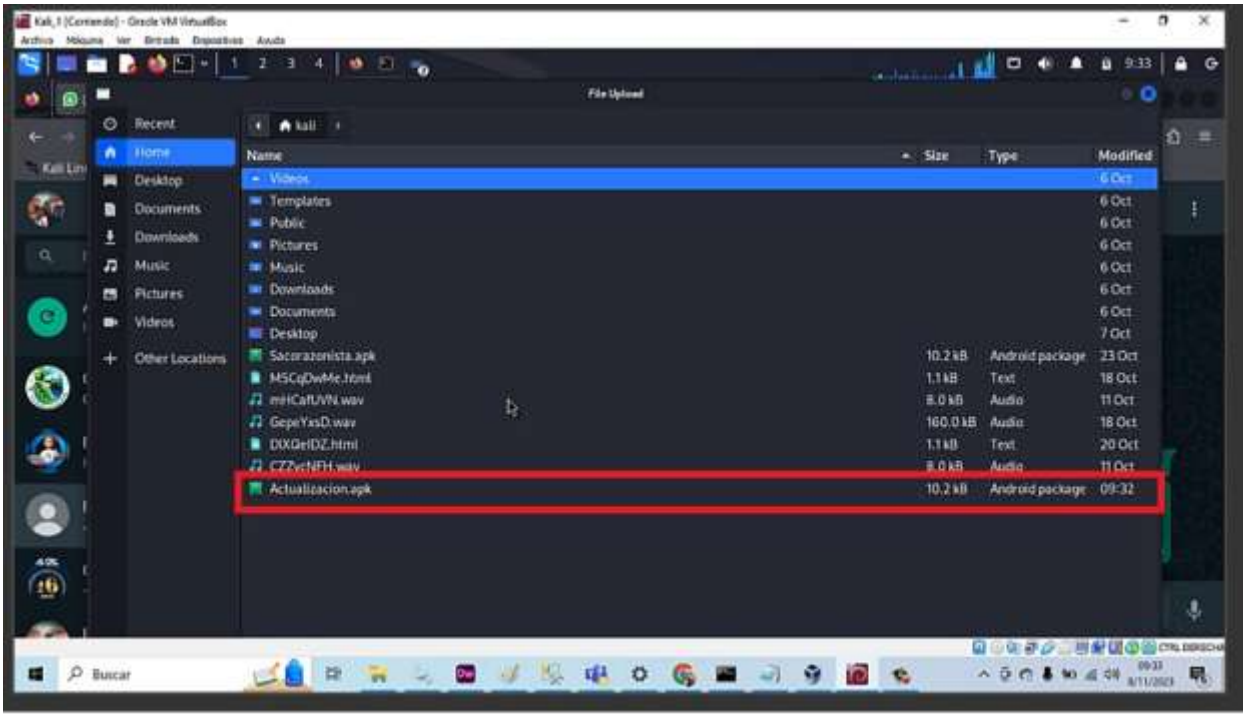


Imagen 2. Generación código malicioso

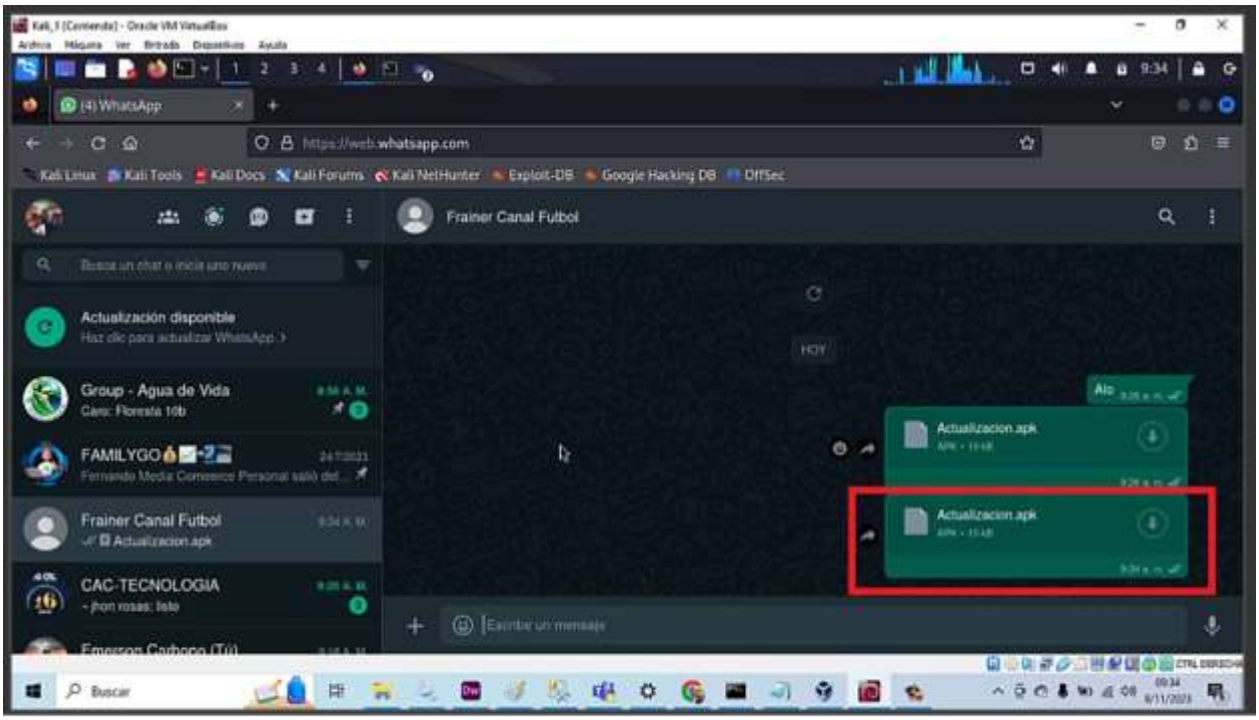


Imagen 3. Envío código malicioso

Una vez que la víctima recibió la aplicación maliciosa y seleccionó el enlace enviado, se desarrolló una conexión entre el dispositivo móvil de la víctima y el servidor remoto.

Utilizando Meterpreter, logramos acceso remoto al sistema confirmado después de haber vulnerado el dispositivo móvil de la víctima. Esta herramienta nos permitió la ejecución de comandos, la manipulación del sistema de archivos, la visualización de mensajes de texto, el control del servicio de llamadas y el acceso interactivo a las funciones del móvil comprometido.

