UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

JUNIO 2023 - OCTUBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA
PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

“ANALISIS DEL ATAQUE DEL MODELO PHISHING EN LOS SISTEMAS INFORMATICOS Y BANCARIOS”

EGRESADA:

AMAIQUEMA CHUQUIANA EVELYN MAOLI

TUTOR:

ING. AGUIRRE RODRIGUEZ CARLOS GONZALO

AÑO 2023

RESUMEN

El uso constante de las tecnologías ha provocado que las personas sean expuestas a las vulnerabilidades que presentan los medios informáticos, provocadas por especialistas en sistemas que se dedican al ciberataque causando amenazas para obtener información confidencial, existen varios tipos de ciberataques entre los más utilizados están malware, el phishing y el ransomware.

El phishing es uno de los métodos de ataque más comunes y efectivos en el ámbito cibernético. Los atacantes utilizan tácticas engañosas para robar información confidencial, como credenciales bancarias y datos personales, lo que puede resultar en pérdidas financieras y robo de identidad.

Mediante el análisis de este estudio de caso se espera poder cumplir el objetivo propuesto, que es el analizar el ataque del modelo phishing en los sistemas informáticos y bancarios, mediante el método de investigación descriptiva el cual nos permitirá describir las técnicas, estrategias y evolución del phishing, perimiéndonos buscar una solución para salvaguardar la información personal y financiera por medio de la ciberseguridad.

Durante el desarrollo de la investigación se indicarán los impactos del método phishing en los sistemas informáticos y bancarios a nivel mundial, también se detallarán resultados de encuestas realizadas por diferentes tipos de personas.

Palabras claves

Ciberataques, Sistemas Informáticos, Programación y usuario.

SUMMARY

The constant use of technologies has caused people to be exposed to the vulnerabilities presented by computer media, caused by system specialists who are dedicated to cyberattacks, causing threats to obtain confidential information. There are several types of cyberattacks, among the most used are malware, phishing and ransomware.

Phishing is one of the most common and effective attack methods in the cyber sphere. Attackers use deceptive tactics to steal sensitive information such as banking credentials and personal data, which can result in financial loss and identity theft.

Through the analysis of this case study, it is expected to be able to meet the proposed objective, which is to analyze the attack of the phishing model on computer and banking systems, through the descriptive research method which will allow us to describe the techniques, strategies and evolution of the phishing, allowing us to seek a solution to safeguard personal and financial information through cybersecurity.

During the development of the research, the impacts of the phishing method on computer and banking systems worldwide will be indicated, and the results of surveys carried out by different types of people will also be detailed.

Keywords

Cyberattacks, Computer Systems, Programming and user.

INTRODUCCION

En la actualidad la era del mundo digital, ha tenido un gran impacto en la sociedad y en la vida de cada persona lo que conlleva a ser parte de la rutina diaria, es por eso que los sistemas informáticos y sistemas bancarios han evolucionado tanto en grandes y pequeñas empresas de tal manera que realizan procesos transacciones y gestionar finanzas personales y empresariales. Sin embargo, esta creciente interconexión y dependencia en la tecnología ha dado lugar a los aumentos de amenazas cibernéticas, en las cuales destaca el sigiloso y pernicioso ataque del phishing.

Para la comprensión de este análisis es necesario tener en cuenta estos puntos importantes ¿Qué es el phishing?, ¿Cuáles son las técnicas?, ¿Qué impacto tiene en los sistemas informáticos y sistemas bancarios?, el phishing es considerada una técnica que suplantan la identidad de compañías u organismos públicos solicitando información personal y bancaria al usuario.

El principal problema que conlleva al estudio de este método es la detención ineficiente de ataques de phishing mediante correos electrónicos, ya que los usuarios por su falta de conocimiento son víctimas al momento de hacer un clic en enlaces maliciosos que son creados por atacantes que emplea técnicas de ingeniería social

El impacto de estos ataques es significativo. En el ámbito bancario, se traduce en robos de fondos y suplantación de identidad, mientras que en los sistemas informáticos puede resultar en la infiltración de malware y el compromiso de la infraestructura. Los perpetradores utilizan técnicas como el "spear phishing" y el "pharming", además de la manipulación telefónica o "vishing"

En los últimos años se ha considerado que el método del phishing ha sido una de las principales técnicas que han sido utilizadas por los ciberdelincuentes para introducirse en las organizaciones del todo el mundo, siendo los más afectados los sectores financieros, educación y gobierno.

El propósito de dicha investigación es comprender a profundidad esta amenaza cibernética, las implicaciones en la seguridad de los datos financieros y la integridad de los sistemas informáticos, identificando las tácticas y estrategias utilizadas por los ciberdelincuentes que usa este método para conseguir sus propios beneficios, el cual se realizará mediante un análisis exhaustivo basándonos en objetivos claros, y un buen desarrollo investigativo para obtener una información más específica sobre estos ataques.

DESARROLLO

El phishing es una técnica de la ingeniería social, cuyo objetivo consiste en el envió de correo electonicos que suplantan una identidad de compañías u organizaciones públicas, dichos correos suelen incluir errores gramaticales, logotipos o imagen que represente la entidad de una empresa, también pueden contener archivos adjuntos infectados con software maliciosos que lleven al usuario a realizar las acciones que solicitan estos email, cumpliendo de esta manera con el propósito de infectar el equipo y robar información personal. (Banco Bilbao Vizcaya S.A, 2023).

