PROPUESTA DE MEJORA Y EFICIENCIA EN LA DETECCIÓN Y NEUTRALIZACIÓN DE SITIOS DE PHISHING Y SUPLANTACIÓN EN UNA INSTITUCIÓN BANCARIA COLOMBIANA

Daniel Felipe Moreno Diaz

Universidad Santo Tomás de Aquino

Facultad de Ingeniería de Telecomunicaciones.

Decano Gustavo Alonso Chica Pedraza

Bogotá, Colombia

2024

PROPUESTA DE MEJORA Y EFICIENCIA EN LA DETECCIÓN Y NEUTRALIZACIÓN DE SITIOS DE PHISHING Y SUPLANTACIÓN EN UNA INSTITUCIÓN BANCARIA COLOMBIANA

Daniel Felipe Moreno Diaz

Director: Decano Gustavo Alonso Chica Pedraza

Trabajo de grado pasantías en Banco Davivienda en el área de Ciberseguridad y Seguridad de la Información con el propósito de obtener el título de Ingeniero de Telecomunicaciones

Universidad Santo Tomás de Aquino

Bogotá, Colombia

2024

Tabla de contenido

Indice de imagenes

Resumen

Este documento aborda de manera exhaustiva los casos de suplantación web dirigidos hacia una Institución Financiera, perpetrados por ciberdelincuentes con la clara intención de obtener beneficios ilícitos. Tales acciones delictivas tienen como objetivo principal acceder a información confidencial de los clientes de la entidad bancaria, así como realizar transacciones fraudulentas para la extracción de fondos de las cuentas afectadas. En el transcurso del análisis, se explorarán los distintos tipos de malware que suelen emplearse en estos actos de phishing, así como se identificarán las diversas páginas fraudulentas que imitan la apariencia de una Institución Financiera con el propósito de engañar a los usuarios.

Además, se desarrollarán estrategias sólidas de mitigación de riesgos destinadas a reducir al mínimo la vulnerabilidad de la marca y de sus clientes frente a estas amenazas cibernéticas. Dichas estrategias están diseñadas con el fin de fortalecer los protocolos de seguridad, implementar medidas preventivas y educativas para los usuarios, así como establecer mecanismos efectivos de detección y respuesta ante posibles incidentes de suplantación web.

Abstract

This document comprehensively addresses cases of web spoofing targeting a financial institution, perpetrated by cybercriminals with the clear intention of obtaining illicit benefits. The main objective of such criminal actions is to gain access to confidential information of the bank's clients, as well as to carry out fraudulent transactions for the extraction of funds from the affected accounts. In the course of the analysis, the different types of malware that are usually used in these phishing acts will be explored, as well as the different fraudulent pages that imitate the appearance of a Financial Institution with the purpose of deceiving users will be identified.

In addition, robust risk mitigation strategies will be developed to minimize the vulnerability of the brand and its customers to these cyber threats. These strategies are designed to strengthen security protocols, implement preventive and educational measures for users, and establish effective detection and response mechanisms for possible web spoofing incidents.

1. Marco contextual del proyecto.

En el contexto digital contemporáneo, el sector bancario se encuentra inmerso en una constante lucha contra una serie de desafíos cruciales, destacándose entre ellos la ciberseguridad como una prioridad indiscutible. En este escenario, el phishing emerge como una de las amenazas más prominentes y complejas que enfrentan las instituciones financieras. Esta táctica, meticulosamente ejecutada por ciberdelincuentes, tiene como objetivo principal engañar tanto a clientes como a empleados bancarios, constituyendo una seria preocupación debido a su capacidad para comprometer la integridad de los datos financieros y personales.

En primer lugar, el phishing se presenta como una amenaza sofisticada, aprovechando ingeniosamente la confianza y la apariencia legítima de comunicaciones electrónicas, como correos electrónicos, mensajes de texto y llamadas telefónicas. Estos mensajes fraudulentos a menudo imitan la marca y el lenguaje de las instituciones financieras, lo que dificulta aún más su detección para el destinatario desprevenido.

