ESCUELA DE EDUCACIÓN SUPERIOR TECNOLÓGICA PRIVADA TOULOUSE LAUTREC

CAMPAÑA AUDIOVISUAL PARA REDUCIR LOS FRAUDES CIBERNÉTICOS EN LA ADQUISICIÓN DE BIENES Y SERVICIOS EN LIMA METROPOLITANA

Tesis para obtener el titulo profesional Licenciado en Comunicación Audiovisual Multimedia

AUTORES:
DIEGO ALONSO DONAYRE DEL RIO
(https://orcid.org/0000-0002-8104-9222)

MARIANO JAVIER ZEVALLOS MATOS
(https://orcid.org/0009-0003-8612-6113)

ASESOR
JONATAN FREDDY SAYAN CHUMBIRIZO
(https://orcid.org/0000-0002-3436-5249)

Lima-Perú
Octubre 2024

PAPER NAME

CAMPA%C3%91A AUDIOVISUAL PARA REDUCIR LOS FRAUDES CIBERN%C3%89TICOS EN LA ADQUISICI%C3%93N DE BIENES Y SERVICIOS EN LIMA METROPOLITANA.pdf

AUTHOR

-

WORD COUNT

7107 Words

CHARACTER COUNT

41414 Characters

PAGE COUNT

40 Pages

FILE SIZE

1.8MB

SUBMISSION DATE

Oct 18, 2024 4:17 PM GMT-5

REPORT DATE

Oct 18, 2024 4:17 PM GMT-5

15% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 11% Internet database
- 4% Publications database
- Crossref database
- Crossref Posted Content database
- 13% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material

Dedicatoria

Esta investigación está dedicada a los miembros de mi familia, Lita Silvia del Rio Muñiz, Brian Rubén Francisco Donayre Palomino, Alejandra Donayre del Rio y en especial a mi novia Kimberly Fabiola Quispe Bautista, por impulsarme a realizar todo lo que me propongo, sin importar lo difícil que se ponga en el camino, todo se puede lograr. Con cariño, Diego.

Yo dedico esta investigación a mi familia, en especial a mi madre Consuelo Gricelda Matos Cubas quien me ha impulsado a la academia desde muy niño, a mi padre Herminio Antonio Zevallos Medina por su sacrificio y a mis amigos más cercanos que siempre me apoyan y luchan conmigo codo a codo. Con cariño, Mariano.

Tabla de contenido

Resumen 7

Abstract 8

Capítulo I: El Problema…….....9

1.1 Planteamiento del Problema 9

1.2 Preguntas de investigación 12

1.2.1 Pregunta general 12

1.2.2 Preguntas específicas 12

1.3 Objetivos de Investigación 13

1.3.1 Objetivo general.....13

1.3.2 Objetivos específicos 13

Capítulo II: Marco Teórico 14

2.1 Mapa de Literatura 14

2.2 Antecedentes de Investigación.....15

2.3 Desarrollo de la Perspectiva Teórica.....17

Capítulo III: Metodología 21

3.1 Muestra, Unidad de Análisis y Muestreo.....21

3.2 Diseño de Investigación 21

3.3 Operacionalización de Variables.....22

3.4 Consentimiento Informado.....23

3.5 Procedimiento para Recolectar y Analizar los Datos.....24

Capítulo IV: Resultados.....25

4.1 Análisis de Resultados 25

4.2 Discusión de Resultados 33

4.3 Recomendaciones 34

Referencias.....36

Anexos 38

Lista de Tablas

Tabla 1 *Operacionalización de la Variable: Consumo masivo* ……..…22

Tabla 2 *Operacionalización de la Variable: Inteligencia artificial y ciberdelincuencia* ……..…23

Lista de Figuras

Figura 1. Mapa de la literatura de los principales aspectos de las compras online masivas ……..……..…...…14

Figura 2. Mapa de la literatura de los factores de ……..……..…14

Figura 3. Sexo de los participantes ……...…….25

Figura 4. Rango de edad de los participantes ……....26

Figura 5. Dispositivos más usados en canales ecommerce ……....26

Figura 6. Nivel de percepción de canales ecommerce ……...……27

Figura 7. Métodos de pago más usados en canales ecommerce ……....27

Figura 8. Plataformas ecommerce más usadas …….……..……28

Figura 9. ¿Ha sido víctima de un cibercrímen? ……..…29

Figura 10. Canales online donde fueron víctima de un cibercrimen 29

Figura 11. ¿Por qué medios estamos más expuestos a un cibercrimen?……...…….30

Figura 12. Nivel de exposición a los ataques de phishing ……..…...…30

Figura 13. ¿Ha visto alguna campaña de ciberseguridad? …….31

Figura 14. ¿Por qué canales has visto alguna campaña de ciberseguridad?.....…31

Figura 15. ¿Por qué medios consideras es más efectivo educar sobre ciberseguridad?.....32

Figura 16. ¿Qué acciones acciones de ciberseguridad sueles tener en consideración?……..33

Resumen

La presente investigación propone una campaña publicitaria para disminuir los casos de phishing en Lima Metropolitana con el fin de contribuir con el bienestar de la sociedad y diversas personas que realizan compras de manera Online. La finalidad de la investigación es estudiar diversos casos y también aprender acerca de estos ciberataques que suceden con mucha frecuencia.

Esta investigación utiliza el método cualitativo y cuantitativo a través de encuestas a un grupo determinado de personas que viven en Lima Metropolitana y que hayan realizado por lo menos una compra de manera online en varias marcas o páginas y haber colocado sus datos personales como parte de pago y el servicio en sí.

La propuesta plantea en sí una investigación y posterior desarrollo de distintas maneras de estos ciberdelitos, los cuales ocurren muy seguido como suplantación de identidad, robo de información bancaria, transacciones no autorizadas, etc.

Como producto final, planteamos una campaña publicitaria en el cual queremos dar a conocer algunos casos y que nuestro público y población entienda la importancia de ser precavidos y cuidadosos de manera que no suframos ninguno de estos ciberdelitos.

Palabras Clave: Ataques de phishing, Ingeniería social, ciberseguridad, Consumo masivo y Psicología del consumidor.

Abstract

This research proposes an advertising campaign to reduce phishing cases in Metropolitan Lima in order to contribute to the welfare of society and various people who make purchases online. The purpose of the research is to study several cases and also to learn about these cyber-attacks that happen very frequently.

This research uses the qualitative and quantitative method through surveys to a certain group of people living in Metropolitan Lima and who have made at least one purchase online in several brands or pages and have placed their personal data as part of payment and the service itself.

The proposal itself raises an investigation and subsequent development of different ways of these cybercrimes, which occur very often as identity theft, theft of banking information, unauthorized transactions, etc..

As a final product, we propose an advertising campaign in which we want to publicize some cases and that our public and population understand the importance of being cautious and careful so that we do not suffer any of these cybercrimes.

Capítulo I: El Problema

En el presente capítulo indicaremos la definición de lo que es Phishing, y también los diferentes tipos de ciberdelito que existen en la actualidad, para poder entender las consecuencias que tiene en consumidores y empresas. Así también, daremos a conocer una campaña audiovisual,

1.1.Planteamiento del Problema

La presencia de la pandemia del COVID-19 cambió drásticamente los canales que tanto las empresas como los consumidores utilizan para comunicarse, y sobre todo comprar. Los canales tradicionales (ventas directas, catálogos) fueron reemplazados por canales online o a distancia. Esto generó un volumen de ventas masivas en la modalidad en línea, el cual fue muy superior al registrado con anterioridad, según La Cámara Peruana de Comercio Electrónico (CAPECE) en El Reporte Oficial de la Industria del Ecommerce edición 2021, las ventas online subieron de $4000 millones de dólares a $6000 millones de dólares en 2020. Llama la atención también que antes de la pandemia el volumen del total de transacciones del comercio electrónico era solo del 12,5% y que para 2021 había alcanzado el 40%, lo que impulsaba al ecommerce pues más negocios requerían de canales online como se establece en el reporte donde el número de negocios online era de 65 800 antes de la pandemia y se incrementó a 263 200 a del 2020.

Durante la crisis, el fraude digital preocupaba a empresas y consumidores, al haberse incrementado el uso de canales digitales, los cuales son herramientas en su mayoría de libre acceso. Estas en su mayoría no brindan mayores garantías en las transacciones, y los oportunistas siempre tratan de aprovechar el desconocimiento de las mismas. Las estafas están sobresaliendo de manera abrupta, el phishing, El phishing es un ataque perpetrado por estafadores, según la empresa Microsoft, quienes buscan obtener información privada de su víctima, haciéndole creer que son una fuente segura. Las víctimas eran contactadas por

correo, sms, llamadas, chat, lo que generaba cierta desconfianza en diversos canales de comunicación. Estos estafadores escogen a su víctima, o también de manera masiva, utilizan técnicas de ingeniería social para poder manipularla y que esta brinde información confidencial, haga algo o dé un objeto al perpetrador. Según la empresa de seguridad digital Kaspersky, la ingeniería social es una técnica de manipulación, que aprovecha la autoridad, motivaciones, o urgencia de la víctima para así acceder a información privada. Dicha técnica, en combinación con plataformas digitales, ciberdelincuentes y una sociedad desinformada y que ignora los riesgos del uso internet, es la más usada por cibercriminales, que utilizan todo tipo de engaños desde productos en oferta hasta sorteos millonarios, departamentos, camionetas, correos sobre problemas con tus datos de pago, chantaje, crédito hipotecario, oportunidades de negocio, préstamos, entre otros.