La presencia de estas amenazas cibernéticas ha sido parte de la evolución tecnológica, teniendo un gran impacto en los tiempos de pandemia motivo por el cual, los criminales aprovecharon el cambio del modelo laboral, como el teletrabajo que permite a los empleados conectarse remotamente a los sistemas de sus organizaciones, las compras en líneas y las grandes transacciones bancarias de corporaciones y gobierno, por este motivo se generó graves daños a empresas y personas en todo el mundo, siendo el phishing unos de los principales atacantes con mayor potencia en América Latina. (Steve, 2023)

Según datos del (Internet Crime Complaint Center del FBI), sobre el impacto económico del phishing se pudo registrar en el último año un incremento del 5% en intentos de phishing. Estos pudieron haber resultado en pérdidas cercanas a los 10.000 millones de dólares.

Características

El engaño es uno de las principales tácticas engañosas para convencer a la víctima que esta interactuando con una fuente confiable. Pero que, al final, acaban hurtando su información y suplantando su identidad sin que este preste su consentimiento.

Tácticas de ingeniería social: son utilizadas para ganarse la confianza de las víctimas, para obtener información con la finalidad de utilizarlos en negocios jurídicos y comprometer la seguridad de los bancos exponiendo en riesgo el comercio electrónico, ya que lleva a la pérdida de confianza hacia el sistema bancario, lo cual es esencial para que el mercado funcione.

Ubicación de los delincuentes: debido a las ventajas tecnológicas, es difícil ubicar geográficamente a estas personas ya que cuentan con la capacidad de trabajar por diferentes cuentas personales o bancarias permitiéndoles escaparse de la de las sanciones legales penales correspondientes y, en consecuencia, dificulta el uso de soluciones jurídicas.

A medidas que la tecnología avanza, las técnicas de phishing son cada vez más sofisticada, para prevenir con éxito es importante proporcionar a los usuarios conocimientos solidos sobre las técnicas del phishing que utilizan los delincuentes. (Panduru, 2022).

Fases

Fase de planificación: En esta fase el atacante decide quién será su víctima y a que organismo o empresa suplantará, utilizando varias técnicas como el envío masivo de correos electrónicos hasta conseguir información valiosa, esta etapa es considerada “el

cebo” porque convence a una persona con una promesa engañosa que apela a su curiosidad o codicia.

Fase de preparación: Una vez obtenida la información necesaria el delincuente prepara el “anzuelo” creando información de tipo alarmante que comprometa al usuario seguir un enlace ingresando datos de algunas de su cuenta de manera urgente, cuyos datos son enviados a una página en la que son recopilados datos de la persona.

Fase del ataque (captura): En esta etapa se realiza el ataque real que dependiendo del tipo de ataque el delincuente realizara diferentes acciones. Por ejemplo, si utilizaron una página de destino para obtener información de la víctima, el delincuente puede proceder a iniciar sección y comenzar a enviar más correo phishing a los contactos del dueño de la cuenta utilizada. (Cicpc, 2022) .

Tipos phishing.

Spear Phishing

Su función consiste en envío de correo electrónico aparentemente de una fuente confiable dirigida a personas, organizaciones o empresas específicas, donde dirige al destinatario a un sitio web falso con gran cantidad de malware utilizando la táctica específica para captar la atención de la víctima.

McKinsey señala que el número de ataques de spear phishing se ha multiplicado casi por siete veces desde el inicio de la pandemia. aprovechando de la tendencia del teletrabajo, los atacantes de spear phishing robaron más de 100 millones de dólares de Facebook y Google haciéndose pasar por proveedores legítimos y engañando a los empleados para que pagaran facturas fraudulentas. (IBM, 2023)

Secuestro de sesión (sesión sniffing)

Este tipo de ataque funcionan mediante la forma en que los dispositivos transmiten datos que generalmente son divididas en pequeñas unidades llamadas “paquetes” y a su vez se envían a través de la red llegando a su destino final. Esto permite al hacker interceptar dichos paquetes y analizar su contenido utilizando un software especializado llamado “sniffer o analizador de web”, que son instalados en el dispositivo del atacante, registrando y analizando todos los paquetes de datos que se transmiten buscando información útil, como contraseñas, nombres de usuario, información de tarjetas de crédito u otra información confidencial, teniendo también la posibilidad de modificar los paquetes de datos y enviar información falsa a la red, lo que puede causar aún más daño. (impulso 06, 2023).

Vishing

Consiste en la combinación de palabras voice(voz) y phishing, donde el delincuente suplantan la identidad de personas u organizaciones que guardan algún tipo de relación con la víctima y las usan de excusa para establecer comunicación y engañarlas por medio de llamadas telefónicas y poder robar información personal y bancaria. (tusdatos.co, 2022).

Smishing

Se envían a teléfonos celulares un SMS ofreciendo algún tipo de beneficios, premio u oportunidad laboral, esto es aplicado actualmente por medio de las redes sociales. (Luis, 2022)

Pharming

Consiste en una nueva técnica y más complicada que utilizan los hackers para la infiltración de ordenadores individuales accediendo a un sitio web para cambiarlo por uno falso mediante los cambios en los DNS. (panda, 2022).

