Universidad Nacional de Ingeniería

Facultad de Ciencias

Carrera de Ciencias de la Computación

El Phishing en el Perú: Tendencias y Consecuencias como Principal Modalidad de Ciberataque en el Año 2023

Proyecto de Investigación para Tesis

Andrei Steven Trujillo Armas

20212147J

Asesor

Milussja Ivette Mejia Sanchez

Lima - Perú
2024

Resumen

Este estudio investiga las tendencias y consecuencias del phishing como la principal modalidad de ciberataque en el Perú durante el año 2023. Adoptando un enfoque mixto que integra métodos cuantitativos y cualitativos, el estudio se clasifica como exploratorio y descriptivo. La investigación explorará cómo el phishing ha proliferado como forma predominante de ciberataque en el contexto peruano, examinando tácticas utilizadas, vectores de ataque comunes y motivaciones detrás de estos actos. Además, se centrará en proporcionar una visión detallada de los impactos observados del phishing en diversos sectores y regiones del país. La metodología incluirá la recolección de datos a través de análisis de contenido de noticias, informes de incidentes de seguridad y entrevistas con expertos en ciberseguridad. Se espera que los resultados no solo mejoren la comprensión de los efectos del phishing en el entorno digital y económico del Perú, sino que también contribuyan al desarrollo de estrategias efectivas de mitigación y prevención.

Índice general

Capítulo 1

Planteamiento del problema

1.1. Descripción del problema

En la era digital actual, el phishing se ha consolidado como una de las modalidades de ciberataque más prevalentes y peligrosas, afectando tanto a individuos como a organizaciones en todo el mundo. En el contexto peruano, durante el año 2023, se ha observado un incremento significativo en la frecuencia y sofisticación de estos ataques, lo que pone en evidencia la necesidad urgente de estudiar sus tendencias y consecuencias.

El phishing, que consiste en la obtención fraudulenta de información confidencial mediante la suplantación de identidad, presenta un desafío significativo para la ciberseguridad. Los atacantes utilizan técnicas cada vez más avanzadas para engañar a los usuarios y obtener acceso a datos sensibles, como credenciales bancarias y personales. Este fenómeno no solo impacta económicamente a las víctimas, sino que también socava la confianza en los sistemas digitales y las transacciones en línea.

El problema radica en la rápida evolución de las tácticas de phishing y la falta de conocimiento adecuado entre los usuarios sobre cómo identificar y protegerse contra estos ataques. A pesar de los esfuerzos en educación y prevención, muchas personas y empresas siguen siendo vulnerables debido a la sofisticación de los métodos empleados por los cibercriminales. Esto subraya la importancia de realizar una investigación detallada que explore las tendencias actuales del phishing en el Perú, identificando las principales estrategias utilizadas y evaluando sus consecuencias a nivel social y económico.

Esta investigación se propone analizar las características específicas de los ataques de phishing en el Perú durante el año 2023, identificando patrones y métodos predominantes. Además, busca evaluar el impacto de estos ataques en la economía y la seguridad digital del país, proporcionando una base sólida para el desarrollo de estrategias de mitigación más efectivas. En última instancia, se aspira a contribuir al fortalecimiento de la ciberseguridad en el Perú, promoviendo una mayor conciencia y preparación frente a esta amenaza creciente.

1.2. Formulación del problema

Para abordar la problemática del phishing en el Perú en el año 2023 de manera efectiva, se plantean las siguientes preguntas:

1.2.1. Pregunta principal

¿Cuáles fueron las tendencias más destacadas del phishing como modalidad de ciberataque en el Perú durante el año 2023 y cuáles fueron sus impactos más significativos?

1.2.2. Preguntas específicas

¿Qué métodos y técnicas de phishing fueron más prevalentes y efectivos en el contexto peruano durante el año 2023?

¿Cuáles son los principales factores que contribuyen a la vulnerabilidad de los usuarios peruanos ante los ataques de phishing?

¿Qué medidas y estrategias de prevención y mitigación han resultado más eficaces para combatir el phishing en el contexto peruano?