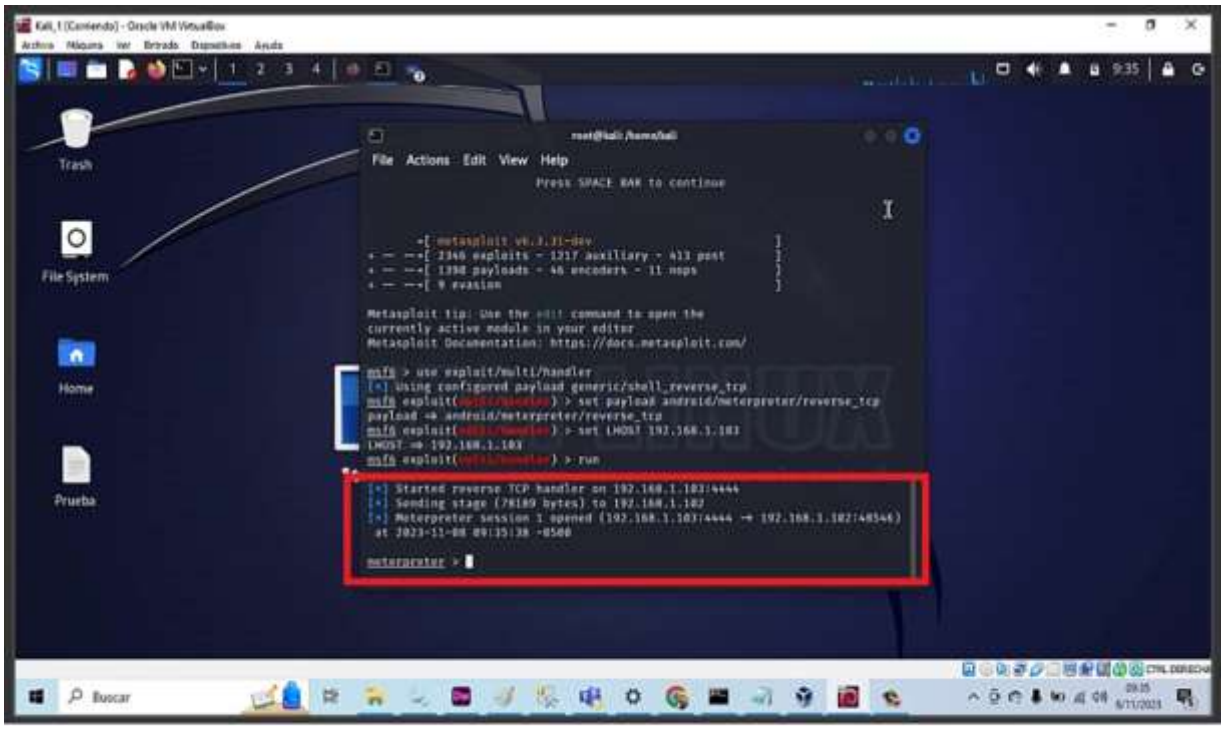


Imagen 4. Utilizando Meterpreter

Se configuró es una red LAN inalámbrica en un entorno controlado con el objetivo de engañar a los usuarios para que se conecten a ella, ofreciendo la ilusión de acceso gratuito a internet.

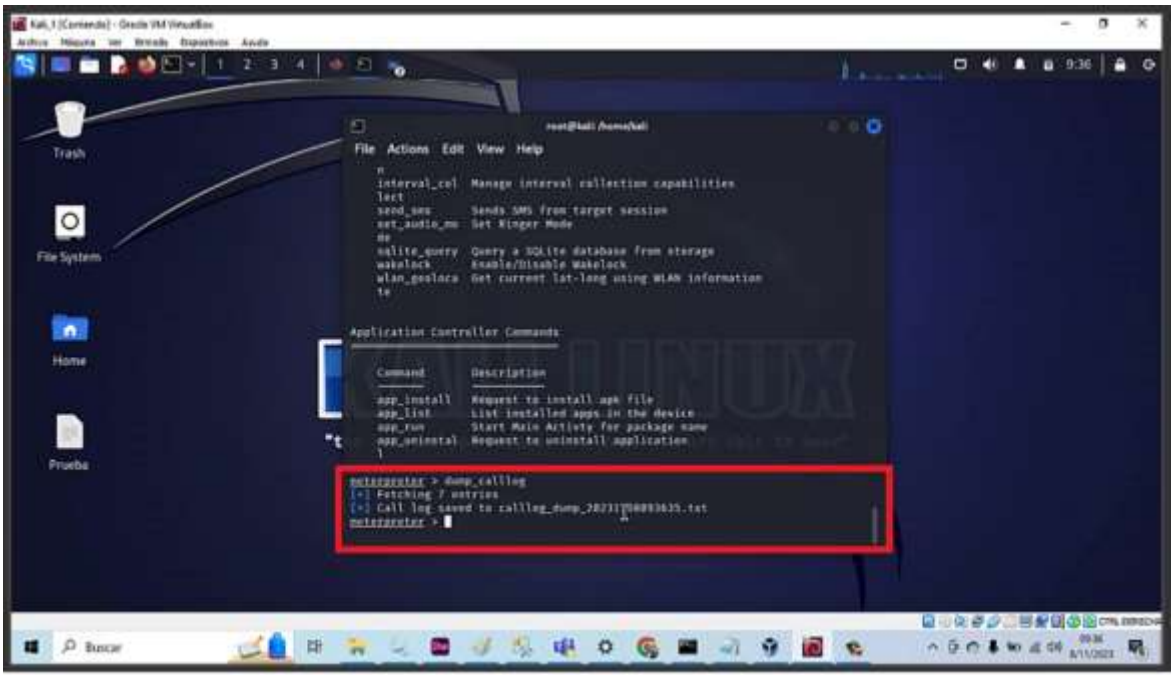


Imagen 5. Accediendo al registro de llamadas de la victima

Una vez se ingresa al dispositivo móvil tenemos acceso a los registros de llamadas.

Realizamos un Web spoofing a la billetera virtual Nequi en la cual se suplanto la página de inicio de sesión, para lograr así capturar los datos personales como el usuario, número de cedula y la calve de ingreso.