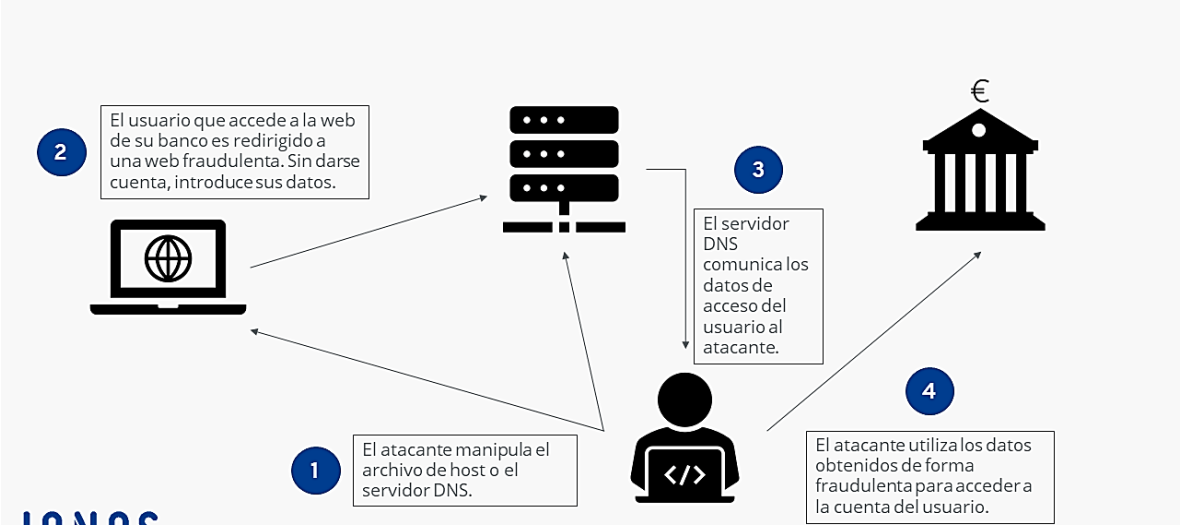


Ilustración 1: desarrollo de un ataque de pharming.

Fuente: imagen extraída de la página la empresa Ionos.

Sectores más vulnerables ante ataques de Phishing

Unos de los mayores problemas que tienen las empresas de distintos sectores, es que son más propicios a pinchar en archivos adjuntos de correo o hacer clicks en links fraudulentos, acostumbrados a trabajar constantemente con distintitos tipos de correos, convirtiéndolos en principales víctimas de estos ataques.

Los tipos de sectores más propensos en recibir ataques phishing, son:

- Consultorías
- Vestimenta y accesorios
- Educación
- Tecnología
- Conglomerados

Datos preliminares de (IT Digital Media Group, 2023), menciona que el sector de educación fue el más atacado durante el año 2022 con un aumento del 576%, seguido por el financiero y el gubernamental en cambio los sectores minoristas y mayorista experimentan un descenso del 67%.

Según (Daniela, 2020), las empresas que han sufrido estos problemas de robo de información, se encuentran orientados a temas administrativos, salud o gestión de calidad.

(Interbel , s.f.) es una empresa dedicada a dar soluciones y software de alta calidad para el email, Work Management y Ciberseguridad, menciona distintas maneras de cómo protegernos del ciberataque

1. Utilice únicamente servicios bancarios en línea en dispositivos que conoce y en los que confía.
2. No envié números de cuentas, números de seguros social, tarjetas de créditos, etc. Las compañías legitimas nunca piden esto por correo electrónico.
3. Si se trata de una página de compras en línea verificar que este certificada bajo los protocolos SSL Secure Sockets Layer (Capa de sockets seguros).
4. Evitar Spam, son correos electrónicos considerados masivos por la gran cantidad de información maliciosa, para dañar el sistema informático.

Phishing utilizando SET (Social- Engineer Toolkit) en Kali Linux.

Los hackers al igual que los programadores web, utilizan varios tipos de lenguaje de programación, La elección de las tecnologías depende de sus objetivos y de las habilidades que posean. A pesar de que los distintos tipos de programación son seguros, los expertos en

tecnología crean paginas bajo códigos maliciosos con el fin de conseguir sus objetivos de estafar información confidencial.

Uno de los mecanismos usados en la creación de páginas web no legitimas es el SET (Social-Engineer Toolkit), conjunto de herramientas de la ingeniería social especialmente diseñado para realizar ataques avanzados a la parte más vulnerables. SET integra muchas funciones de Metasploit (proyecto de código abierto), por lo tanto, es necesario instalarlo en un sistema operativo que permita explotar brechas de seguridad como lo es Kali Linux que es una distribución de Linux basado en Debian destinada a pruebas de penetración y auditoría de seguridad.

Para que SET sea ejecutado debe ser instalado un lenguaje de programación, el intérprete de Python es una de las opciones ya que ejecuta línea por línea el código fuente convirtiéndolo a un lenguaje de máquina.

Ingeniería social

Es el uso de distintas técnicas de manipulación para cumplir con el objetivo de conseguir información valiosa por parte de las víctimas. Se clasifican según la función de numero de comunicaciones que realiza el ciberdelincuente para cumplir con su propósito.

Hunting: Es dirigida mediante una sola comunicación en ataques phishing o distribución de malware.

Farming: esta técnica es utilizada en sextorsión, fraude, y RR. HH, que consiste en enviar más de una comunicación para cumplir con el objetivo de atacante. (AITANA SOLUCIONES ERP Y CRM, 2023).

Sistemas Informáticos

Es un conjunto de elementos físicos y lógicos encargados de recibir, procesar y guardar información compuesta por una parte física (hardware) y lógica (software), permiten acceder a diversas funcionalidades útiles como lo es en el ámbito empresarial que se encargan de automatizar procesos, delegar actividades repetitivas.

Una de las principales desventajas que tienen los sistemas informáticos, son sus altos costo de instalación, es por ellos que muchas empresas optan por uno básico presentando problemas técnicos el cual conlleva a distintos tipos de ataque de virus.

El phishing puede tener un impacto significativo en los sistemas informáticos y en las organizaciones. A continuación, se detallan factores importantes del phishing en los sistemas informáticos

- Robo de credenciales
- Acceso no autorizado
- Distribución de Malware
- Pérdidas financieras
- Daños a la reputación
- Costos de recuperación
- Amenazas persistentes

El investigador Mario Micucci, de seguridad informática de ESET compañía dedicada a la ciberseguridad para América Latina, detallo que los delincuentes de ataques phishing han logrado estafar a sus víctimas por redes sociales, buscadores, plataformas de streaming y aplicaciones y aplicaciones de mensajería como WhatsApp, teniendo un aumento en regiones como Perú, México, Ecuador, Argentina. (Mauricio, 2022).