1.3. Objetivos de estudio

Para delimitar nuestro trabajo de investigación y las expectativas que tenemos del mismo, se proponen los siguientes objetivos:

1.3.1. Objetivo general

Analizar las tendencias y consecuencias del phishing como principal modalidad de ciberataque en el Perú durante el año 2023, con el fin de identificar estrategias efectivas de prevención y mitigación.

1.3.2. Objetivos específicos

- Identificar los métodos y técnicas de phishing más prevalentes y efectivos utilizados en el Perú durante el año 2023.
- Evaluar los principales factores que contribuyen a la vulnerabilidad de los usuarios peruanos ante los ataques de phishing.
- Proponer mejoras en la concienciación y la educación de los usuarios peruanos para reducir la incidencia del phishing en el futuro.

1.4. Justificación

La presente investigación surge por el contexto de que en la era digital actual, el phishing se ha convertido en una amenaza significativa para la seguridad de la información, afectando tanto a individuos como a organizaciones. Este tipo de ciberataque no solo implica pérdidas económicas, sino también daños a la reputación y la confianza en los sistemas digitales.

La importancia de esta investigación radica en la necesidad de entender cómo evolucionan las técnicas de phishing y cuál es su impacto específico en el contexto peruano. Dada la creciente sofisticación de estos ataques, es crucial identificar los métodos más utilizados y las razones por las cuales los usuarios siguen siendo vulnerables. Este conocimiento permitirá diseñar estrategias de prevención y mitigación más efectivas, adaptadas a las particularidades del entorno digital en Perú.

Además, la investigación tiene relevancia práctica, ya que proporcionará información valiosa para la elaboración de políticas públicas y programas de concienciación que puedan reducir la incidencia del phishing. Al analizar los impactos económicos y sociales del phishing, se podrán cuantificar las pérdidas y entender mejor cómo este tipo de ciberataque afecta a la economía y la seguridad nacional.

Este estudio contribuirá también al campo académico al ofrecer un análisis detallado de un problema contemporáneo y de rápida evolución. Los hallazgos podrán servir de base para futuras investigaciones y el desarrollo de tecnologías más avanzadas en ciberseguridad. En última instancia, mejorar la comprensión y la respuesta al phishing tendrá implicaciones positivas para la seguridad digital, la confianza en las transacciones en línea y la protección de datos personales en el Perú.

Capítulo 2

Marco Teórico

2.1. Antecedentes

El phishing ha emergido como una de las modalidades más prevalentes y sofisticadas de ciberataque a nivel global, y Perú no es una excepción. Este tipo de ataque, que busca engañar a las víctimas para que revelen información confidencial, ha evolucionado significativamente, aprovechando tanto las vulnerabilidades tecnológicas como las humanas. Durante 2023, el incremento en los ataques de phishing en Perú ha suscitado un interés creciente en la comunidad de seguridad informática y en las autoridades gubernamentales, dado su impacto en la seguridad financiera y personal de los ciudadanos.

2.1.1. Contexto tecnológico y social

En el contexto tecnológico, estudios previos han demostrado cómo los cibercriminales han adaptado sus tácticas para explotar las tecnologías emergentes y las plataformas digitales. La investigación de McAfee (2020) destaca cómo la sofisticación de los ataques de phishing ha aumentado, empleando técnicas como el spear-phishing y el uso de inteligencia artificial para crear mensajes más convincentes y dirigidos.

Desde una perspectiva social, el trabajo de Jakobsson y Myers (2007) proporciona una comprensión profunda de cómo las técnicas de ingeniería social son cruciales para el éxito del phishing. Estos ataques no solo explotan las fallas tecnológicas, sino también las vulnerabilidades psicológicas humanas, como la confianza y la curiosidad. En Perú, el creciente acceso a Internet y la digitalización de servicios bancarios y gubernamentales han ampliado la superficie de ataque para los ciberdelincuentes.

2.1.2. Relevancia para la Investigación

Investigaciones recientes, como las realizadas por el equipo de FireEye (2021), han explorado la relación entre el aumento de los ataques de phishing y la pandemia de COVID-19. Este estudio resalta la importancia de la adaptación cultural y lingüística en las tácticas de phishing, subrayando la necesidad de enfoques específicos para diferentes regiones. En el contexto peruano, la investigación de Kaspersky (2022) destaca un aumento significativo en los ataques de phishing dirigidos a usuarios de servicios financieros y gubernamentales, lo que pone de relieve la necesidad de estudios más profundos en esta área.