Página suplantada:

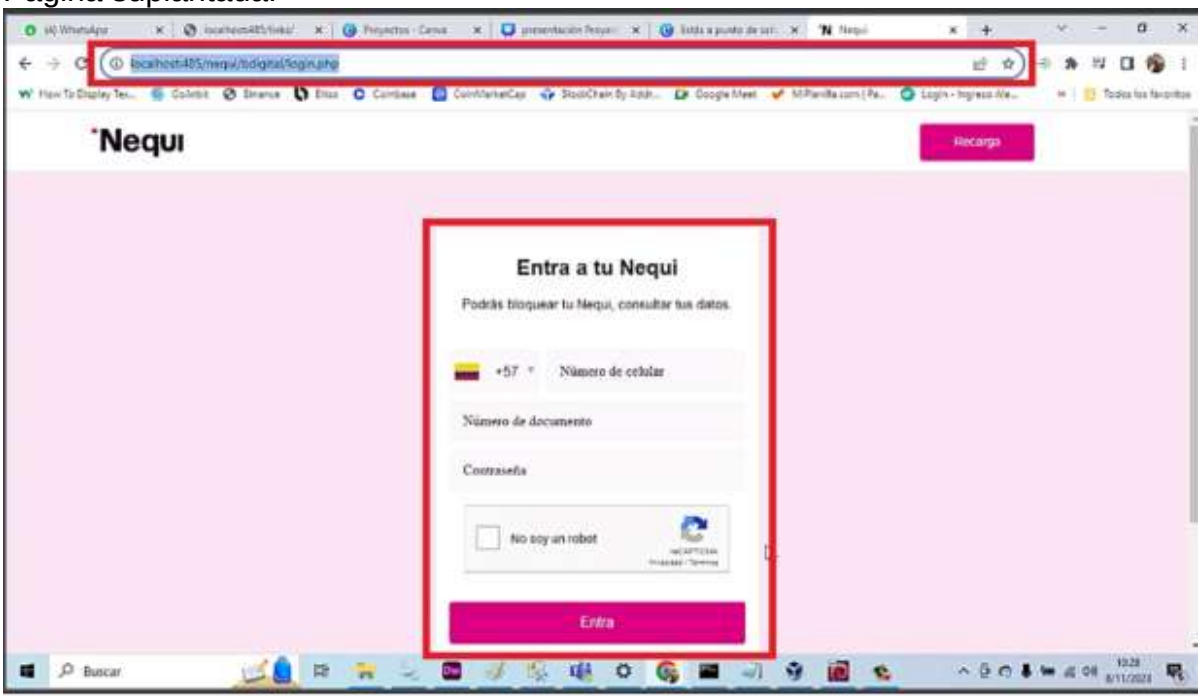


Imagen 6. Web spoofing a Nequi

Página oficial de Nequi:

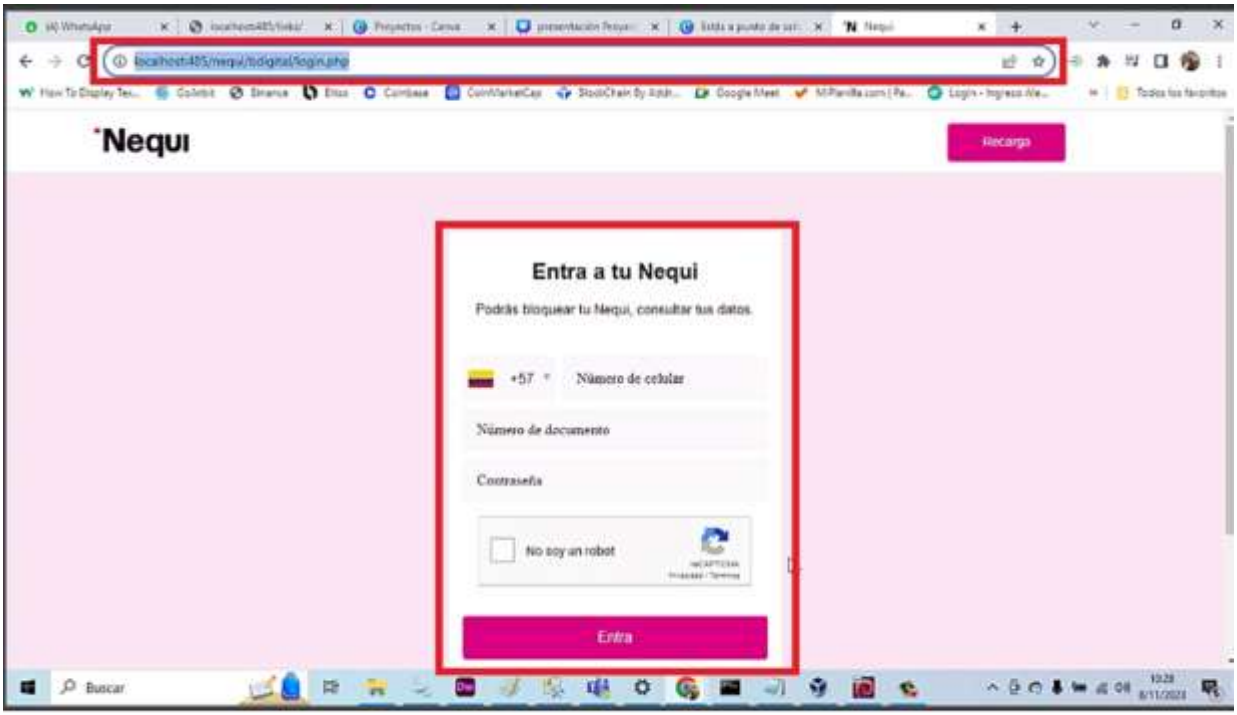
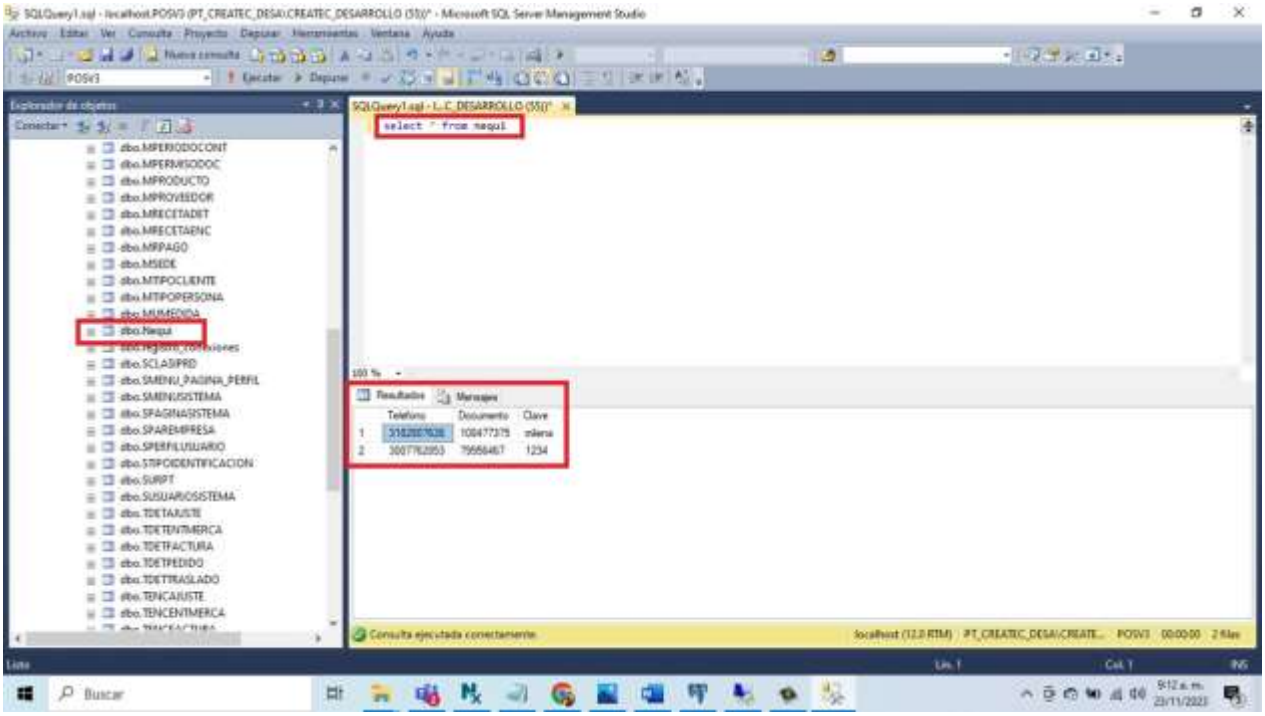