Ilustración 2: Resultados sobre ataques phishing a medios informáticos en América latina.
Fuente: Security Report Latinoamérica 2022.

Ilustración 3: Empresas que sufrieron ataque phishing en el tercer trimestre del 2022.

Fuente: Datos extraído de la página McPro (muy computer pro).

Sistemas Bancarios

Es el conjunto de instituciones (bancos), dedicadas a la parte financiera de una persona o empresa, Su actividad consiste canalizar el ahorro de los prestamistas y dar seguridad a los

movimientos de dinero y a los propios sistemas de pago. Estos sistemas son fundamentales para el funcionamiento del sector bancario y desempeñan un papel crucial en la gestión de cuentas, la seguridad de los datos, la transferencia de fondos, la gestión de préstamos y muchas otras operaciones financieras.

Los sistemas bancarios están compuestos por diferentes aspectos que son:

Sistemas de Core Baking: Se utiliza para la incorporación y apertura de una cuenta y procesamiento de transacciones, su sistema consiste en gestionar funciones claves para el negocio de los bancos.

Banca en línea y Móvil: Los sistemas bancarios modernos permiten a los clientes acceder a sus cuentas y realizar transacciones a través de aplicaciones móviles y plataformas en línea.

Cajeros Automáticos (ATM): Los cajeros automáticos son parte integral de los sistemas bancarios y permiten a los clientes retirar efectivo, consultar saldos y realizar otras transacciones las 24 horas del día.

Tarjetas de Débito y Crédito: Los sistemas bancarios gestionan la emisión y el procesamiento de tarjetas de débito y crédito, lo que permite a los clientes realizar compras y pagos en todo el mundo.

Gestión de Riesgos: Los bancos utilizan sistemas avanzados de gestión de riesgos para evaluar la solvencia crediticia de los clientes, detectar actividades sospechosas y garantizar la seguridad de las transacciones.

Transferencias Internacionales: Los sistemas bancarios facilitan las transferencias de fondos entre cuentas nacionales e internacionales, lo que es esencial para el comercio internacional y las transacciones financieras globales

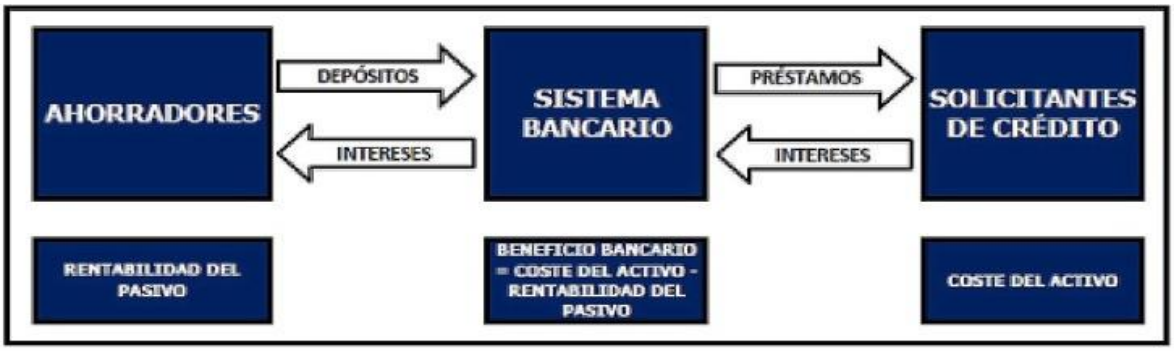


Ilustración 3: Esquema de funcionamiento del Sistema Bancario.

Fuente: Imagen extraída de la página AMCES (ASOCIACIÓN ESPAÑOLA DE MENTORING).

Estos sistemas bancarios se enfrentan a distintos tipos de riesgo como el de mercado, crédito, liquidez y el más importante el riesgo operativo que consiste a las perdidas financiera por mala gestión o fallos tecnológicos que se da cuando se emplea un software que no está actualizado, afrontando una serie de problemas, como caídas de los sistemas informáticos o ciberataque. (Antander Universidades, 2022).

El phishing bancario es la técnica utilizada por los delincuentes para el robo de dinero de las cuentas y tarjetas, funcionan bajo el uso de correos electrónicos, mensajes de texto, llamadas telefónicas y redes sociales creando perfiles y páginas falsas para engañar a los usuarios y obtener su información bancaria.

Cómo afecta el phishing bancario al sector bancario y a los clientes.

El phishing bancario puede tener un impacto significativo tanto en el sector bancario como en los clientes. Los bancos pueden tener grandes pérdidas de dinero y sufrir daños en su reputación llevándolos a una responsabilidad legal por parte de los clientes, también tendrían perdidas de los ingresos en la institución financiera debido a los reembolsos que tendría que hacer a los clientes por dinero perdido o robado por el phishing

En los clientes les ocasionaría la perdida financiera y la confianza en la entidad bancaria, el robo de identidad utilizadas por los estafadores para abrir cuentas fraudulentas o cometer otros delitos en nombre de la víctima, motivo por el cual lleva a la persona a una angustia y estrés emocional al saber que les tomara tiempo y esfuerzo en recuperar su cuenta bancarias (Tirant, 2023).

Ciberseguridad

Es la practica para proteger los equipos o sistemas informáticos ante posibles amenazas digitales, su objetivo principal generar confianza entre clientes, proveedores y el mercado en general salvaguardando información importante de una organización,

De acuerdo a los expertos de Information Systems Audit and Control Association (ISACA) la seguridad informática se define como "una capa de protección para los archivos de información".

Como funciona la ciberseguridad

Esta función radica en los expertos en seguridad informática, el cual consiste en evaluar los riesgos de los sistemas informáticos, almacenamiento de datos, entre otros distintos dispositivos conectados a una red, creando un macro de seguridad integral e implementando medidas protectoras en la organización.