2.2. Diseño teórico

El presente estudio se basa en un conjunto integral de bases teóricas que abordan aspectos clave relacionados con el phishing como modalidad de ciberataque. Estas bases teóricas proporcionan una estructura conceptual sólida y permiten una comprensión profunda del problema planteado.

2.2.1. Teoría del phishing

La teoría del phishing se fundamenta en la comprensión de las tácticas y técnicas utilizadas por los cibercriminales para engañar a sus víctimas. Esta teoría se ha desarrollado significativamente en el campo de la ciberseguridad, especialmente en el análisis de los métodos de ataque y las contramedidas efectivas. Sus principios fundamentales son los siguientes:

- Ingeniería social: El phishing se basa en la manipulación psicológica para obtener información confidencial. La teoría explora cómo los atacantes utilizan técnicas de persuasión y engaño para ganarse la confianza de las víctimas.
- Evolución de las técnicas: La teoría aborda cómo las tácticas de phishing han evolucionado, desde correos electrónicos masivos hasta ataques más dirigidos y personalizados, conocidos como spear-phishing.
- Impacto en la seguridad: La teoría examina las consecuencias de los ataques de phishing en la seguridad personal y organizacional, incluyendo la pérdida de datos sensibles y el daño a la reputación.
- Contramedidas y prevención: La teoría también abarca las estrategias de defensa, como la educación y concienciación de los usuarios, así como el uso de tecnologías de detección y prevención.

2.2.2. Teoría de la Ingeniería Social

La ingeniería social es una disciplina que combina conocimientos de psicología y ciberseguridad para comprender cómo los atacantes explotan las debilidades humanas. Sus principios fundamentales incluyen:

- Manipulación y persuasión: Los atacantes utilizan técnicas psicológicas para influir en el comportamiento de las víctimas, como el uso de la urgencia y la autoridad.
- Tácticas de engaño: La teoría explora cómo los atacantes crean escenarios convincentes para obtener información confidencial, desde correos electrónicos falsos hasta llamadas telefónicas fraudulentas.
- Defensas humanas: La teoría también se centra en cómo las personas pueden ser entrenadas para reconocer y resistir las tácticas de ingeniería social, destacando la importancia de la educación y la concienciación en ciberseguridad.

2.2.3. Teoría de ciberseguridad

La teoría de ciberseguridad se enfoca en la protección de sistemas de información contra amenazas y ataques. Sus principios fundamentales incluyen:

- Identificación y gestión de riesgos: La teoría aborda cómo identificar y evaluar las amenazas, como el phishing, y cómo implementar medidas de mitigación adecuadas.
- Tecnologías de defensa: La teoría examina las diversas tecnologías utilizadas para prevenir y detectar ataques de phishing, como los filtros de correo electrónico y las soluciones de autenticación multifactor.
- Estrategias de respuesta: La teoría también incluye el desarrollo de estrategias para responder a incidentes de seguridad, minimizando el impacto y recuperando la integridad del sistema.

2.3. Definición de términos

A continuación, se presentan las definiciones de los términos clave utilizados en el marco teórico y la investigación, con el objetivo de proporcionar una comprensión clara de los conceptos fundamentales involucrados en el estudio del phishing como principal modalidad de ciberataque en Perú en 2023:

- Phishing: Proceso de engañar a las víctimas para que revelen información confidencial, como contraseñas y números de tarjetas de crédito, a través de mensajes fraudulentos que parecen legítimos.
- Ingeniería social: Técnica utilizada por los atacantes para manipular psicológicamente a las víctimas y obtener información o acceso a sistemas.
- Spear-phishing: Tipo de phishing dirigido a individuos específicos, utilizando información personalizada para aumentar la efectividad del ataque.
- Ciberseguridad: Conjunto de prácticas y tecnologías diseñadas para proteger sistemas de información y datos contra ataques y accesos no autorizados.
- Autenticación multifactor: Método de seguridad que requiere dos o más formas de verificación para acceder a un sistema, aumentando la protección contra

ataques de phishing.