El ciberdelito es, pues, el delito más investigado en Perú. En el 2023 el diario "El Peruano" informaba que se han registrado más de 21,842 denuncias por phishing. Con el avance de la tecnología, el internet de las cosas, y las tecnologías de la información más presentes que nunca en nuestra vida cotidiana, el tiempo que pasamos con dispositivos electrónicos se ha incrementado exponencialmente tanto en países desarrollados como los que se encuentran en pleno desarrollo económico. Solo en la Unión Europea se estimó que en 2022 un mínimo de 80% de la población tenía acceso a internet, alcanzando picos máximos del 98% en algunos países, de acuerdo a datos del sitio web Statista. En Estados Unidos, los usuarios de internet en 2022 fueron alrededor de 313,600 millones, y en 2023 fueron alrededor de 318,660 millones, lo que sugiere que el aumento para el 2029 podría ser de más de 40 millones de usuarios, de acuerdo con el sitio Statista. Si comparamos los casos de USA y la UE con el nuestro en Perú en 2021 el 72% de la población tenía acceso a internet según estadísticas de OSIPTEL. Para el 2022 esta cifra se incrementó hasta el 87,7% es decir cerca de 8 779 988 millones de familias tendría acceso a dicho servicio, representando así un incremento del

21% en el número de usuarios de internet que corren el riesgo de un ataque de phishing o una estafa online. Ya que ahora pasamos más tiempo con un dispositivo conectado a internet es importante estar preparado ante un ataque de phishing pues estos no solo pueden ser detectados en los sitios de ecommerce, y redes sociales, sino también fuera de estos espacios, a través de tu teléfono o laptop. Desde el 2021 la Fiscalía Especializada en Ciberdelitos viene operando y hasta el 2023 había atendido más de 33,372 casos de ciberdelitos, con un total de 23,016 casos resueltos, una tasa de efectividad del 68,9% y un incremento de los ciberdelitos del 58% respecto del año anterior. Los usuarios al pasar más tiempo con dispositivos electrónicos, teléfono, pc, entre otros, son vulnerables a un ciberataque que sabemos pueden ser masivos o focalizados. Los cibercriminales encuentran la manera de manipular a los internautas a través de diferentes engaños, ya sea por correo, sms, llamada, chat, junto con la ingeniería social es usada para sacar ventaja de las motivaciones y necesidades de los desprevenidos internautas.

El cibercrimen es un tema que causa mucha preocupación no solo en nuestro país, en la Unión Europea precisamente en 2023 promulgó la “Ley de Internet” dirigida a 19 gigantes del ciber espacio, entre ellos Google, Facebook, X (antes Twitter) y Amazon, con el fin de que sean reguladas fuera de sus jurisdicciones y reducir la información falsa, pornografía de menores y todo tipo de actividad fraudulenta. El gran número de usuarios por segundo, compras online, atrae a posibles hackers que buscan crear inestabilidad, acceder a información sensible, robar información, etc. Consumidores y empresarios pueden perder la confianza en las garantías que ofrecen los canales digitales, no solo eso, sino también en las empresas que apuesten por ellos al ser espacios que no protegen su información. Es importante conocer el estado actual de los avances tecnológicos y conocer los riesgos que supone el internet tanto como cuales son los canales más usados por los estafadores, ahora

con tecnologías como la inteligencia artificial que supone un gran poder en manos de los ciberdelincuentes.

El objetivo es brindar mecanismos a la mayoría de usuarios digitales para combatir ataques de phishing y de ingeniería social que pueden resultar en robos, secuestros, extorsión y toda clase de crímenes. Queremos no solo que entiendan los riesgos, sino también las responsabilidades de usar internet, pero también exponer situaciones que se dan en este espacio abstracto no regulado, y demostrar por qué es importante que los gobiernos y organismos internacionales establezcan leyes claras, que protejan tanto a consumidores como empresas a fin de combatir colectivamente al cibercrimen. Debemos tomar conciencia sobre los riesgos del uso debido del internet, el cual es una herramienta que facilita las relaciones humanas.

1.2.Preguntas de investigación

1.2.1 Pregunta general

¿Cómo concientizar a los usuarios digitales acerca de los riesgos del uso del internet, en compras online o a través de ataques de phishing?

1.2.2 Preguntas específicas

P1. ¿Cuáles son los factores más efectivos en las campañas educativas digitales para aumentar la conciencia sobre los riesgos de las compras online y los ataques de phishing entre los usuarios de internet?

P2. ¿De qué manera la percepción del riesgo influye en el comportamiento de los usuarios digitales al realizar compras en línea y al enfrentar potenciales ataques de phishing?

P3. ¿Qué métodos de formación y concientización en ciberseguridad son más efectivos para reducir la vulnerabilidad de los usuarios frente a ataques de phishing y fraudes en compras online?

1.3.Objetivos de Investigación

1.3.1 Objetivo general

Identificar los factores más efectivos en las campañas educativas digitales para aumentar la conciencia sobre los riesgos de las compras online y los ataques de phishing entre los usuarios de internet.

1.3.2 Objetivos específicos

O1. Analizar cómo la percepción del riesgo influye en el comportamiento de los usuarios digitales al realizar compras en línea y al enfrentar potenciales ataques de phishing.

O2. Determinar los métodos de formación y concientización en ciberseguridad más efectivos para reducir la vulnerabilidad de los usuarios frente a ataques de phishing y fraudes en compras online.

O3. Educar a los internautas sobre la ingeniería social y cómo detectar los tipos más usuales de ataques de phishing.

Capítulo II: Marco Teórico

En el presente capítulo se presentarán y describirán los factores principales de la temática, como también analizar los antecedentes que hemos investigado previamente en la presente investigación.

2.1. Mapa de Literatura

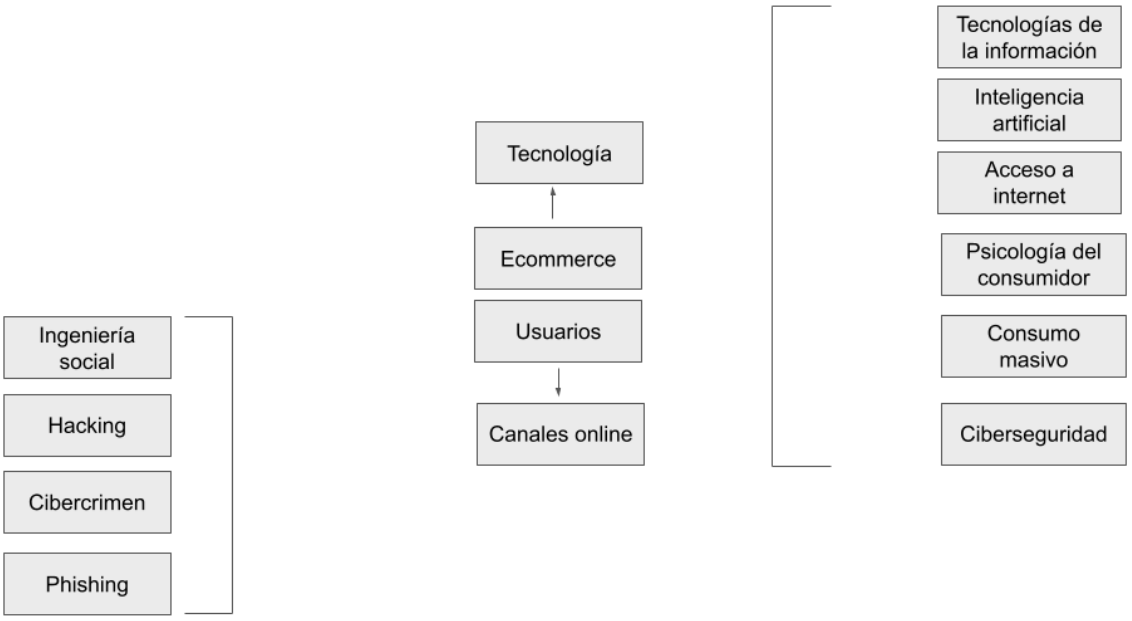


Figura 1. Mapa de la literatura de los principales aspectos del consumo online masivo