Un especialista en ciberseguridad trabaja junto con otras personas para crear varias capas de protección contra posibles amenazas en los puntos de acceso a datos, buscando anomalías en las infraestructuras de TI que existe en una empresa, permitiéndoles llegar a un análisis de dicho problema para la solución de recuperar datos después de un evento.

Tipos de ciberseguridad

- Seguridad en la red: Se la utiliza para los equipos conectados a una red, para la regular el acceso de los usuarios y administrar los permisos es necesario utilizar el firewall, basado en proporcionar un control detallado del tráfico de red.
- Seguridad en la nube: Describe las medidas para proteger los datos y aplicaciones que se ejecuten en la nube. Una estrategia sólida de seguridad en la nube implica la responsabilidad compartida entre el proveedor de nube y la organización.
- Seguridad de IoT: Se refiere al internet de las cosas, tiene como características la constante conectividad hacia el internet y los posibles errores ocultos que tiene un software, esto presentan un riesgo en la seguridad, por tal motivo es importante introducir política de protección en la infraestructura de red para evaluar y mitigar los posibles riesgos de los distintos dispositivos iot.
- Seguridad de los datos: Protege la seguridad de los datos con un sistema solido de almacenamiento y una transferencia segura de datos, por ejemplo AWS Nitro System sistema diseñado para la confidencialidad del almacenamiento y la restricción del acceso de operadores.
- Seguridad de las aplicaciones: están dirigidos a los programadores de software, cuya función es de crear códigos seguros para evitar errores que puedan aumentar los riesgos de seguridad. (Amazon Web Services, s.f.).

Componentes para una estrategia de seguridad

Una estrategia básica para la seguridad consiste en:

Las personas: la falta de conocimiento acerca de los riesgos informático en una organización provoca a que los trabajadores sean víctima de estos ataques. Es importante la formación y educación de los empleados con respecto a los principios de la seguridad informática, reduciendo riesgos de descuido que pueden llevar a casos no deseados.

Procesamiento: El equipo de especialistas crea un macro de seguridad solido para el monitoreo de las vulnerabilidades de la TI, garantizando la recuperación inmediata de información ante posible incidencia de seguridad.

Tecnología: existen distintos de software para la protección de datos como el firewall, antivirus, filtrado DNS o la seguridad de confianza Zero Trust, modelo de seguridad que permite al usuario la identificación antes de acceder a las aplicaciones datos y otros sistemas

Tabla 1: Detección de Phishing a través de herramientas antivirus

Antivirus	Avast	Kaspersky	AVG	Norton Antivirus	ESET
Phishing Correos electrónicos Detectado	92.3%	87.7%	91.8%	37.4%	7.3%
Phishing Correos electrónicos no Detectado	7.7%	12.3%	8.2%	62.6%	92%7
Enlaces detectados en Navegador	80%	81.08%	60%	98%	98%

Fuente: Datos extraídos de la revista cubana de Ciencias Informáticas.

Análisis: Según los porcentajes mostrados en la tabla 1, se pudo ver que son resultados favorables para la detección de phishing de manera automática, lo que nos indica que es

muy seguro la implementación de estos antivirus para la protección de los datos o información.

CONCLUSIONES

El ataque phishing y otros métodos de agresión dentro del campo informático, abarca mucha información, por lo que son considerados técnicas que frecuentemente evolucionan con el pasar de los años.

Durante la investigación se pudo analizar que el phishing, es la técnica más utilizada en la ingeniería social, debido a las varias formas que presenta al momento de operar especialmente atacando a varias empresas a nivel mundial.

Con respecto al ataque de phishing en los sistemas informáticos se pudo determinar que el mayor impacto que tuvo fue durante la pandemia, debido a la modalidad de trabajo que se presentó en esos momentos, afectando sistemas de teletrabajo, compras en línea e incluso la suplantación de sitios web de organizaciones aparentemente confiables para la obtención de datos personales. En los sistemas bancarios fue necesario realizar resumen de cómo están compuestos y cuál es el funcionamiento básico de un sistema dentro de una empresa financiera, para poder llegar al análisis de como los atacantes crean diversos métodos para hacer caer a la víctima y que está, a su vez genere datos como numero de cuentas o tarjetas de créditos.

Las herramientas utilizadas para este estudio proporcionan la información suficiente para poder entender con más facilidad sobre las características, fases y tipos de phishing

que existen, aunque es muy recomendable estar en constante actualización para ver los avances que sigue teniendo en diferentes sectores empresariales y así prevenirnos de sus nuevas técnicas.

Para la seguridad de las empresas y datos personales, fue necesario incluir información sobre la seguridad informática que consiste en la práctica de proteger una infraestructura computacional dentro de una organización.

Con los resultados obtenidos en la elaboración de este caso de estudio se concluye, con el cumplimiento del objetivo propuesto acerca del análisis ataque phishing en los sistemas informáticos y bancarios.

REFERENCIAS

AITANA SOLUCIONES ERP Y CRM. (16 de Febrero de 2023). *Aitana*. Obtenido de https://blog.aitana.es/2023/02/16/ataque-de-ingenieria-social-que-es-fases-y-como-identificarlo/

Amazon Web Services. (s.f.). *aws*. Obtenido de https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20pr%C3%A1ctica,cliente%20y%20cumplir%20la%20normativa.