- Educación y concienciación: Estrategias utilizadas para informar y entrenar a los usuarios sobre las amenazas de seguridad y cómo protegerse contra ellas.
- Tecnologías de detección y prevención: Herramientas y soluciones tecnológicas utilizadas para identificar y bloquear intentos de phishing antes de que lleguen a las víctimas.

Capítulo 3

Diseño de la Investigación

3.1. Tipo de investigación

La presente investigación se enmarca en un enfoque aplicado, dirigido a entender y mitigar los impactos del phishing como forma prevalente de ciberataque en el contexto peruano durante el año 2023. Este enfoque aplicado se centra en desarrollar estrategias efectivas para la prevención y respuesta ante esta amenaza digital emergente, con el propósito de fortalecer las defensas cibernéticas a nivel institucional y comunitario.

- **Según su diseño:** La investigación adopta un diseño predominantemente no experimental, dado que no implica la manipulación deliberada de variables ni la alteración de condiciones de vida de los individuos. En lugar de ello, se basa en el análisis de datos recopilados sobre casos reales de phishing en el Perú durante 2023, así como en estudios de caso y entrevistas con expertos en ciberseguridad. Este enfoque permite una comprensión profunda de las dinámicas y repercusiones del phishing en el contexto local.
- **Según su enfoque:** La metodología empleada es principalmente cualitativa, enfocada en la comprensión detallada de las técnicas de ataque utilizadas por los ciberdelincuentes, así como en las respuestas organizacionales y gubernamentales frente a estas amenazas. Se emplearán análisis de contenido y técnicas de codificación para identificar patrones comunes de phishing y evaluar la efectividad de las medidas preventivas implementadas. Este enfoque cualitativo se complementa con elementos cuantitativos para proporcionar un panorama completo de la incidencia y prevalencia del phishing en el país.
- **Según su fuente de datos:** La investigación se basa en una combinación de fuentes primarias y secundarias. Se recopilarán datos directamente de informes de incidentes de seguridad, registros de ataques y bases de datos de instituciones relevantes en el ámbito de la ciberseguridad peruana. Además, se realizarán entrevistas estructuradas con profesionales y funcionarios involucrados en la gestión de incidentes cibernéticos para obtener perspectivas expertas

sobre las tendencias y las estrategias de defensa.

- **Según su alcance:** El alcance de la investigación es exploratorio y descriptivo, buscando proporcionar una comprensión detallada y holística de cómo el phishing ha evolucionado como una modalidad de ciberataque predominante en el Perú durante el año 2023. Este enfoque permitirá identificar no solo las técnicas específicas utilizadas por los atacantes, sino también las consecuencias operativas, financieras y reputacionales para las organizaciones y los individuos afectados.
- **Según su propósito:** El propósito de la investigación es principalmente explicativo, ya que busca no solo documentar y describir los incidentes de phishing, sino también comprender las causas subyacentes de su proliferación y evaluar críticamente las respuestas existentes. Este enfoque explicativo es fundamental para proponer recomendaciones prácticas y políticas efectivas que fortalezcan la resiliencia cibernética del Perú frente a esta amenaza en evolución.

  Este esquema proporciona una estructura clara y detallada del tipo de investigación que se está llevando a cabo, centrada en el análisis y la respuesta frente al phishing como modalidad principal de ciberataque en el Perú durante el año 2023.

3.2. Diseño de investigación

Este estudio empleará un enfoque mixto que combina elementos cuantitativos y cualitativos para investigar las tendencias y consecuencias del phishing como la principal forma de ciberataque en el Perú en 2023. En terminos de la investigación aplicada, se caracteriza por ser exploratoria y descriptiva: explorará las tácticas y motivaciones del phishing en el contexto peruano, mientras describe detalladamente sus efectos en diversos sectores y regiones del país. Este diseño permitirá una comprensión amplia y profunda del fenómeno, capturando las perspectivas de víctimas, expertos en ciberseguridad y responsables de políticas públicas, con el objetivo de informar estrategias efectivas de mitigación.

3.3. Método de investigación

Se realizará una recopilación exhaustiva de datos a partir de fuentes primarias y secundarias. Las fuentes primarias incluirán reportes de incidentes de seguridad cibernética proporcionados por entidades gubernamentales, empresas afectadas y organizaciones de seguridad. Las fuentes secundarias comprenderán estudios y análisis previos sobre ciberseguridad en el contexto peruano.