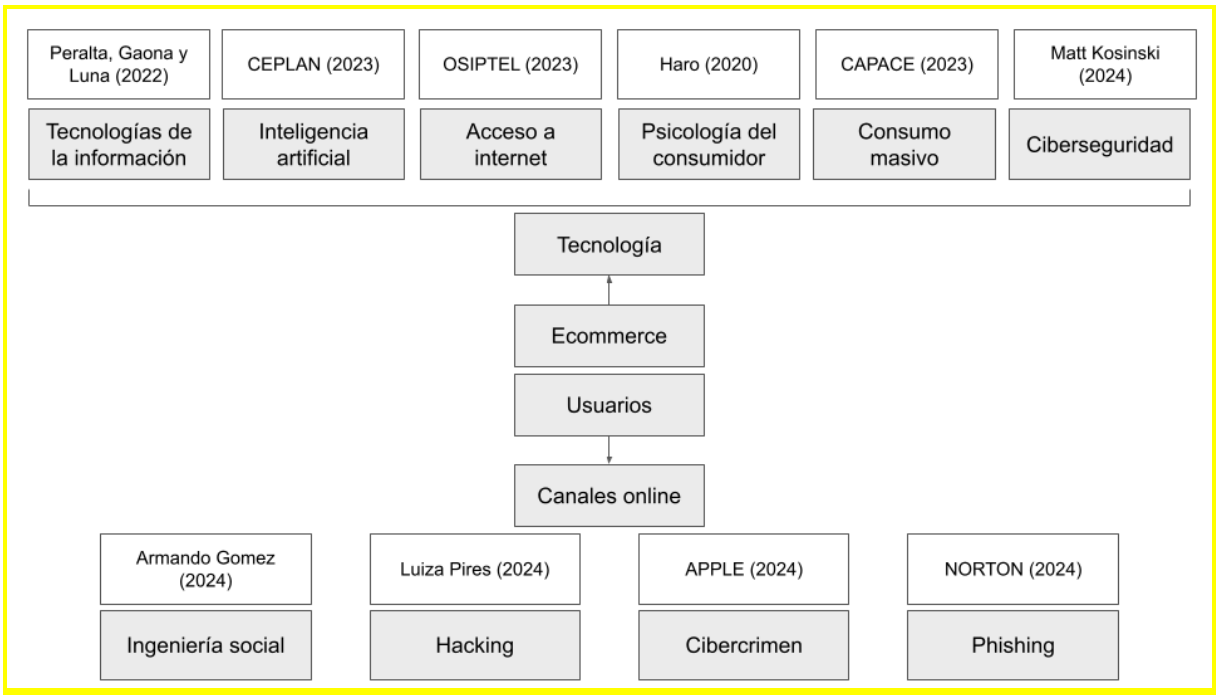


Figura 2. Mapa de la literatura de los principales factores del phishing

2.2. Antecedentes de Investigación

Calvo (2022) Realizó la investigación "La Responsabilidad Civil de los Bancos en los Delitos de Estafa por Phishing", donde expone que el patrimonio económico de los usuarios también recae sobre las instituciones financieras. Para la autora, internet es una herramienta explotada por ciberdelincuentes, que abusan tanto de hardware como de software para robar dinero y/o datos sensibles. En dicha tesis la autora expone la dificultad del usuario de tomar acciones ante una compra no autorizada y basándose en leyes vigentes involucra a las entidades bancarias a velar por el patrimonio de los usuarios. Siempre que el usuario no haya actuado con negligencia y reporte el fraude, es responsabilidad de la institución financiera salvaguardar los datos de sus clientes así como reintegrar sus fondos, salvo puedan probar que el usuario está incurriendo haya actuado de manera negligente.

Castro (2022) realizó la investigación "Elaboración de una herramienta de concienciación para dispositivos Android para evitar ser víctima de phishing". Dicha investigación concluye en que la población global ya ha sido víctima de ataques de phishing debido a que estos son regularmente perpetrados de forma masiva. El INCIBE (Instituto Nacional de Ciberseguridad es ciberseguridad), es una de las pocas instituciones en España que lucha contra la cibercriminalidad, proporcionando información para prevenir estos ataques. Sin embargo, los intentos de proteger a la población y empresas en general son muy pocos y se debe unir fuerzas en todos los niveles de la sociedad (estado, sociedad civil, empresas) creando campañas para proteger la información de las personas a través de paneles, pancartas, marquesinas en buses, tv, etc, haciendo un llamado específico a las empresas que son las primeras en ser llamadas a luchar contra los intentos de phishing, tanto contra sus intereses como que usen su marca para perpetrar ataques cibernéticos. Concluye

alegando que el porcentaje de éxito de los ciberataques se debe en su mayoría a que la población carece o desconoce las acciones recomendadas en materia de ciberseguridad.

Barrantes y Espitia (2024) llevaron a cabo la investigación “Proceso de phishing y pautas para la identificación de sitios web falsos A phishing process and guidelines for identifying fake websites” Se resalta que el phishing es una técnica que busca explotar el desconocimiento de los internautas, quienes desconocen los medios por los que serán atacados. También se brinda las siguientes recomendaciones: siempre contar con antivirus, esto es esencial pues los ataques suelen ser perpetrados de manera masiva. Otra recomendación es activar la verificación de dos pasos y verificar siempre las URL de los sitios, desde otro dispositivo, el sitio oficial para detectar cualquier tipo de indicio que indique la veracidad del sitio web.

Zambrano (2024) Realizó la investigación “Impacto de la inteligencia artificial en los ciberataques”, en la cual expone que es fundamental la educación en ciberseguridad. Esta iniciativa debe provenir tanto de entidades del gobierno y la empresa privada, a fin de unificar esfuerzos y poner en práctica acciones efectivas en pro de la ciberseguridad. Si bien es cierto, el autor reconoce que la IA puede ser una herramienta vital en contrarrestar amenazas que usen esta misma tecnología, hace énfasis en que su uso indebido por parte de hackers maliciosos es más peligrosa que beneficiosa para la ciberseguridad, ya que con ella los ciberataques son sofisticados, difíciles de detectar hasta ser capaces de vulnerar la mayor cantidad de sistemas en un entorno donde el usuario está expuesto al carecer de educación sobre protección de datos. Concluye mencionando que es fundamental impulsar la especialización de los profesionales en materia de seguridad informática y establecer un ecosistema donde toda la sociedad esté involucrada en la ciberseguridad, generando así una cultura donde la prevención y el uso correcto de la tecnología sea una práctica común.

2.3. Desarrollo de la Perspectiva Teórica

La ingeniería social consiste en emplear tácticas psicológicas para persuadir a una persona para condicionar su comportamiento, muchas veces en contra de su voluntad, principalmente busca que el usuario comparta información a través de internet. *Juan Armando Gómez, (actualizado 03/05/24) Ingeniería social: 6 consejos para proteger a tu empresa de su impacto. Cyberblog. https://www.deltaprotect.com/blog/ingenieria-social.* No necesariamente ejecutada por hackers, la ingeniería social es un arma cuyo propósito es que la víctima entregue voluntariamente información confidencial. Puede tomar muchas formas, como llamadas o correos, una vez que obtengan información de su víctima el siguiente paso es vulnerar cuentas y dispositivos. *Panda Security, (28/12/2022). ¿Qué es la ingeniería social y cómo puedes protegerte de ella?. Educación Digital. https://www.pandasecurity.com/es/mediacenter/que-es-ingenieria-social/.*

Se conoce como un ciberataque de phishing a aquel que tiene por objetivo robar o dañar intencionalmente datos privados, haciendo que los usuarios brinden información entre ella personal, contraseñas, números de tarjeta de crédito, y que pueden ser de diferentes tipos: correo, malware, SMS, mensaje de voz, *Microsoft, 2024¿Qué es el phishing? Seguridad de Microsoft, (https://www.microsoft.com/es-es/security/business/security-101/what-is-phishing)*. Es definida como una táctica de la ingeniería social que a través de métodos fraudulentos intenta obtener información personal, priman los intentos por correo pero no se limitan a suplantación de identidad, suscripciones, promociones, ventanas emergentes *Apple, (27 de septiembre de 2024), Reconocer y evitar estrategias de ingeniería social, como los mensajes de suplantación de identidad (phishing), llamadas de soporte falsas y otras estafas https://support.apple.com/es-es/102568*

En el año 2021 el 63.3% de hogares peruanos contaba con servicio de internet según el Instituto Nacional de Estadística e Informática (INEI), (Estadísticas de las tecnologías de la

información en los hogares). Dos años después, OSIPTEL reportaba que 9 de cada 10 peruanos tenían internet fijo o móvil(Reporte Estadístico 2023).

En el Perú en el año 2023 hubo un consumo masivo en plataformas marketplace como se señala en la edición 2024 de la Revista CAPECE *(Observatorio Ecommerce 2024)* se reveló que entre el 50% y 70% de las ventas online en 2023 fueron a través de sitios marketplace (Falabella, Mercado Libre, Amazon, Vea, Ripley, Aliexpress, Promart, Oechsle e Ebay siendo los más solicitados) donde Falabella lideraba con más de 18,9 millones de visitas online. También pudimos conocer que entre 2020 y 2024 el consumo con tarjeta por ecommerce se incrementó de 14% a 60%.