Antander Universidades. (29 de junio de 2022). *becas-santander*. Obtenido de https://www.becas-santander.com/es/blog/riesgos-financieros.html

Banco Bilbao Vizcaya S.A. (7 de Marzo de 2023). *bbva*. Obtenido de https://n9.cl/pgv24

Cicpc. (22 de Agosto de 2022). *Delitos Informaticos*. Obtenido de https://delitosinformaticos.cicpc.gob.ve/procesos-de-un-ataque-de-phishing/

Daniela, G. (7 de Octubre de 2020). *Interbel*. Obtenido de https://www.interbel.es/sectores-vulnerables-phishing/

IBM. (8 de febrero de 2023). *ibm*. Obtenido de https://www.ibm.com/mx-es/topics/spear-phishing

impulso 06. (9 de febrero de 2023). *impulso 06*. Obtenido de https://impulso06.com/ataques-sniffer-que-son-y-como-protegerte/

Interbel . (s.f.). *interbel.es*. Obtenido de https://www.interbel.es/sectores-vulnerables-phishing/#:~:text=Entre%20los%20grupos%20que%20m%C3%A1s,salud%20o%20gesti%C3%B3n%20de%20calidad

ionos. (11 de 02 de 2020). *ionos.es*. Obtenido de https://n9.cl/0uklj

IT Digital Media Group. (21 de Abril de 2023). *It Digital Security*. Obtenido de https://www.itdigitalsecurity.es/actualidad/2023/04/los-ataques-de-phishing-se-incrementaron-a-nivel-mundial-casi-un-50-en-2022

Luis, R. (2022). *El Phishing como riesgo informático.* Guayaquil: Microsoft® Word para Microsoft 365.

Mauricio, H. (26 de octubre de 2022). *forbes*. Obtenido de https://n9.cl/4bzwm

panda. (19 de Septiembre de 2022). *pandasecurity*. Obtenido de https://www.pandasecurity.com/es/mediacenter/seguridad/pharming/

Panduru, D. (19 de Abril de 2022). *attacksimulator.es*. Obtenido de https://n9.cl/9rm4i

Sergio, D. (28 de Octubre de 2022). *MC PRO*. Obtenido de https://www.muycomputerpro.com/2022/10/28/dhl-microsoft-linkedin-pishing

Steve, R. (10 de Julio de 2023). *manageengineblog*. Obtenido de https://n9.cl/yu4d1v

Tirant. (27 de Marzo de 2023). *Tirant lo blanch*. Obtenido de https://tirant.com/noticias-tirant/noticia-phishing-bancario-abogados-deben-saber/#:~:text=El%20phishing%20bancario%20es%20una,de%20sus%20cuentas%20y%20tarjetas.

tusdatos.co. (9 de diciembre de 2022). *tusdatos.co*. Obtenido de https://n9.cl/uvpe9

ANEXOS

En las encuestas se realizaron las siguientes preguntas a 20 personas.

1. Sabias usted, que puede ser víctima de ataques cibernéticos mediante correos electonicos, mensajes de texto, llamadas etc.

- SI
- NO

2. ¿Ha recibido correos electrónicos o mensajes sospechosos que afirmaban ser de su institución bancaria solicitando información personal o financiera?

- SI
- NO

3. Sabía usted, que el "Phishing" es un método de ataque cibernético que roba información personal mediante correos y redes sociales.

- SI
- NO

4. ¿Sabe cómo reconocer señales de phishing en correos electrónicos o mensajes? Por ejemplo.

- SI
- NO

5. Con respecto al ejemplo anterior.

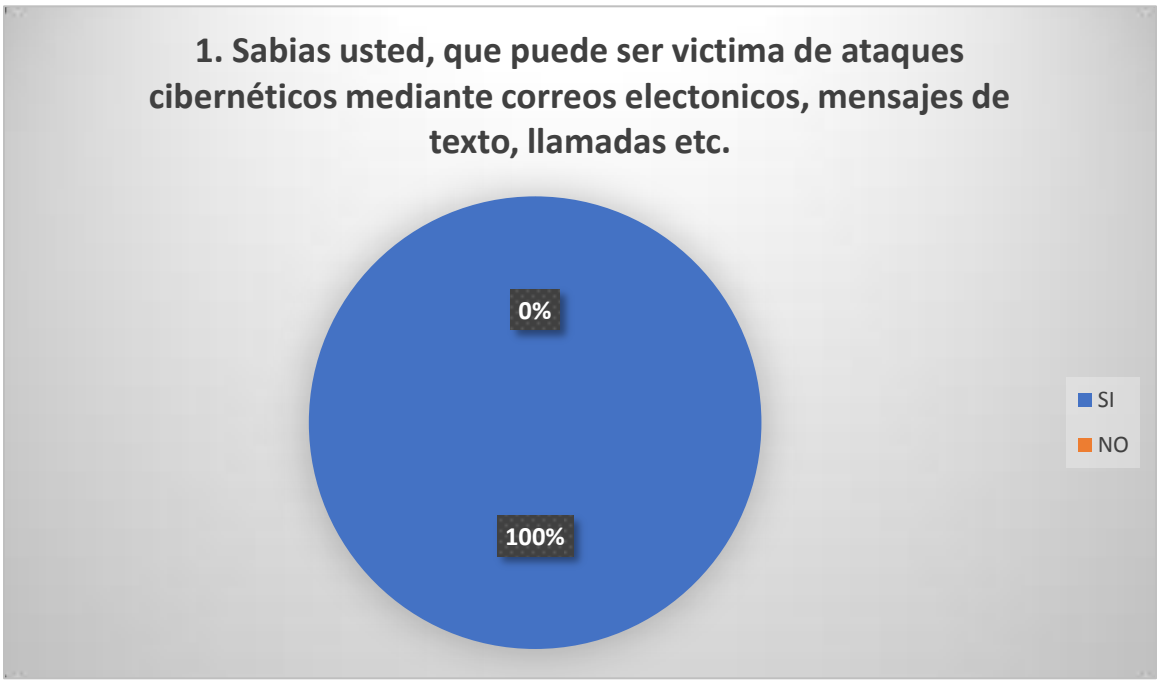
¿Ha compartido información personal o financiera en esos tipos de correo electrónico?