Imagen 6. Web spoofing a Nequi

Una vez la victima está conectada a red trampa creada, e ingresa a la página suplantada de la billetera virtual Nequi y digita la información solicitada, numero de celular, documento y contraseña, se realiza la captura de la información.



Luego de obtener las credenciales de la víctima, y el control sobre el dispositivo móvil, se procede a realizar una transacción en la billetera virtual de Nequi, con la finalidad de tomar recursos económicos y transferirlos al atacante.

Análisis de la encuesta previa de conocimientos

La seguridad en línea es un aspecto fundamental para el uso responsable y ético de las tecnologías de la información y la comunicación (TIC). Sin embargo, existen diversos riesgos y amenazas que pueden afectar la privacidad, la integridad y la reputación de los estudiantes al navegar por Internet. Algunos de estos riesgos son la ingeniería social, el phishing, la suplantación de identidad, el ciberacoso y el spam. Estos términos se refieren a diferentes formas de manipulación, engaño, acoso o envío de mensajes no solicitados que buscan obtener información personal, acceso a sistemas, beneficios económicos o causar daño a las víctimas.

La encuesta previa de conocimientos consta de 12 preguntas de opción múltiple con una sola respuesta correcta, que abordan los siguientes temas:

Qué es la ingeniería social y cómo se puede evitar.
Qué es el phishing y cómo se puede identificar.
Qué es la suplantación de identidad y cómo se puede prevenir.

Qué es el ciberacoso y cómo se puede actuar ante él.
Qué es el spam y cómo se puede filtrar.

La encuesta tuvo una duración aproximada de 15 minutos y se realizó de forma voluntaria. Los resultados de la encuesta se utilizarán para indagar acerca de los conocimientos previos al experimento de ingeniería social y seguridad en línea dirigido a los estudiantes de la escuela, con el fin de mejorar sus competencias digitales y ciudadanas. La participación en la encuesta implica la aceptación de estas condiciones y el consentimiento informado de los estudiantes y sus padres o tutores.

Resultados:

Grafico 1. ¿Has oído hablar del término "ingeniería social" en el contexto de la seguridad en línea?

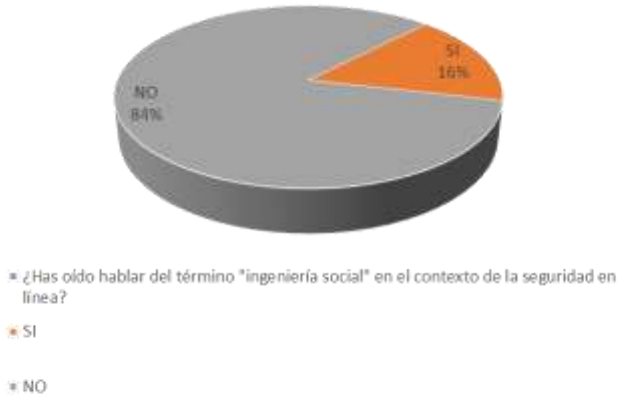


Grafico 1. encuesta previa de conocimientos .
Fuente propia

La mayoría de los estudiantes no están familiarizados con el concepto de ingeniería social en el ámbito de la seguridad cibernética. Esto se evidencia en la encuesta, donde el 84% de los participantes indicó no tener conocimiento sobre el término "ingeniería social" en el contexto de la seguridad en línea, revelando así una carencia generalizada de comprensión sobre este concepto entre los estudiantes.

Grafico 2.

Grafico 2. encuesta previa de conocimientos .
Fuente propia

Es posible concluir que el 42% de los estudiantes participantes asocian la "ingeniería social" con algo relacionado con la ingeniería de software sugiere una falta de conocimiento específico sobre el término en el contexto de la seguridad en línea. Esto indica una posible confusión o falta de familiaridad con el concepto preciso de ingeniería social.

La encuesta sugiere que hay diversidad en la comprensión del término "ingeniería social" entre los participantes, y podría ser ayuda para brindar una mayor claridad y educación sobre este concepto específico en el contexto de la seguridad en línea. La información resultante podría ser utilizada para adaptar futuras iniciativas de concienciación y formación en seguridad cibernética.

Grafico 3.

Grafico 3. encuesta previa de conocimientos .
Fuente propia

La mayoría de los estudiantes encuestados más del 50% no tiene hábitos de seguridad adecuados para proteger su información personal en línea. Esto puede exponerlos a riesgos como el robo de identidad, el fraude, el espionaje o el chantaje por parte de ciberdelincuentes que pueden acceder a sus datos personales, financieros, laborales o académicos. Según los resultados de la búsqueda web, el 64% de los usuarios de Internet ha experimentado algún tipo de ciberataque en el último año y el 85% de los usuarios de Internet considera que la protección de su información personal en línea es muy importante.

Grafico 4.