El término hacker se atribuye a una persona con muchos conocimientos en tecnología y que emplea dicho conocimiento para vulnerar sistemas, redes y dispositivos, aunque antiguamente se usaba para denominar a un experto en programación. *Luiza Pires (06/06/2024)¿Qué es un hacker y qué hace?.Cultura y Seguridad Digital. https://www.eset.com/latam/blog/cultura-y-seguridad-digital/que-es-un-hacker-y-que-hace/.* El concepto de hacking se refiere a hacer uso de canales poco convencionales y a veces hasta ilícitos para adquirir acceso no autorizado a un dispositivo digital, sistema o en algunos casos, redes informáticas. Si bien es cierto, esta actividad puede ser vista como positiva en materia de ciberseguridad, negativa si es una amenaza o neutral, como en algunas formas de piratería, es preciso distinguirlo del hacking ético, que es utilizado para fortalecer la seguridad de las organizaciones, todo lo contrario a un ciberataque. *Mateo Kosinski (16/06/2024) ¿Qué es el hacking?.Temas. https://www.ibm.com/mx-es/topics/cyber-hacking.*

La ciberseguridad es la puesta en práctica de medidas, acciones, políticas y tecnologías usadas para prevenir y contrarrestar los ciberataques. Su principal función es la de proteger datos, sistemas, aplicaciones, dispositivos, y activos en general de ataques de phishing, malware, y ransomware. *Gregg Lindemulder, Matt Kosinski, (12/06/2024). ¿Qué es*

la ciberseguridad?. Temas. https://www.ibm.com/es-es/topics/cybersecurity. Es imperativo establecer acciones y prácticas concretas adicionales al uso de software. Estas acciones van pero no se limitan a copias de seguridad, buenos hábitos tecnológicos, actualizar software, usar contraseñas únicas, autenticación múltiple, bloqueo de dispositivos, entre otros, con el fin de proteger cuentas, dinero, archivos, fotos e información personal. *Microsoft,(2024) Soporte Técnico.¿Qué es la ciberseguridad? https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390.*

Las tecnologías de la información son herramientas producto de los avances de la ciencia y tecnología que son usados para simplificar tareas y optimizar procesos. Las herramientas más destacadas de nuestro tiempo son sin duda el ordenador, dispositivos móviles, y el internet. *(Peralta, Gaona y Luna, 2022)*. El término abarca diversas tecnologías presentes en nuestro día a día y se basa fundamentalmente en la informática, las comunicaciones y la electrónica, con el fin de almacenar, procesar y distribuir la información. *Ministerio de Educación. "Educación Técnica Tecnológica y Productiva - Carrera Tecnología de la Información Digital" (2024)*

La inteligencia artificial es una tecnología que permite sin la intervención del hombre la creación de contenido, desde texto, y sonidos hasta imágenes y videos *(CEPLAN, 2023*). Es una nueva oportunidad de adoptar nuevas tecnologías, en especial TIC, las cuales prometen acelerar el progreso humano y facilitar el libre acceso a la información. La agenda 2030 para el Desarrollo sostenible señala que los ODS pueden ser positivos en áreas como la industrialización sostenible, la innovación, salud y energía. *(CEPAL Tecnologías digitales para un nuevo futuro 2021).*

El cibercrimen se define como el delito realizado de manera online. Se considera cibercrimen a acciones que vulneran la privacidad, acoso, abuso sexual, acoso, y suplantación

de indentidad. Dichas acciones son cada vez más frecuentes en el ciberespacio. *Norton, (08/08/2018) De qué manera distinguir el cibercrimen y protegerse. How to. https://lam.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime.* El cibercrimen es una actividad delictiva cuyo objetivo son los dispositivos y las redes. Perpetrado en la mayoría de casos por hackers que buscan algún beneficio económico, puede ser motivado por otras razones distintas a las económicas. *Kaspersky, (2024) ¿Qué es el cibercrimen? Cómo protegerse del cibercrimen. Tipos de amenazas. https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime.*

La Psicología de los consumidores es la percepción que estos tienen sobre los diferentes servicios, productos, empresas, marcas y hasta estereotipos. Los medios de comunicación son los que más influyen en las decisiones de consumo, siendo internet el más influyente. La prensa en menor medida cala más en grupos de mayor edad, le siguen las revistas con un mejor material impreso que causa mayor impacto, está dirigido a grupos específicos. Sorprende, pero aún la radio es un canal viable, ya que tiene un efecto inmediato que explota horarios y audiencias. Por último la TV, que a diferencia de la radio explota la imagen, el color y el sonido, es capaz de emplear diversos formatos con espacios de hasta 30 segundos por mensaje. *(Villegas, Medina y Abril, 2020)*. Está constituida por la percepción que tienen los consumidores sobre los estímulos provenientes de la publicidad, con el fin de captar su atención. De acuerdo a la complejidad de los elementos estimulantes, estos pueden ser más o menos ventajosos, basado en las leyes de la Gestalt que priorizan la naturaleza, el color o el tamaño, *(Haro, 2020*).

Capítulo III: Metodología

En el presente capítulo se desarrollará el tipo de diseño de investigación que se aplicó y los elementos con los que se obtuvo los datos necesarios para conocer los canales digitales por los cuales los usuarios se sienten más vulnerables a los ataques de phishing.

3.1. Muestra, Unidad de Análisis y Muestreo

Para la presente investigación, se trabajará en concreto con (30) personas que con frecuencia realizan compras de manera online a través de diversos E-commerce de Lima Metropolitana.

El tipo de muestreo es no probabilístico por conveniencia debido a las características que posee un grupo en particular. De esa forma se podrá hallar muestras con mayor facilidad y así conocer las necesidades básicas de la población seleccionada con el objetivo de definir un diseño cómodo y sencillo para el usuario.

3.2. Diseño de Investigación

Se utilizó un diseño de encuesta para obtener de forma más organizada la información de la población determinada, adquirir datos más precisos y medibles a partir de porcentajes.

La población seleccionada para el muestreo fueron jóvenes y adultos con edades entre los 18 y 99 años.

3.3. Operacionalización de Variables

Tabla 1

Variable	Definición conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de medición / opciones de respuesta
Consumo masivo	(Observatorio Ecommerce 2024) reveló que entre 2020 y 2024 el consumo con tarjeta por ecommerce se incrementó de 14% a 60%.	Se analizará los métodos de pago más frecuentes en compras online de nuestros encuestados y así determinar cuál es la tendencia en la población en estudio.	Servicios básicos Compras online	Formas de pago Canales e commerce más usados	Encuesta de opción simple a personas que cuenten con internet fijo o móvil

Operacionalización de la Variable: Consumo masivo

Tabla 2

Variable	Definición conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de medición / opciones de respuesta
Inteligencia artificial y ataques de ingeniería social (phishing)	Zambrano (2024) define a la inteligencia artificial como, más peligrosa que beneficiosa en manos de hackers ya que les brinda herramientas sofisticadas, evasivas y difíciles de detectar ya que explota la desinformación de usuario.	Se analizará cuáles son para los usuarios los canales por los que se sienten más expuestos a los ataques de phishing.	Nivel de exposición a ciberataques Nivel de seguridad de plataformas ecommerce	Canales para educar en ciberseguridad Dispositivos más usados para ecommerce	Encuesta de opción simple a personas que acostumbren a realizar compras online

Operacionalización de la Variable: Inteligencia artificial y ciberdelincuencia

3.4. Consentimiento Informado

La presente investigación requirió del uso de encuestas para validar la información de usuarios que realizan compras de manera online, a través de sitios web, formas de compra, método de pago y qué dispositivo utiliza para realizar dichas operaciones. Con dicha encuesta, hemos podido llegar a una cantidad de personas que realiza compras a través de e-commerce.

3.5. Procedimiento para Recolectar y Analizar los Datos

Se aplicó como instrumento de medición una encuesta de opción múltiple a personas de distintos rangos de edades, los cuales suelen realizar compras de manera online. Utilizando diversas páginas, aplicativos y pagando principalmente con tarjetas de crédito. Dicha encuesta fue aplicada en Lima Metropolitana. Los puntos principales para la obtención de datos fueron los siguientes:

- Edad
- Qué dispositivo utiliza para realizar compras online
- Métodos de pago
- Seguridad a través de este tipo de compras
- Sitios web para realizar compras

Se utilizó la herramienta de Google Docs para realizar la encuesta y mostrar los resultados obtenidos de la misma, mediante la obtención de tablas estadísticas y barras gráficas de la información recolectada.

Capítulo IV: Resultados

Esta sección recopila información sobre usuarios que cuentan con el servicio de internet tanto fijo como móvil y que utilizan distintos medios de ecommerce. En base a los datos obtenidos podremos plantear recomendaciones que permitan a los usuarios tomar acciones en materia de ciberseguridad, a fin de reducir la cantidad de estafas y crímenes cibernéticos.

4.1. Análisis de Resultados

Se aplicó una encuesta simple a 31 personas para que nos cuenten su experiencia con los principales canales de ecommerce y su experiencia con crímenes cibernéticos.