- SI

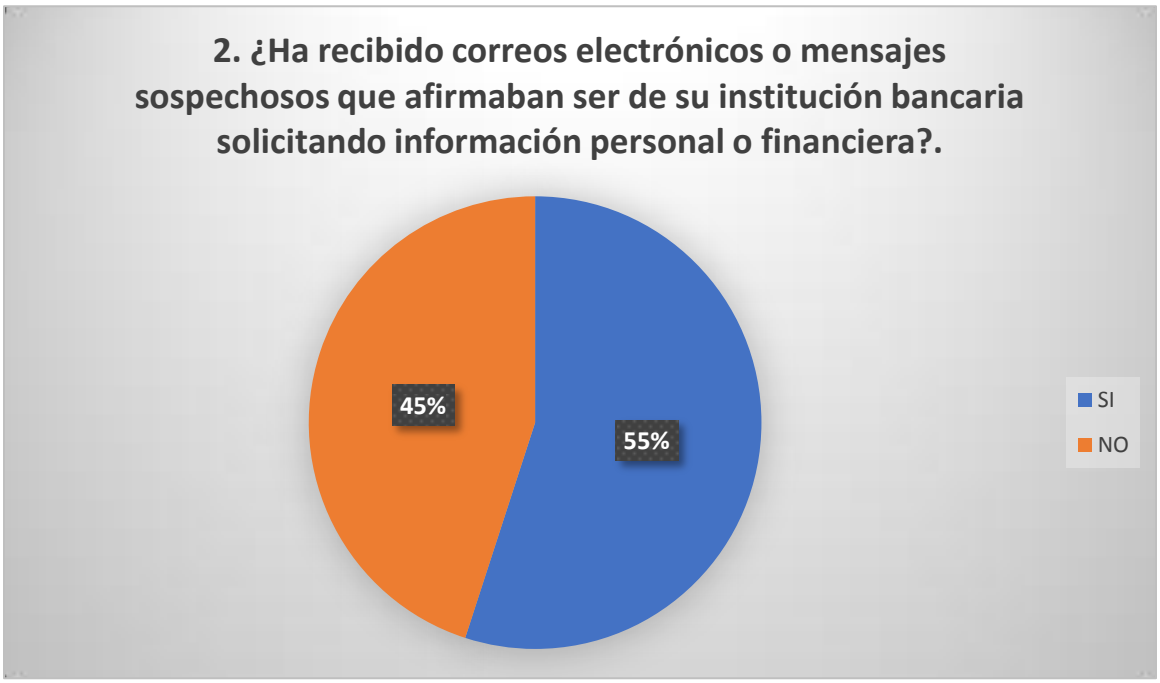
- NO

5. **Te gustaría recibir programas o capacitaciones de seguridad cibernética, sobre cómo detectar y prevenir ataques de phishing en su lugar de trabajo o institución financiera.**

- SI
- NO

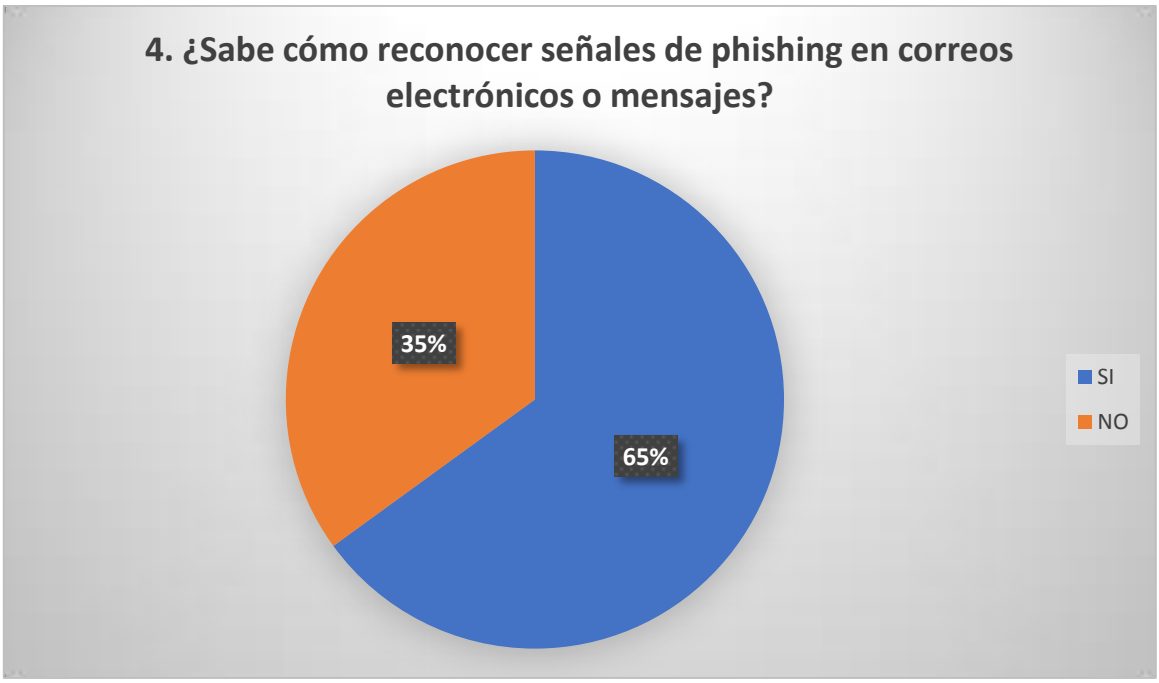


En la primera pregunta, el total de las 20 personas encuestadas respondieron a que conocen sobre los ataques cibernéticos.