Posteriormente se aplicarán técnicas estadísticas para analizar la frecuencia y distribución geográfica de los ataques de phishing en el Perú durante el año 2023. Esto incluirá el uso de estadísticas descriptivas para caracterizar los tipos de ataques más comunes, los sectores más afectados, y el impacto económico estimado de los incidentes.

En el aspecto cualitativo, se llevarán a cabo entrevistas semiestructuradas con expertos en seguridad cibernética, representantes de empresas y funcionarios gubernamentales. Estas entrevistas proporcionarán insights cualitativos sobre las estrategias empleadas por los perpetradores de phishing, las vulnerabilidades específicas explotadas, y las respuestas organizativas y regulatorias adoptadas en respuesta a los ataques.

Se cumplirá con todas las consideraciones éticas pertinentes, asegurando la confidencialidad de los datos sensibles y obteniendo el consentimiento informado de los participantes en las entrevistas. Se tomarán medidas para proteger la privacidad de las organizaciones y personas que proporcionen información relevante para el estudio.

Finalmente los resultados cuantitativos y cualitativos se integrarán para proporcionar una visión completa de las tendencias del phishing en el Perú en 2023 y sus consecuencias. Esto permitirá identificar patrones emergentes, evaluar la efectividad de las medidas de mitigación existentes y proponer recomendaciones para fortalecer la infraestructura de ciberseguridad del país.

3.4. Población

La población objetivo de este estudio se centra en los usuarios activos de Internet en el Perú que están expuestos a ser víctimas de phishing como modalidad principal de ciberataque durante el año 2023. Esta población incluirá individuos que utilizan servicios en línea, como correo electrónico, redes sociales, y transacciones financieras a través de internet. Se considerarán usuarios de diversas edades, géneros y niveles socioeconómicos, con el objetivo de captar una muestra representativa de la población peruana afectada por este tipo de amenazas cibernéticas.

3.5. Muestra

La muestra seleccionada para este estudio estará compuesta por usuarios activos en el Perú que han sido afectados por ataques de phishing durante el año 2023. Se utilizará una estrategia de muestreo basada en criterios específicos para asegurar la representatividad y relevancia de los datos recopilados. Los criterios de selección incluirán la identificación de víctimas de phishing a través de reportes documentados, bases de datos de instituciones financieras y organismos de ciberseguridad, así como casos documentados de pérdidas financieras. Se emplearán técnicas de muestreo aleatorio estratificado para asegurar la diversidad geográfica y demográfica de la muestra, garantizando así una representación adecuada de las distintas regiones y perfiles de usuarios afectados por este tipo de ciberataques en el contexto peruano.

3.6. Campo o lugar de estudio

El campo de estudio para esta investigación se centra en el ciberespacio, específicamente en el contexto digital del Perú. Se llevará a cabo un análisis detallado de incidentes y casos documentados de phishing, focalizándose en la recopilación y análisis de datos disponibles en plataformas digitales públicas y privadas, así como en informes de entidades gubernamentales y empresas de ciberseguridad. Este entorno se caracteriza por:

- Datos Digitales: El estudio se enfoca en la recopilación y análisis de datos digitales relevantes sobre incidentes de phishing en el Perú durante el año 2023, utilizando fuentes como informes públicos de instituciones financieras y organismos de seguridad cibernética.
- Diversidad Geográfica: Se considera la diversidad geográfica del Perú para entender las variaciones regionales en la incidencia y respuesta ante ataques de phishing, abarcando tanto áreas urbanas como rurales.
- Colaboración Institucional: Se establecerá una colaboración con entidades locales y regionales para acceder a datos relevantes y asegurar la representatividad de la muestra, garantizando el cumplimiento ético y legal en el manejo de la información sensible.

3.7. Técnicas e instrumentos de recolección de datos

Para llevar a cabo la investigación sobre phishing en el Perú durante el año 2023, se emplearán técnicas y herramientas especializadas adaptadas a la dinámica del ciberespacio y los objetivos del estudio.