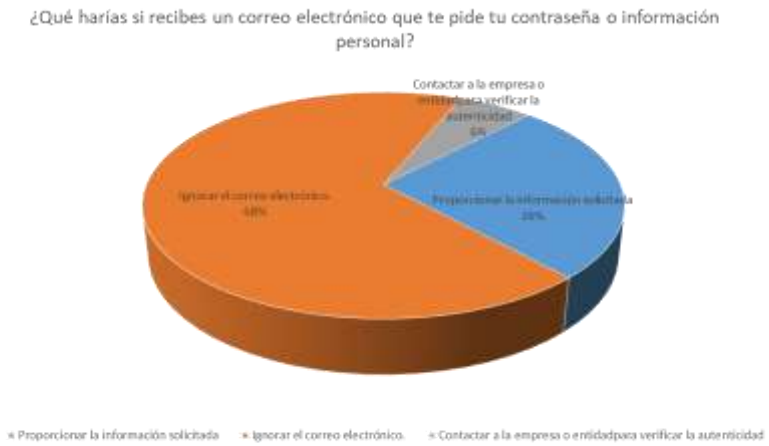


Grafico 4. encuesta previa de conocimientos .
Fuente propia

Los estudiantes desconocen cómo reaccionar adecuadamente ante un posible intento de phishing. El phishing es una técnica de ingeniería social que consiste en enviar correos electrónicos falsos que imitan la apariencia de empresas o entidades legítimas, con el fin de engañar a los usuarios para que proporcionen información confidencial, como contraseñas, datos bancarios o números de tarjetas de crédito.

Proporcionar la información solicitada es la peor opción que se puede tomar, ya que implica entregar voluntariamente los datos personales a los atacantes, que pueden usarlos para acceder a las cuentas, realizar compras fraudulentas, extorsionar o suplantar la identidad de las víctimas. Ignorar el correo electrónico es una opción mejor, pero no suficiente, ya que no impide que el atacante siga enviando más correos falsos o que intente engañar a otras personas. La mejor opción es contactar a la empresa o entidad para verificar la autenticidad del correo electrónico, ya que permite confirmar o descartar la veracidad del mensaje y alertar sobre el intento de phishing. Además, se debe reportar el correo electrónico como spam o phishing al proveedor de correo electrónico o a las autoridades competentes.

Grafico 5.

Grafico 5. encuesta previa de conocimientos
Fuente propia

El phishing no tiene nada que ver con el deporte acuático ni con el método para pescar en ríos, que se escriben con “f” en lugar de “ph”. Estas respuestas pueden indicar que los encuestados no conocen el origen del término, que proviene de la palabra inglesa “fishing” (pescar), pero con una alteración ortográfica que hace referencia a la palabra “phreaking” (piratear líneas telefónicas). El phishing se basa en la idea de lanzar un anzuelo (el correo electrónico falso) para atrapar a un pez (el usuario desprevenido).

Algunos encuestados confundieron el phishing con el deporte acuático o el método para pescar en ríos, lo que demuestra que no están familiarizados con este concepto ni con sus implicaciones para la seguridad en línea.

Grafico 6.

Grafico 6. encuesta previa de conocimientos .
Fuente propia

La mayoría de los estudiantes encuestados no tiene una definición clara o precisa de lo que es la suplantación de identidad en línea. La suplantación de identidad en línea es un tipo de fraude que consiste en usar una identidad falsa o robada para realizar acciones ilícitas o perjudiciales en Internet, como acceder a cuentas ajenas, obtener beneficios económicos, difamar, extorsionar o acosar a otras personas.

El hecho de que el 52% de los participantes asocie la suplantación de identidad con "hacerse pasar por otra persona en la vida real" sugiere una falta de precisión en la comprensión del concepto específico de la suplantación de identidad en línea. Esto indica que una parte significativa de los encuestados podría no tener una comprensión precisa de la naturaleza digital de este fenómeno.

Grafico 7.

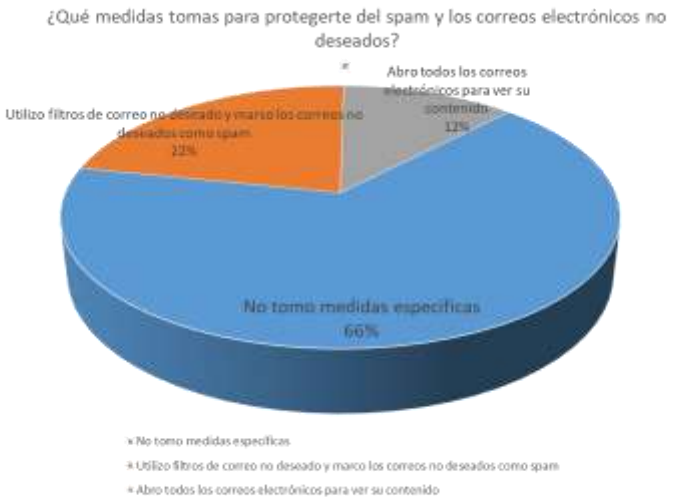


Grafico 7. encuesta previa de conocimientos .
Fuente propia

La respuesta más prevalente, en la cual el 66% de los estudiantes participantes señaló que no implementan medidas específicas para resguardarse del spam y los correos electrónicos no deseados, es motivo de preocupación. Este hallazgo sugiere una falta potencial de conciencia o acción preventiva por parte de los estudiantes en relación con este aspecto de la seguridad en línea. Es preocupante que una proporción considerable de los estudiantes no esté adoptando prácticas específicas para mitigar el riesgo asociado con la recepción de mensajes no deseados.

No obstante, no es menos relevante señalar que un pequeño porcentaje, el 12% de los estudiantes, manifestó abrir todos los correos electrónicos para revisar su contenido. Esta respuesta sugiere un enfoque menos precavido, lo cual expone al estudiante a un mayor riesgo de recibir contenidos no deseados o potencialmente maliciosos.

Análisis encuesta evaluación de conocimientos

Con este análisis determinamos las percepciones y niveles de comprensión alcanzados por los estudiantes de la Escuela Rural de Niñas en el corregimiento Isla del Rosario, del municipio de Pueblo Viejo, Magdalena, tras la implementación de un experimento social mediante una técnica de ingeniería social.

También confirmamos la adquisición y comprensión del concepto de ingeniería social, así como las implicaciones en seguridad y el desarrollo de la conciencia en seguridad cibernética. Mediante una cuidadosa evaluación de las respuestas recopiladas, este análisis nos permitió identificar áreas de mejora y señalar puntos específicos donde la educación en seguridad digital puede tener un impacto significativo.

Grafico 8.