Resultados:

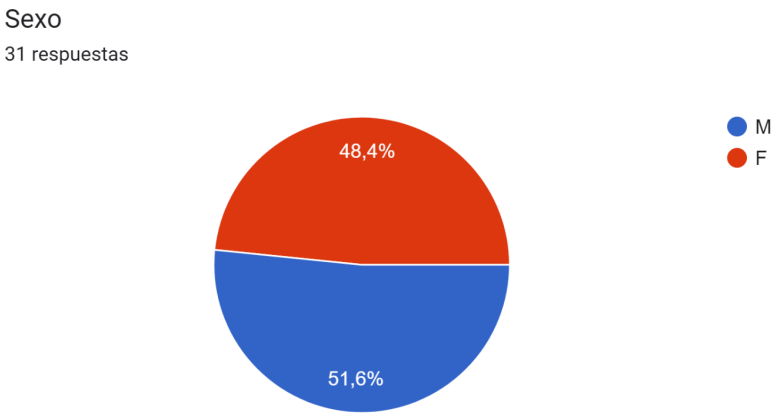


Figura 3. Sexo de los participantes

La figura 3 nos muestra que en la encuesta participaron más hombres, con un total del 51.6%, mientras que el porcentaje de hombres que participaron fue de 48.4%.

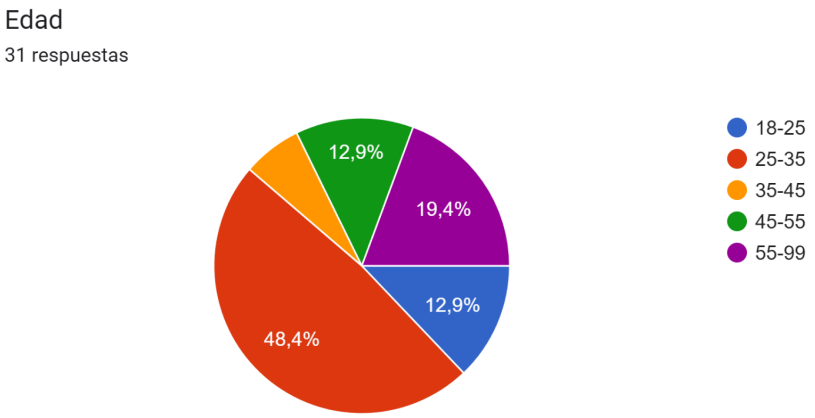


Figura 4. Rango de edad de los participantes

La figura 4 nos muestra que la edad promedio de las personas que participaron es de entre 25 a 35 años con un porcentaje de 48.4%, seguido de los grupos que tienen entre 18 a 25 años y los que tienen entre 45 a 55, ambos con un total de 12.9%. Y finalizando con los grupos de entre 55 a 99, con un porcentaje de 19.4%.

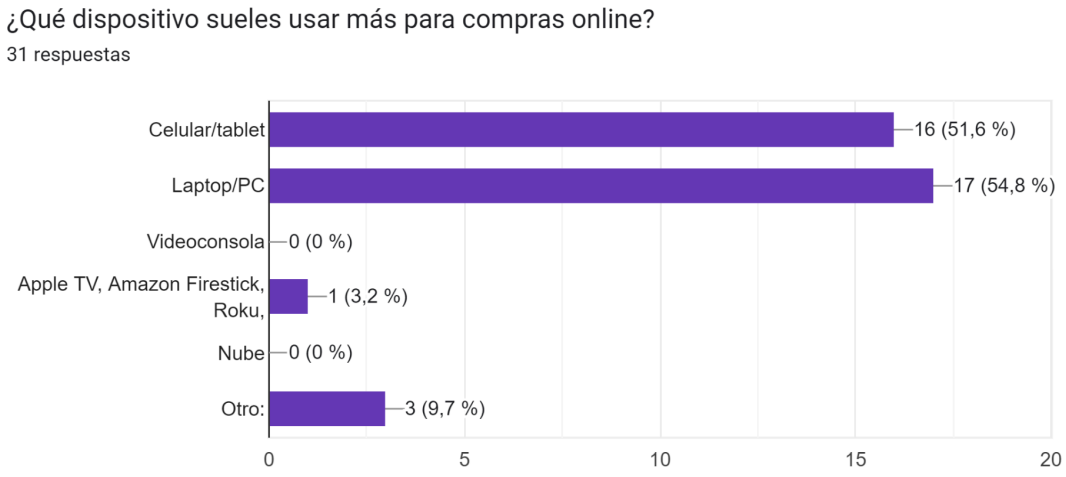


Figura 5. Dispositivos más usados en compras online

La figura 5 nos muestra los dispositivos más usados por los participantes de nuestra encuesta. Con un porcentaje de 58.8% los usuarios prefieren realizar sus compras online a traves de laptop/PC. En segundo lugar, se ubica el celular/tablet.

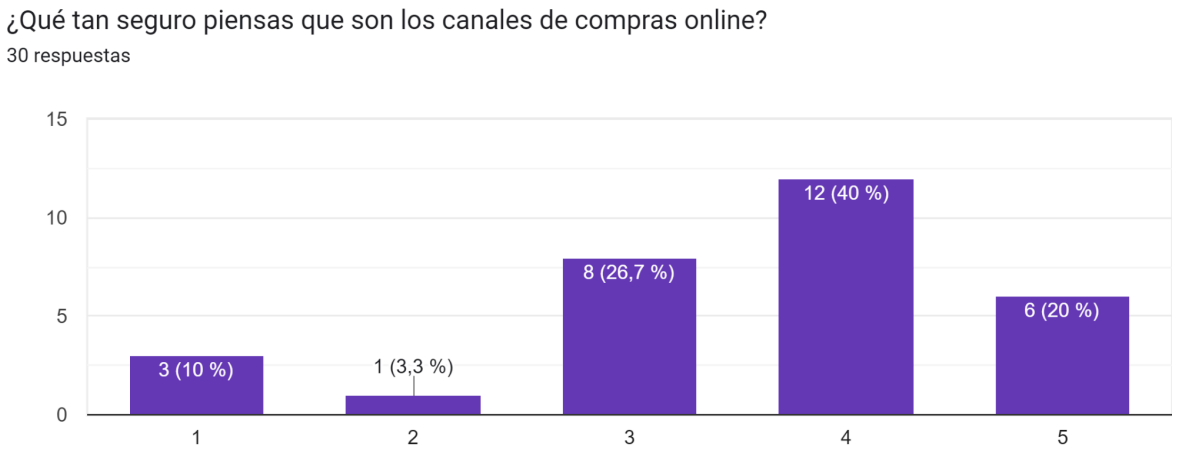


Figura 6. Nivel de percepción de canales online

La figura 6 nos muestra el nivel de percepción que tienen los usuarios acerca de los canales online, siendo 1 poco seguro y 5 muy seguro. 10% de los encuestados consideran que los canales de compras online son nada seguros, seguido de un 3,3% que consideran que son poco seguros. El 26.7% considera que los canales de compras online no son ni muy seguros ni poco seguros. Luego, con un 40%, los usuarios consideran que estos canales son seguros y por último, un 20% de los encuestados considera que los canales de compras online son muy seguros.

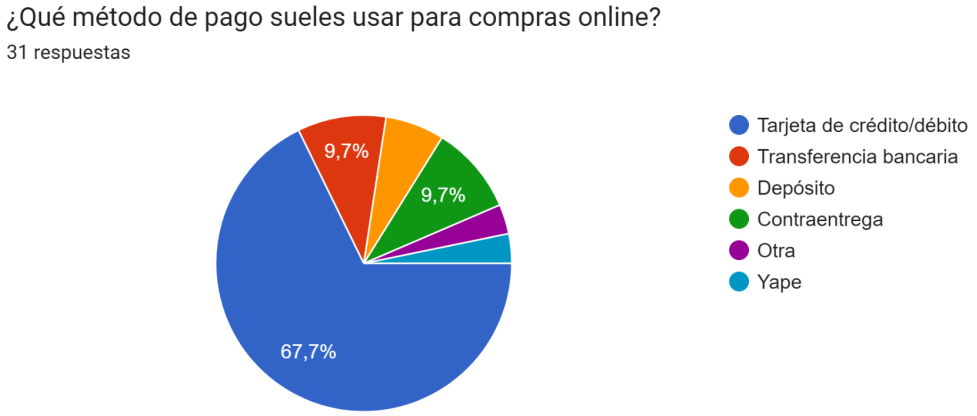


Figura 7. Métodos de pagos más usados en compras online.

La figura 7 nos muestra los medios de pago más usados en las compras online. El medio más usado por los encuestados es sin duda la tarjeta de crédito con un 67.7% de los encuestados. Le sigue la transferencia bancaria y la contraentrega con un 9.7% respectivamente. Yape se ubica en tercer lugar con 3.2% junto con otros medios. Por último, el depósito representa un 6.5% entre los métodos de pago preferidos por los encuestados.