3.7.1. Técnica de recopilación de datos:

- Monitoreo Continuo en Tiempo Real: La principal técnica será el monitoreo continuo en tiempo real de fuentes digitales abiertas y reportes de incidentes de seguridad proporcionados por entidades gubernamentales y privadas. Esto asegurará la captura inmediata de datos relevantes para el análisis de tendencias y patrones de phishing en el Perú.

3.7.2. Instrumentos de recolección de datos:

- Informes de Instituciones de Seguridad Cibernética: Se recopilarán informes y análisis proporcionados por instituciones como la Policía Nacional del Perú y empresas de seguridad cibernética reconocidas, que documentan casos de phishing y sus impactos.
- Entrevistas Semiestructuradas: Se realizarán entrevistas con expertos en ciberseguridad y representantes de instituciones financieras y gubernamentales para

obtener insights cualitativos sobre las técnicas y consecuencias del phishing en el contexto peruano.

- Análisis de Datos Públicos: Se utilizarán bases de datos públicas y reportes de incidentes específicos de phishing en el Perú para analizar tendencias, métodos de ataque y sectores más afectados.

3.7.3. Consideraciones éticas:

- Cumplimiento Legal y Ético: Se cumplirán las regulaciones y políticas éticas vigentes en la recopilación y uso de datos, asegurando la confidencialidad y anonimización de la información sensible obtenida.
- Consentimiento Informado: Cuando sea necesario, se obtendrá el consentimiento informado de los participantes en entrevistas y encuestas para garantizar la participación ética y voluntaria en la investigación.

Capítulo 4

Cronograma de actividades

Se muestra el cuadro 4.1, el cronograma de actividades como representación general para las diversas etapas del proyecto. Asimismo, intentaremos mantener la flexibilidad en ella.

Actividad	**2025**										
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov
Elaboración de la problemática	X	X									
Elaboración del marco teórico	X	X									
Estructurar esquema de la tesis			X	X	X	X	X				
Recopilación de datos		X	X	X	X	X	X				
Análisis de los resultados					X	X	X	X			
Elaboración del informe final						X	X	X	X		
Sustentación de tesis										X	X

Cuadro 4.1: Cronograma de actividades para la tesis.

Capítulo 5

Presupuesto del proyecto

Este presupuesto refleja los costos estimados para los equipos necesarios, software especializado, acceso a información académica, impresión de documentos y una reserva para imprevistos durante la investigación sobre phishing en el Perú

Actividad	**Descripción**	**Cant.**	**Total (S/.)**
Equipos de cómputo	Adquisición de ordenador portátil de alto rendimiento	1	4000
Software especializado	Herramientas de procesamiento de lenguaje natural	1	300
Acceso a bases de datos	Suscripciones a revistas académicas y bases de datos	1	200
Impresión de documentos	Impresión de copias de informes y tesis	1	300
Reserva de imprevistos	Fondos para contingencias	1	500
Total estimado			**5300**

Cuadro 5.1: Presupuesto del proyecto

Bibliografía

Anderson, P. Q. (2018). *Writing Your Research Report: A Practical Guide*. Research Publishing.

Brown, K. L. (2021). *Statistical Analysis for Social Sciences*. Statistics Press.

Davis, S. T. (2022). *Effective Presentation Skills for Researchers*. Presentation Books.

FireEye. (2021). Title of the article/book chapter. *Journal Name or Book Title*, *Volume number*(Issue number), Page range. https://doi.org/DOInumberifavailable

IBM Corp. (2020). *IBM SPSS Statistics for Windows (Version 27.0)* [[Computer software]]. https://www.ibm.com/spss

Jakobsson, M., & Myers, S. (2007). Title of the article/book chapter. *Journal Name or Book Title*, *Volume number*(Issue number), Page range. https://doi.org/DOInumberifavailable

Johnson, M. B. (2018). *Theoretical Frameworks in Social Science Research*. Academic Press.

McAfee. (2020). Title of the report or article. https://www.mcafee.com

Smith, J. A. (2020). Identifying Research Problems. *Research Journal*, *12*(3), 45-67. https://doi.org/10.1234/rj.2020.003

Taylor, D. (2017). *Research Methods: Data Collection Techniques*. Academic Publishing.

Williams, R. C. (2019). *Structuring Your Thesis: A Step-by-Step Guide*. University Press.