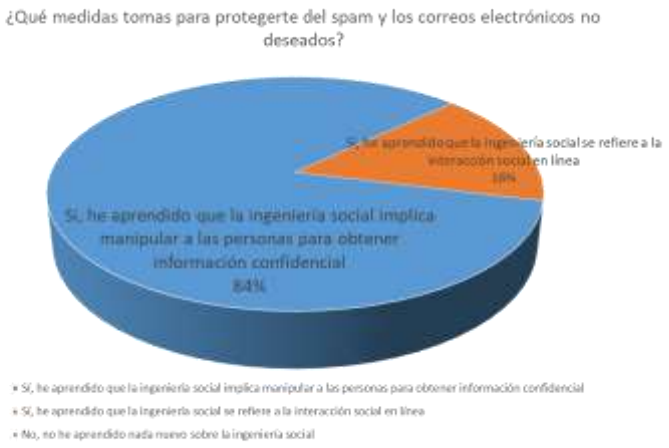


Grafico 8. encuesta previa de conocimientos .
Fuente propia

El 84.3% de los participantes expresaron que aprendieron el concepto ingeniería social; el cual manipula a las personas para obtener información confidencial. Esta respuesta refleja una comprensión clara de la naturaleza de la ingeniería social, subrayando su asociación con tácticas de manipulación con el propósito de obtener datos confidenciales.

En resumen, la mayoría de los estudiantes participantes demostraron una comprensión más clara de la ingeniería social en términos de manipulación para obtener información confidencial. Sin embargo, existe una minoría que interpreta la ingeniería social en el contexto de la interacción social en línea, lo que podría indicar la presencia

de diferentes perspectivas o interpretaciones del concepto. Este análisis puede orientar futuras técnicas educativas para abordar las diversas interpretaciones y mejorar la comprensión general del término.

Grafico 9.

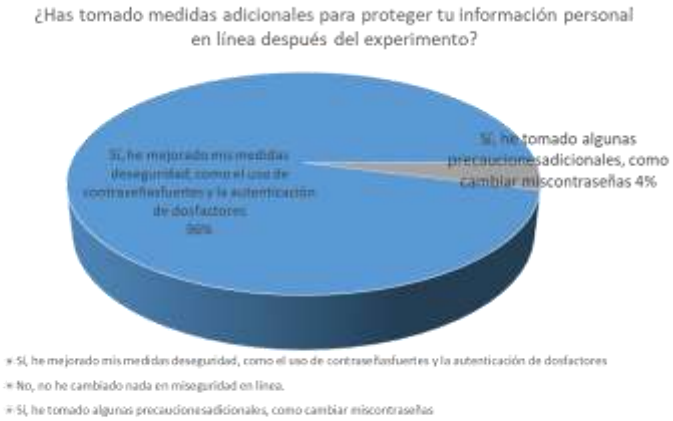


Grafico 9. encuesta previa de conocimientos .
Fuente propia

El 96% de los estudiantes exhibieron una mejora significativa en sus prácticas de seguridad en línea, lo que indica un impacto positivo derivado del experimento de ingeniería social en términos de conciencia y acciones relacionadas con la protección de la información personal. Esta conclusión respalda la eficacia del experimento al motivar cambios positivos en el comportamiento de seguridad en línea de los estudiantes, para fortalecer la protección de su información personal.

Grafico 10.

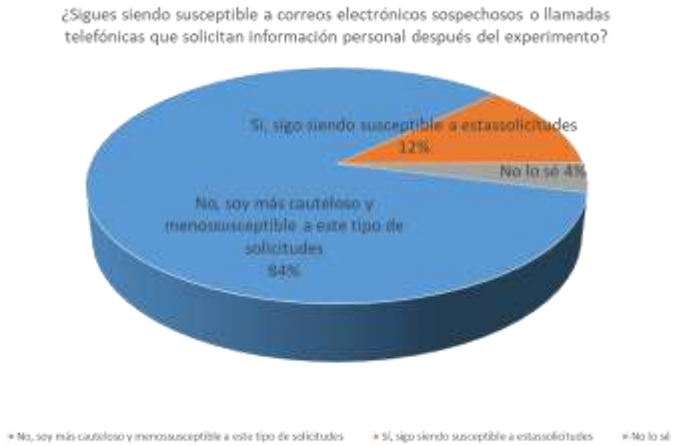


Grafico 10. encuesta evolución de conocimientos adquiridos .
Fuente propia

El 84% de los estudiantes participantes indicó que luego del experimento sobre técnicas de ingeniería social son más cautelosos y menos susceptibles a este tipo de solicitudes. Esta respuesta sugiere un cambio positivo, indicando que la experiencia ha tenido un impacto beneficioso en la actitud de los participantes hacia la protección de su información personal.

Aunque es una proporción menor, el 12% de los participantes afirmó seguir siendo susceptible a estas solicitudes lo que nos lleva a concluir que no ha experimentado una mejora significativa en su resistencia a este tipo de tácticas de ingeniería social

Grafico 11.

Grafico 11. encuesta evolución de conocimientos adquiridos .
Fuente propia

La mayoría de los participantes ha experimentado una mejora sustancial en su capacidad para identificar intentos de phishing después del experimento de ingeniaría social en el cual participaron activamente. La presencia de un grupo que ha mejorado moderadamente sugiere la posibilidad de ajustes específicos en la educación para abordar aspectos de mejora más específicas.

El 80% de los estudiantes señaló que luego del experimento de ingeniería social, ahora posee una mayor capacidad para reconocer intentos de phishing. Esta respuesta evidencia una mejora en la habilidad de los estudiantes para identificar y comprender posibles amenazas de phishing tras la realización de la actividad de ingeniería social. Constituye un indicador positivo de que el experimento ha tenido un impacto sustancial en el desarrollo de habilidades de detección.

Grafico 12.

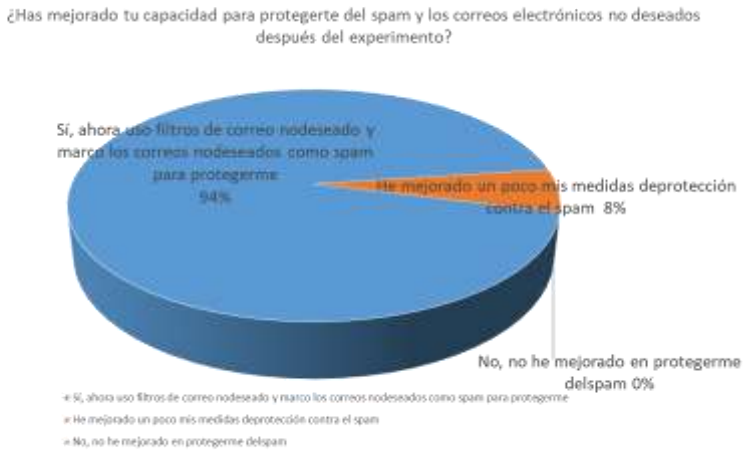


Grafico 12. encuesta evolución de conocimientos adquiridos .
Fuente propia

El 94% de los estudiantes participantes indicó que ahora utiliza filtros de correo no deseado y marcan los correos no deseados como spam para protegerse. Esta respuesta nos confirma que hubo una mejora en las medidas de protección contra el spam por parte de la gran mayoría de los estudiantes. La adopción de filtros y el etiquetado como spam son estrategias efectivas para gestionar correos no deseados.