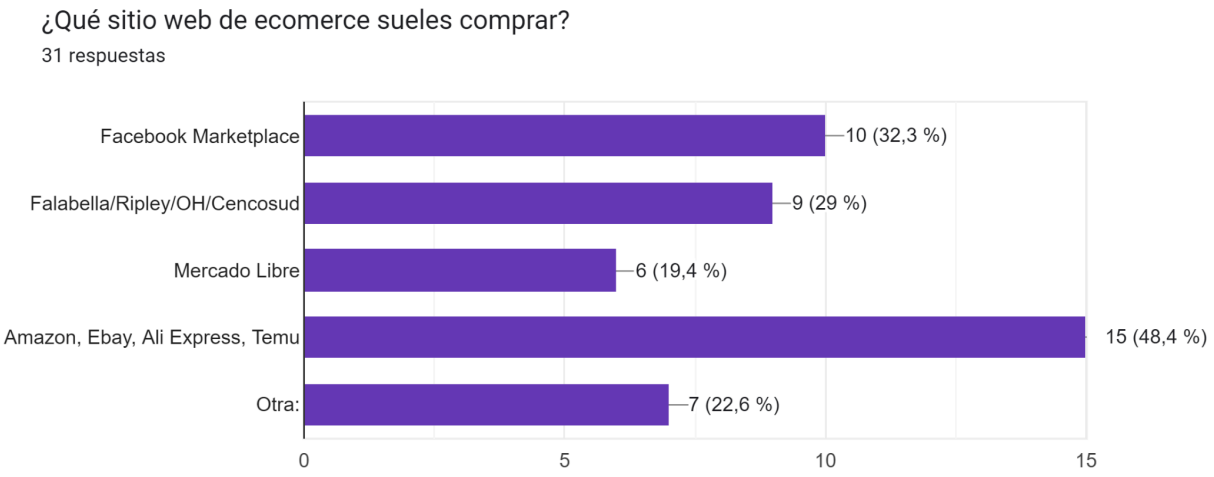


Figura 8. Sitios web ecommerce más usados.

Los usuarios prefieren mayormente utilizar sitios de ecommerce internacionales (Amazon, Ebay, Aliexpress, Temu), con un 48.4%. El segundo sitio más usado es Facebook Marketplace con un 32.3% de usuarios. En tercer lugar tenemos plataformas locales (Falabella, Ripley, Oh, Cencosud) con un 29%. En cuarto lugar, con un 22.6% los usuarios prefieren usar otros sitios a los propuestos anteriormente. Por último, con un 19.4% de usuarios, se ubica Mercado Libre.

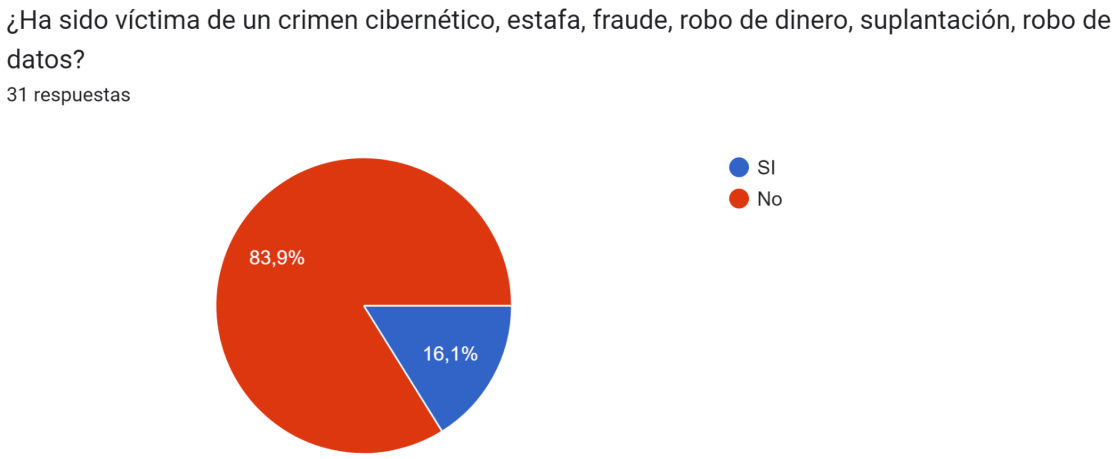


Figura 9. ¿Ha sido víctima de un cibercrímen?

La figura 9 nos muestra si los usuarios han sido víctima de algún cibercrimen. Con un 83.9%, los usuarios indican que no han sido víctimas de un cibercrimen. Con un 16.1% los usuarios indican que sí han sufrido de un crimen cibernético.

Si tu respuesta fue sí, cuéntanos brevemente el canal utilizado.7 respuestas

Usaron mis datos y sacaron una tarjeta del bcp

Compraron en línea con mi número de tarjeta de crédito, aun cuando yo la tenia

Facebook marketplace

Mercado libre

No

Facebook

Marketplace

Figura 10. ¿Por qué medio ha sido víctima de un ciberdelito?

La figura 10 nos muestra los canales por los cuales han sufrido un ciberdelito. Podemos observar que la respuesta más común es Facebook Marketplace.

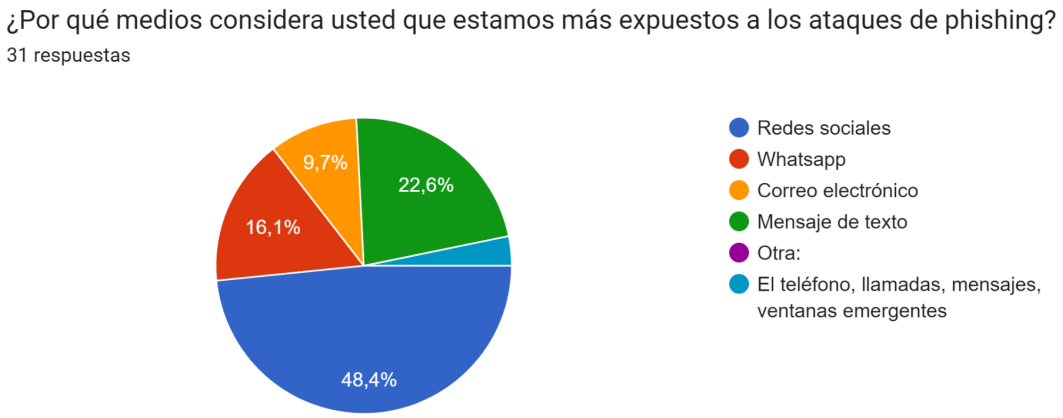


Figura 11. ¿Por qué medios estamos más expuestos a un cibercrimen?

La figura 11 nos muestra los canales que los usuarios consideran que suponen un mayor riesgo de ataques de phishing. En primer lugar se ubican las redes sociales con un 48.4%. En segundo lugar, los usuarios consideran al mensaje de texto con un 22.6%. En tercer lugar el whatsapp con un 16.1%, seguido del correo electrónico con un 9.7%. Por último, el teléfono, llamadas y ventanas emergentes con un 3.2.

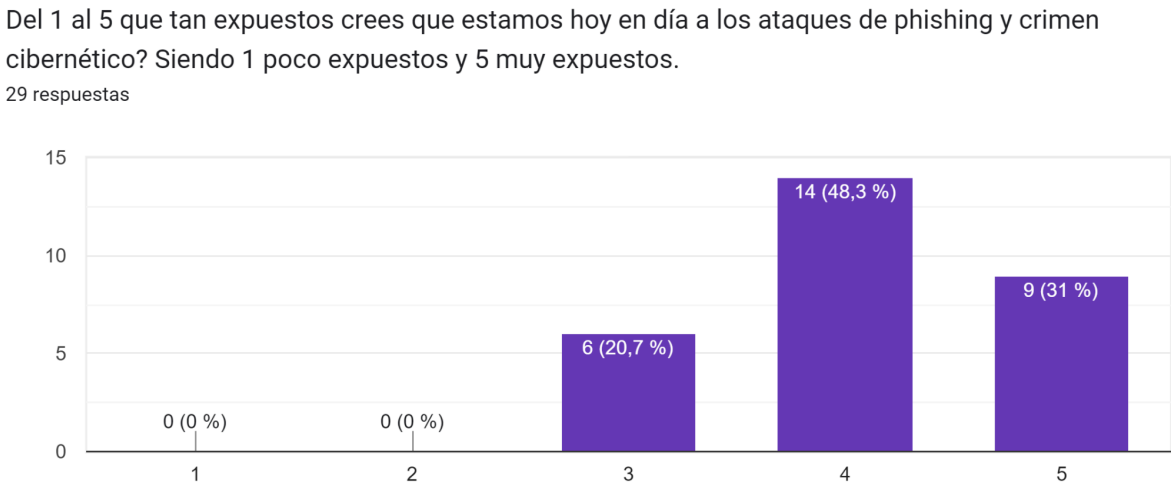


Figura 12. ¿Qué tan expuestos estamos ante un crímen cibernético y ataque de phishing?