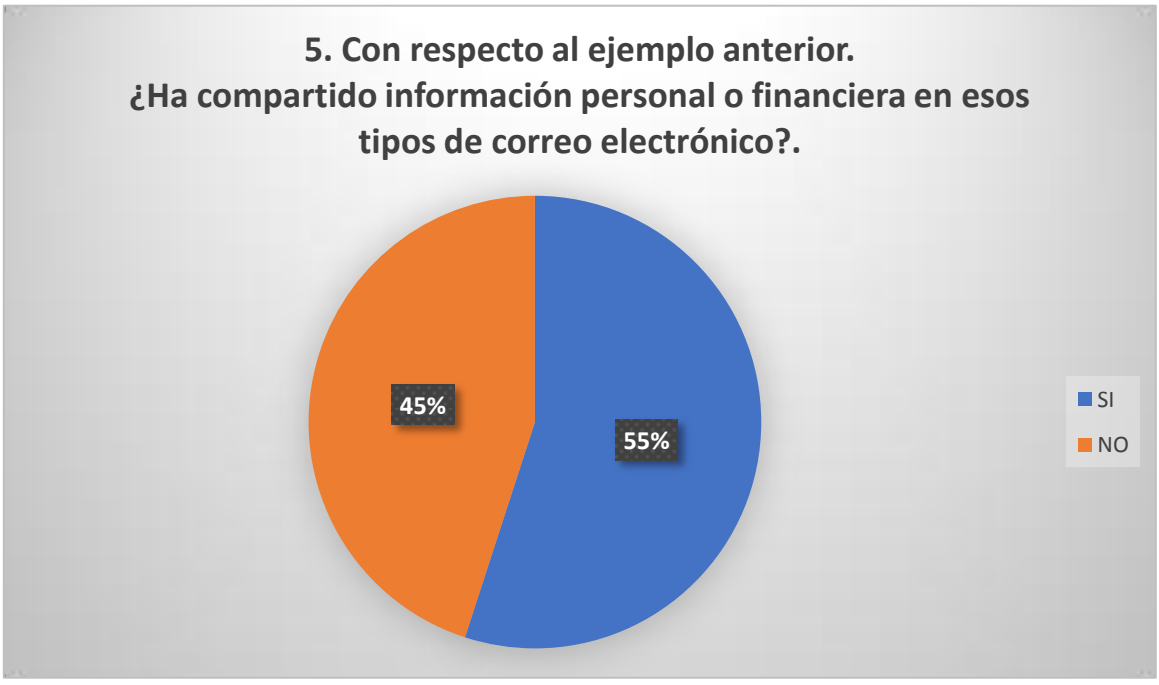


Con respecto a la segunda pregunta, el 55% afirman que han recibido tipos de ataques cibernéticos mediante correos electrónicos.

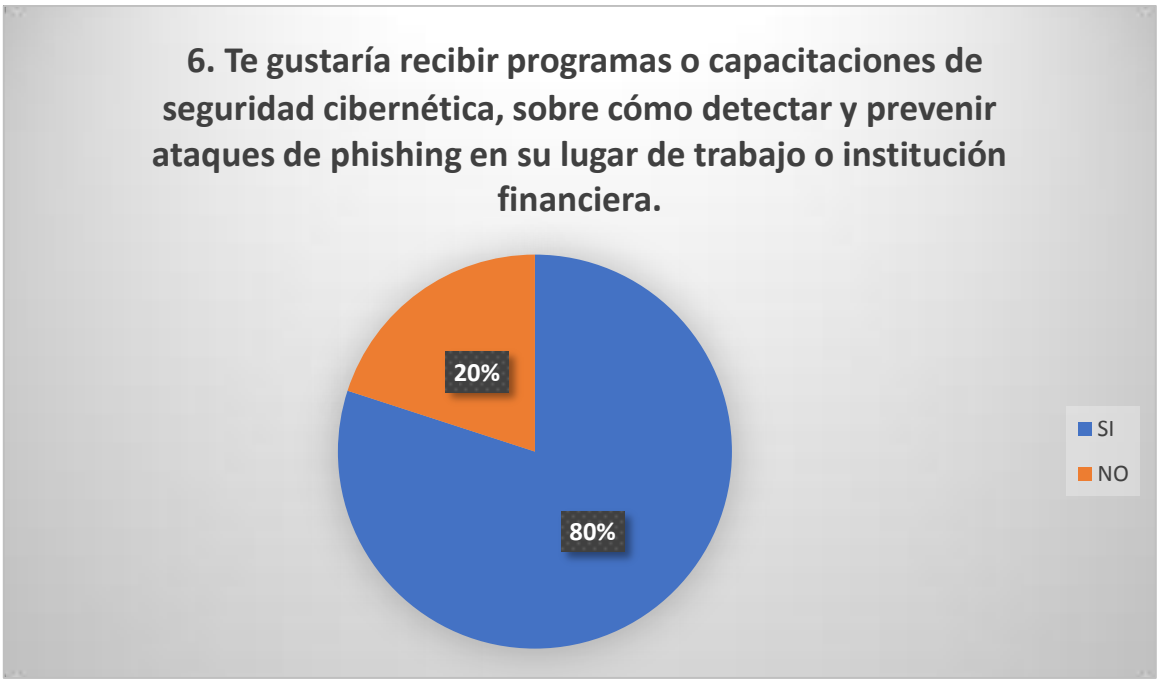
En esta pregunta se visualiza que el 60% de las personas no saben el concepto de phishing ni que función tiene.



Estos resultados reflejan que el 65% de la población entrevistada, no pueden reconocer ataques de phishing, lo cual pueden ser víctimas de este ataque.



Debido al poco conocimiento reflejado en las entrevistas sobre el tema del phishing, las personas ya han sido víctimas de estos correos maliciosos.



Por lo tanto, el 80% de las personas encuestadas han optado por recibir una capacitacion y saber sobre todo este metodo de ataque.