El 6% de los participantes afirmó haber mejorado un poco sus medidas de protección contra el spam. Aunque es una proporción menor, indica que existe un grupo que ha experimentado cierta mejora, aunque posiblemente no tan pronunciada como la mayoría. Esto podría sugerir áreas específicas que podrían beneficiarse de un enfoque adicional en la educación sobre seguridad en línea.

Grafico 13.

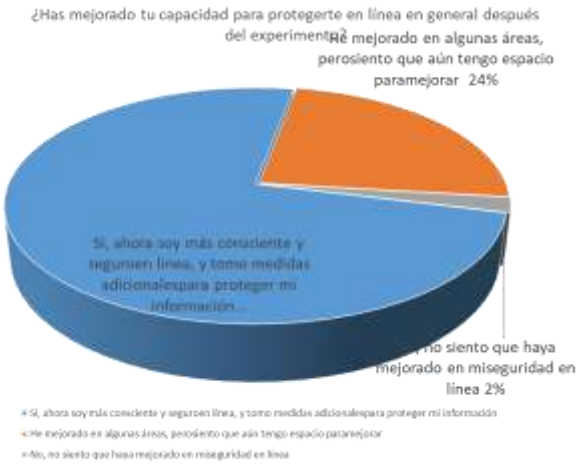


Grafico 13. encuesta evolución de conocimientos adquiridos .
Fuente propia

En resumen, la mayoría de los estudiantes participantes mostro una mejora significativa en su capacidad para protegerse en línea, al crear conciencia y adopción de medidas adicionales. Este progreso evidencia el crecimiento y la adquisición de conocimientos en buenas prácticas de ciberseguridad, reflejando una disposición general hacia la mejora continua.

Específicamente, el 74% de los estudiantes participantes indicó que ahora se siente más consciente y seguro en línea, implementando medidas adicionales para resguardar su información. Este resultado destaca de manera contundente el impacto positivo del experimento en el fortalecimiento de las prácticas de seguridad digital entre los estudiantes, subrayando su disposición proactiva hacia la protección de su información en línea.

A continuación, les compartimos evidencias fotográficas que documenta la ejecución del proyecto "Exponiendo Vulnerabilidades en la Red" con la participación de estudiantes de la Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo, Magdalena. Estas imágenes capturan momentos significativos y actividades clave, ofreciendo una visión más detallada del desarrollo de la iniciativa, destacando la participación activa y el compromiso de los estudiantes para adquirir y explorar conceptos relacionados con la ciberseguridad.

CONCLUSIONES

Las conclusiones derivadas del experimento social realizado en una zona rural de Colombia revelan una serie de hallazgos significativos en relación con la seguridad digital entre los jóvenes estudiantes. A lo largo del estudio, se exploraron las vulnerabilidades en la cultura digital, la exposición a riesgos cibernéticos y la efectividad de las estrategias de protección en entornos con menor acceso a la educación en ciberseguridad.

Los datos analizados confirman que los estudiantes adolescentes perciben tener un nivel adecuado de conocimiento y control sobre la tecnología que les rodea. Sin embargo, la realidad es distinta: sus conocimientos son insuficientes y, lo que es más preocupante, desconocen la magnitud de su vulnerabilidad especialmente en las regiones más apartadas de Colombia.

Al llevar a cabo un ejercicio práctico utilizando servicios de mensajería instantánea como SMS y WhatsApp, se observó que, de los 50 estudiantes participantes, 38 de ellos (más del 50%) abrieron el enlace malicioso, revelando una falsa percepción de seguridad, exponiéndolos a visitar sitios web suplantados que pueden contener malware.

Los estudiantes tienen dificultades para identificar mensajes falsos, lo que resulta en su ignorancia o caída en trampas preparadas por delincuentes. La falta de comprensión sobre la ingeniería social y sus métodos los convierte en blancos fáciles para los ciberdelincuentes. Este problema se evidencia claramente en la mensajería instantánea, a pesar de creer que pueden identificar y evitar trampas, más del 50% de los estudiantes abren enlaces sin cuestionar su autenticidad. Esto indica que, independientemente de su capacidad para identificarlas, caen en estas trampas, lo que podría generar problemas graves, tanto inmediatos como a largo plazo.

Este experimento de ingeniería social, llevado a cabo con estudiantes de una zona rural, arroja la conclusión de que los adolescentes, en efecto, cuentan con un conocimiento en seguridad informática por debajo de lo necesario, lo que los hace más vulnerables a ser hackeados con relativa facilidad. Los resultados y conclusiones obtenidas a través de este experimento proporcionan una perspectiva valiosa sobre la importancia de la educación en ciberseguridad en entornos con acceso limitado a la información digital, y se evidencia la necesidad crítica de implementar programas educativos en ciberseguridad en comunidades con menor acceso digital, buscando cerrar la brecha y fortalecer la conciencia de seguridad en línea.

Luego de participar en el ejercicio de ingeniería social los estudiantes de los grados 8 y 9 de la Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo Magdalena, que utilizan el Internet adquirieron conocimientos, habilidades y actitudes que les permitirán proteger su información y su identidad en línea, así como reconocer y denunciar las situaciones de abuso o violencia que puedan sufrir o presenciar.

Para abordar nuestra pregunta inicial sobre cómo reducir los riesgos y vulnerabilidades en los dispositivos móviles de los estudiantes de la Escuela Rural de Niñas en el corregimiento Isla del Rosario del municipio de Pueblo Viejo del Magdalena, hemos comparado los resultados más significativos de cada una de las preguntas formuladas como parte del experimento social. Este análisis nos permite evaluar el conocimiento real de los adolescentes y sus acciones al respecto.

Los resultados obtenidos resaltan la necesidad urgente de abordar la falta de comprensión en seguridad informática entre los adolescentes, así como la importancia de fomentar hábitos más seguros en el uso de dispositivos móviles, la educación en este aspecto resulta fundamental para protegerse de amenazas cibernéticas y evitar posibles riesgos a corto y largo plazo.