La figura 12 nos muestra la percepción de los usuarios a ser víctimas de ataques de phishing. En primer lugar, el 31% considera que estamos muy expuestos a un ataque de phishing. El 48.3% considera que estamos expuestos a un ataque. Por último, el 20.7% considera que no estamos ni muy seguros ni muy expuestos a un ataque de phishing.

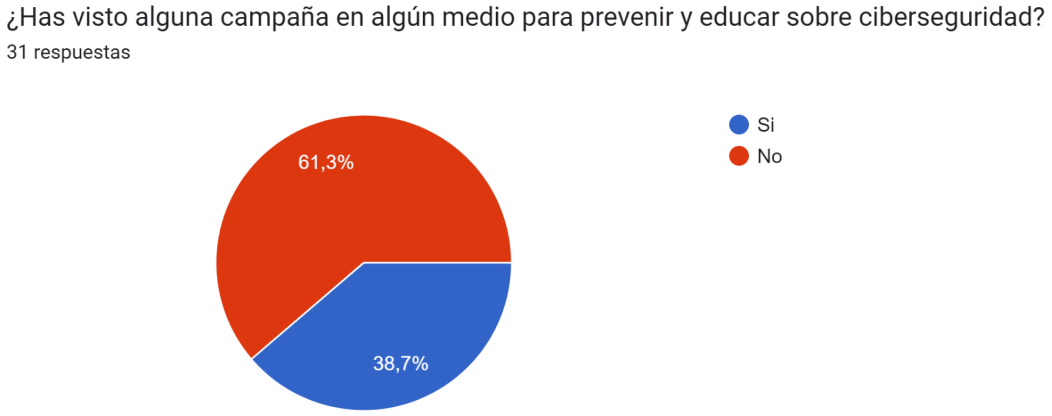


Figura 13. ¿Ha visto alguna campaña de ciberseguridad?

La figura 13 nos muestra si los usuarios han visto o no alguna campaña sobre ciberseguridad. El 61.3% indica que no ha visto ninguna campaña sobre ciberseguridad. El 38.7% indica que sí ha visto campañas de ciberseguridad.

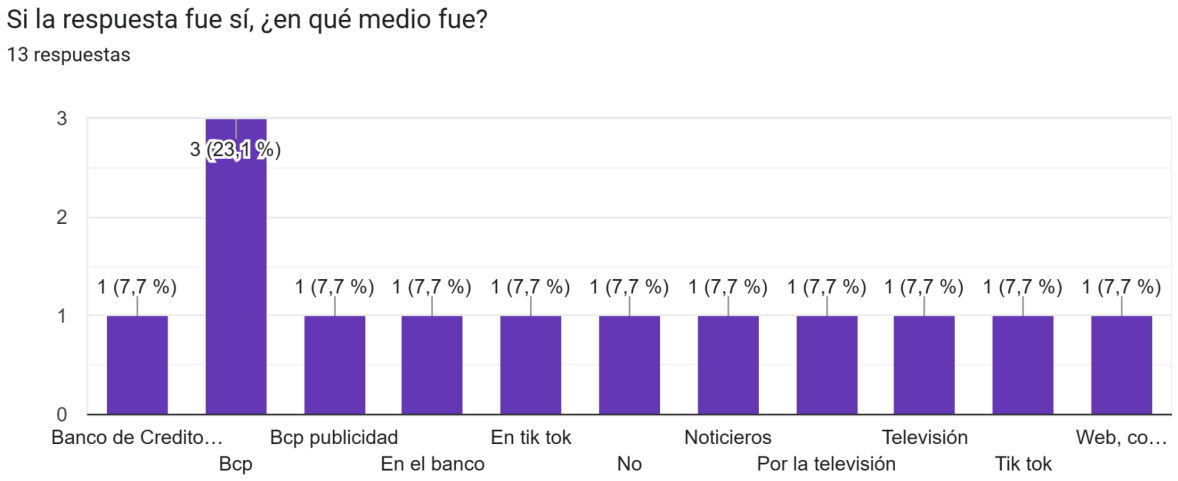


Figura 14. ¿Por qué canales has visto alguna campaña de ciberseguridad?

La figura 14 nos muestra los medios por los cuales los encuestados han visto alguna campaña de ciberseguridad. Como podemos apreciar, nuestros encuestados han visto campañas de ciberseguridad en los bancos, específicamente en el BCP.

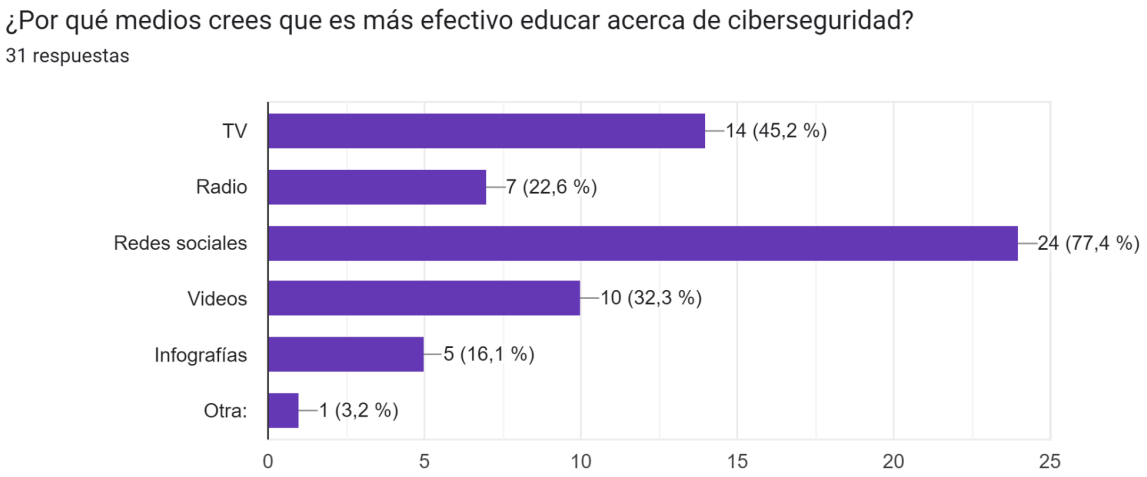


Figura 15. ¿Por qué medios consideras es más efectivo educar sobre ciberseguridad?

La figura 15 nos muestra los medios por los cuales los encuestados consideran que la educación en ciberseguridad es más efectiva. En primer lugar, se ubica las redes sociales con un 77.4%. En segundo lugar está la TV con un 45.2%. En tercer lugar, los usuarios sugieren que por medio de vídeos, con un 32.3%. En cuarto lugar tenemos a la radio, con un 22.6% y por último, los usuarios consideran otros canales para educar en temas de ciberseguridad.

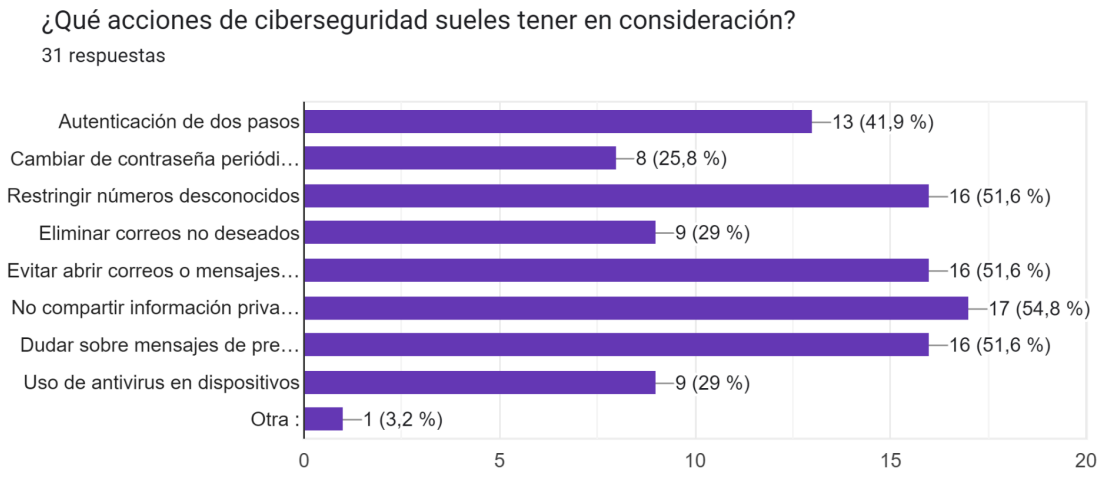


Figura 16. ¿Qué acciones acciones de ciberseguridad sueles tener en consideración?

La figura 16 nos muestra qué acciones de ciberseguridad suelen tomar los encuestados. En primer lugar tenemos no compartir información bancaria, con un 54.8%. Con un 51.6% los usuarios consideran tres acciones, las cuales son: restringir números desconocidos, evitar abrir mensajes y correos sospechosos y dudar de mensajes de premios y regalos. La siguiente acción más considerada es la autenticación de dos pasos con un 41.9%. Otras medidas que los usuarios consideran son: eliminar correos no deseados y hacer uso de antivirus en dispositivos, ambas con un 29%. A estas medidas le sigue cambiar de contraseña periódicamente con un 25.8%. Por último, los usuarios consideran otras medidas (3.2%).

4.2. Discusión de Resultados

Respecto a las preguntas de investigación aplicadas, se realizaron encuestas por medio de Google Forms donde los participantes del grupo estudiado mostraron que la mayoría no ha sido víctima de un ciberataque aún, por otro lado del grupo que sufrió algún ciberataque, señalaron que el canal con mayor incidencia de ciberdelincuencia fue Facebook Marketplace.

Los encuestados consideran que la educación en materia de seguridad informática puede ser más viable y/o efectiva si se realiza a través de las redes sociales. Un segundo grupo propone a la TV como medio para dicho propósito, y un tercer grupo considera que por

medio de videos la educación informática y de ciberseguridad puede ser la vía para lograr mejores resultados.

Encontramos que un alto índice de encuestados no han visto una campaña de ciberseguridad, del grupo que respondió que sí, en su mayoría resaltaron que en las entidades bancarias han visto por lo menos una campaña a favor de la ciberseguridad.

Los datos recopilados mostraron que los usuarios prefieren realizar sus compras online con tarjeta de débito/crédito y que en mayor medida, los canales de compras online más solicitados suelen ser plataformas internacionales (Amazon, Ebay, Aliexpress, Temu).

Finalmente, destacamos las encuestas realizadas nos dieron información sustancial para confirmar que gran parte de los encuestados consideran como muy seguros o bastante seguros a los canales de compras online, tanto locales como los gigantes del ecommerce.

4.3. Recomendaciones

El objetivo de la investigación fue comprobar que tan familiarizados están los internautas con la ciberseguridad y los ataques de phishing para poder conocer cuál sería el canal idóneo para difundir información sobre protección de datos. Buscamos que sean conscientes de los riesgos que están latentes con cada avance tecnológico, como lo son las tecnologías de la información y la inteligencia artificial. Precisamente esta última supone más riesgos que ventajas para los internautas, pues sus herramientas novedosas y sofisticadas son un arma poderosa en manos no solo de hackers sino de oportunistas del engaño.

Lo primero fue llevar a cabo una investigación de cuáles son los sitios ecommerce más solicitados por los compradores, si los consideran seguros o no, y cuál es el medio de pago más utilizado, a fin de que sean conscientes de los riesgos que conlleva el comercio electrónico.

Por último, recomendamos tanto a empresas, entidades bancarias y gubernamentales consolidar una propuesta de educación en ciberseguridad sólida que se materialice en todos

los niveles de la sociedad, medios de comunicación, redes sociales, instituciones públicas y privadas, centros de estudios, vía pública, a fin de lograr una cultura de la ciberseguridad que sea constante, vigilante, con la cuál el ciudadano tanto informado o no, pueda estar seguro de que los crímenes cibernéticos van a ser una prioridad, a fin de garantizar que las transacciones realizadas en el ciberespacio sean seguras, avaladas por los bancos y protegidas por todos los actores sociales.

Referencias

- Zambrano Rendón, Aura Dolores (2024). Impacto de la inteligencia artificial en los ciberataques https://www.itsup.edu.ec/myjournal/index.php/sinapsis/article/view/895/2078
- Barrantes Bernal,Cristian Camilo; Espitia Velásque, Snattan Andrey (2024). Proceso de phishingy pautas para la identificación de sitios web falsos https://revistas.uniss.edu.cu/index.php/pedagogia-y-sociedad/article/view/1745/4261
- Castro Crespo,José Domingo (2022). Elaboración de una herramienta de concienciación para dispositivos Android para evitar ser víctima de phishing https://repositorio.unican.es/xmlui/bitstream/handle/10902/26135/443388.pdf?sequence=1&isAllowed=y
- Calvo San José, Maria José (2022). La responsabilidad civil de los bancos en los delitos en los delitos de estafa por "phishing" Actualidad Jurídica Iberoamericana Nº 18, 1788- 1809 https://revista-aji.com/articulos/2023/18/AJI18_64.pdf
- *Juan Armando Gómez, (actualizado 03/05/24) Ingeniería social: 6 consejos para proteger a tu empresa de su impacto. Cyberblog. https://www.deltaprotect.com/blog/ingenieria-social.*
- *Panda Security, (28/12/2022). ¿Qué es la ingeniería social y cómo puedes protegerte de ella?. Educación Digital. https://www.pandasecurity.com/es/mediacenter/que-es-ingenieria-social/*
- *Microsoft, 2024¿Qué es el phishing? Seguridad de Microsoft, https://www.microsoft.com/es-es/security/business/security-101/what-is-phishing*
- *Apple, (27 de septiembre de 2024), Reconocer y evitar estrategias de ingeniería social, como los mensajes de suplantación de identidad (phishing), llamadas de soporte falsas y otras estafas https://support.apple.com/es-es/102568*

- *Luiza Pires (06/06/2024)¿Qué es un hacker y qué hace?.Cultura y Seguridad Digital. https://www.eset.com/latam/blog/cultura-y-seguridad-digital/que-es-un-hacker-y-que-hace/*
- *Mateo Kosinski (16/06/2024) ¿Qué es el hacking?.Temas. https://www.ibm.com/mx-es/topics/cyber-hacking*
- *Gregg Lindemulder, Matt Kosinski, (12/06/2024). ¿Qué es la ciberseguridad?. Temas. https://www.ibm.com/es-es/topics/cybersecurity*
- *Microsoft,(2024) Soporte Técnico.¿Qué es la ciberseguridad? https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390*
- *Norton, (08/08/2018) De qué manera distinguir el cibercrimen y protegerse. How to. https://lam.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime*
- *Kaspersky, (2024) ¿Qué es el cibercrimen? Cómo protegerse del cibercrimen. Tipos de amenazas. https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime*
- CAPACE (s.f) Reporte oficial de la industria ecommerce en Perú 5°edición https://drive.google.com/file/d/1iGYwamkoRRHR7JySArq5Zjmql07ay5v8/view
- OSIPTEL (s.f) Reporte estadístico 2023 Octubre N°9 https://cdn.www.gob.pe/uploads/document/file/6824663/5905886-reporte-estadistico-n-09-octubre-202.pdf?v=1724357307
- INEI (s.f) Estadísticas de las tecnologías de la información en los hogares 2021 Junio N°2 https://www.inei.gob.pe/media/MenuRecursivo/boletines/02-informe-tecnico-tic-i-trimestre-2021.pdf

Anexos

Anexo A. Encuesta sobre preferencias digitales

1. Edad
    - 18-25
    - 25-35
    - 35-45
    - 45-55
    - 55-99
    - Otros:
2. Sexo
    - M
    - F
    - Otro:
3. ¿Qué dispositivo sueles usar más para compras online?
    - Celular/tablet
    - Laptop/PC
    - Videoconsola
    - Apple TV, Amazon Firestick, Roku,
    - Nube
    - Otro:
4. ¿Qué tan seguro piensas que son los canales de compras online?
    - 1
    - 2
    - 3
    - 4
    - 5
5. ¿Qué método de pago sueles usar para compras online?
    - Tarjeta de crédito/débito
    - Transferencia bancaria

- Depósito
- Contraentrega
- Otra
- Otros:

6. ¿Qué sitio web de ecommerce sueles comprar?
    - Facebook Marketplace
    - Falabella/Ripley/OH/Cencosud
    - Mercado Libre
    - Amazon, Ebay, Ali Express, Temu
    - Otra:
7. ¿Ha sido víctima de un crimen cibernético, estafa, fraude, robo de dinero, suplantación, robo de datos?
    - Si
    - No
8. Si tu respuesta fue sí, cuéntanos brevemente el canal utilizado.
9. ¿Por qué medios considera usted que estamos más expuestos a los ataques de phishing?
    - Redes sociales
    - Whatsapp
    - Correo electrónico
    - Mensaje de texto
    - Otra:
    - Otros:
10. Del 1 al 5 que tan expuestos crees que estamos hoy en día a los ataques de phishing y crimen cibernético? Siendo 1 poco expuestos y 5 muy expuestos.
    - 1
    - 2
    - 3
    - 4
    - 5
11. ¿Has visto alguna campaña en algún medio para prevenir y educar sobre ciberseguridad?
    - Si

- No
- Otros:

12. Si la respuesta fue sí, ¿en qué medio fue?
13. ¿Por qué medios crees que es más efectivo educar acerca de ciberseguridad?
    - TV
    - Radio
    - Redes sociales
    - Videos
    - Infografías
    - Otra:
14. ¿Qué acciones de ciberseguridad sueles tener en consideración?
    - Autenticación de dos pasos
    - Cambiar de contraseña periódicamente
    - Restringir números desconocidos
    - Eliminar correos no deseados
    - Evitar abrir correos o mensajes sospechosos
    - No compartir información privada (bancaria)
    - Dudar sobre mensajes de premios y regalos.
    - Uso de antivirus en dispositivos
    - Otra :