Los datos analizados confirman que los estudiantes perciben tener un nivel adecuado de conocimiento y control sobre la tecnología que les rodea. Sin embargo, la realidad es distinta: sus conocimientos son insuficientes y lo que es más preocupante, desconocen la magnitud de su vulnerabilidad, lo que los expone a diversos tipos de hackeos.

RECOMENDACIONES

Un tema crítico son las contraseñas. Aunque los adolescentes son conscientes de la importancia de tener contraseñas diferentes para cada aplicación, más del 70% utiliza la misma contraseña para varias cuentas o utiliza una variable. Esta práctica representa un peligro evidente: si una contraseña es comprometida, todas las cuentas quedan expuestas, abriendo la puerta a la falsificación de identidad o al robo de datos.

El mayor peligro radica en el uso del Wi-Fi. La falta de comprensión sobre su seguridad es alarmante: el 75% de los adolescentes se conecta a redes públicas sin verificar su fiabilidad. Esto no solo expone las cuentas, sino todos los datos del dispositivo conectado, incluyendo multimedia, información privada y datos bancarios. La utilización descuidada de esta opción para ahorrar datos o tener Wi-Fi gratuito podría tener consecuencias graves, ya que los dispositivos móviles almacenan cada vez más información personal importante.

Otro aspecto crítico es el desconocimiento general sobre los virus informáticos. Solo aquellos que han cursado asignaturas de informática poseen algún tipo de conocimiento sobre el tema. La mayoría de las personas carece de este conocimiento, lo que los deja vulnerables a hackeos sin ser conscientes de ello. La dependencia creciente de los antivirus priva a los adolescentes de la necesidad de aprender a defenderse por sí mismos. Además, el uso generalizado de antivirus gratuitos o de prueba no brinda una protección efectiva contra ataques.

Este estudio concluye que, efectivamente, los adolescentes poseen un conocimiento en seguridad informática por debajo de lo necesario, lo que los deja

vulnerables a hackeos con mayor facilidad. En un mundo cada vez más dependiente de la tecnología y donde almacenamos más información en dispositivos, es crucial adquirir conocimientos mínimos para protegersen de posibles ataques. Descuidar este tema puede llevar a consecuencias desastrosas para los afectados, transformando el pensamiento de "esto no me pasará" en "si hubiera sabido que esto podía pasar".

- Exposición a amenazas cibernéticas: La falta de conocimientos sobre ataques informáticos y la tendencia a compartir contraseñas comunes exponen a los jóvenes a diversos riesgos cibernéticos, incluyendo robo de identidad, fraudes financieros y pérdida de datos personales.

- Desafíos en la cultura digital: La disparidad en la adopción de la cultura digital en áreas rurales plantea desafíos significativos en la protección y comprensión de los riesgos asociados con el uso de la tecnología, requiriendo estrategias específicas para abordar estas brechas.

- Efectividad de la ingeniería social**:** El experimento demostró la efectividad de la ingeniería social al explotar la falta de conocimiento y conciencia de seguridad entre los jóvenes, lo que resalta la necesidad de crear estrategias proactivas para prevenir estos ataques.

- Importancia de la formación en seguridad: Los resultados resaltan la urgencia de implementar programas educativos integrales que enseñen habilidades prácticas en seguridad cibernética y promuevan la conciencia de los riesgos asociados con la actividad en línea.

- Concientización sobre prácticas seguras: Es fundamental fomentar una mayor conciencia sobre prácticas seguras en línea, incluyendo la importancia de utilizar contraseñas fuertes y únicas, verificar la autenticidad de los enlaces y comprender las señales de posibles amenazas cibernéticas.

- Rol de las comunidades en la protección digital: Existe una necesidad apremiante de involucrar a las comunidades rurales en la promoción de prácticas seguras en línea y la creación de un entorno que valore y priorice la seguridad cibernética.

Estas conclusiones refuerzan la importancia de abordar las brechas en la seguridad digital, especialmente en entornos rurales, y subrayan la necesidad de adoptar estrategias educativas y preventivas para proteger a los jóvenes frente a amenazas cibernéticas.

Las consecuencias de un ataque utilizando técnicas como el web spoofing, phishing y smishing pueden ser significativas y dañinas para los usuarios, como el robo de información personal al no verificar la legitimidad de las páginas web o mensajes, los usuarios están expuestos al riesgo de proporcionar información personal sensible, como contraseñas, números de tarjetas de crédito, y otra información confidencial a sitios

falsos controlados por atacantes. Los ataques pueden realizar transacciones no autorizadas, lo que resulta en pérdidas financieras para los usuarios.

Es fundamental que los usuarios sean conscientes de los riesgos mencionados y adopten medidas para resguardar su seguridad en línea. Esto incluye verificar la autenticidad de las páginas web, abstenerse de hacer clic en enlaces sospechosos y emplear prácticas de seguridad sólidas, tales como la autenticación de dos factores o biométrica, estas acciones son esenciales para resguardarse eficazmente contra las diversas amenazas cibernéticas que podrían comprometer la privacidad y seguridad en línea de los usuarios.

REFERENCIAS BIBLIOGRAFICAS

Datos, A. E. (10 de 06 de 2021). *https://www.aepd.es*. Obtenido de https://www.aepd.es: https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

de Oliveira Santos, D., Alves Gomes, ,., Raspante Teixeira, K., Roever, L., de Andrade Fuzissaki , M., Faleiros , T., & de Campos Lima, T. (2017). La vulnerabilidad de los adolescentes en la. *scielo*. Obtenido de https://www.scielo.br/j/bioet/a/hHJLcbGbrMSzn5K6rFM5y6q/?lang=es&format=pdf

Francisco Labrador Encinas, A. R. (22 de 03 de 2015). *https://www.ucm.es/*. Obtenido de https://www.ucm.es/.

Gil Oliver, J. M., & Prendes espinosa, M. (01 de 06 de 2019). *https://gredos.usal.es/*. Obtenido de https://gredos.usal.es/: https://gredos.usal.es/bitstream/handle/10366/142858/Uso_de_aplicaciones_y_dispositivos_movil.pdf;jsessionid=71FCA0A75D6D37E5F86889CF2E393F4F?sequence=1

https://www.unicef.org/. (2022). https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo. Obtenido de https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

INCIBE (INCIBE). (05 de 09 de 2019). *https://www.incibe.es*. Obtenido de https://www.incibe.es: https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

TIC´s, M. d. (01 de 03 de 2021). (M. d. TIC´s, Productor) Recuperado el 15 de 11 de 2023, de https://mintic.gov.co