Además, el alcance del phishing se extiende más allá de los clientes individuales, alcanzando también a los propios empleados de los bancos. Los ciberdelincuentes pueden dirigirse específicamente a los trabajadores del sector financiero, empleando tácticas de ingeniería social para obtener acceso a sistemas internos y datos sensibles. Esta vulnerabilidad interna resalta la importancia de la concientización y la capacitación continua del personal bancario en materia de ciberseguridad.

1.1 Planteamiento del problema:

En los últimos 5 años, los reportes de ataques cibernéticos hacia instituciones financieras han aumentado en más de un 150% anualmente de acuerdo con cifras de organizaciones como el FBI y Europol. En 2021 se registraron más de 25,000 incidentes a nivel mundial, un salto significativo con respecto a los 9,000 casos de 2020[1].

Este alza se correlaciona directamente con la expansión de los canales de banca digital, que pasaron de representar el 20% del total de operaciones en 2017 a un vertiginoso 65% en la actualidad[2]. Los ciberdelincuentes han enfocado sus esfuerzos en modalidades como el phishing, que les ha permitido comprometer alrededor de 5 millones de usuarios bancarios por año según estimativos de Kaspersky[3].

Los efectos de estos ataques no se han hecho esperar. En Latinoamérica, bancos importantes reportaron pérdidas que superaron los $500 millones de dólares tan solo en 2021, derivadas de fraudes bancarios, robo de identidad y transacciones no autorizadas. La afectación a la reputación y marca también ha sido cuantiosa, con una caída promedio del 10% en la satisfacción del cliente según mediciones de Siegel+Gale[4].

De no implementarse estrategias contundentes, se estima que para 2025 estas instituciones podrían registrar cifras de afectación anuales cercanas a los $1,000 millones, principalmente por técnicas como ingeniería social a través de sites de phishing falsos, abandono de dominios clonados y descargas masivas de keylogger desde programas maliciosos[5][6].

Teniendo en cuenta lo anterior se plantea la siguiente pregunta ¿Cómo pueden las entidades financieras en Colombia optimizar sus estrategias de ciberseguridad para combatir eficazmente el aumento de los casos de phishing y otros tipos de fraude digital evitando repercusiones en pérdidas económicas, mientras garantizan una experiencia segura para sus clientes y optimizan sus inversiones en medidas preventivas tecnológicas?

1.2 Justificación :

El propósito de este documento es evidenciar cómo la ciberseguridad en las instituciones financieras colombianas ha experimentado un aumento en los diferentes ataques cibernéticos en los últimos años, así como las cifras exorbitantes de dinero que han tenido que pagar a sus clientes debido a estos ataques. También se mencionarán los ataques más importantes a los que se han enfrentado estas instituciones, así como algunos ejemplos de los principales tipos de ataques. Además, se discutirán posibles soluciones como mejorar su infraestructura tecnológica, lo que podría ayudar a mitigar la cantidad de usuarios internos y externos vulnerables a este tipo de ataques y evitar pérdidas financieras derivadas de los mismos.

El objetivo es analizar la situación actual de la ciberseguridad en el sector financiero colombiano y proponer acciones que permitan fortalecer las defensas contra amenazas cibernéticas crecientes, de modo que puedan proteger mejor los datos e intimidad de sus clientes y el patrimonio de las propias instituciones.

1.3 Objetivos.

1.3.1 Objetivo general:

Identificar opciones de mejora para la protección contra casos de phishing y suplantación de identidad en los sitios web de una institución bancaria colombiana, con el fin de reducir la cantidad de usuarios afectados y fortalecer la confianza en la marca.

1.3.2 Objetivos específicos:

- Identificación de la actualidad de los ataques cibernéticos al sector bancario.
- Identificación de los ataques cibernéticos más recurrentes en una institución bancaria colombiana.
- Identificación de las acciones de mejora propuestas para fortalecer la eficiencia en la detección y neutralización de sitios de phishing o suplantación en la institución bancaria colombiana.

1.4 Alcance:

El presente proyecto abordará el tema de los ataques cibernéticos dando enfoque al phishing y suplantación de identidad que afectan a las instituciones financieras en Colombia, tomando como caso de estudio una entidad bancaria del sector.

Se realizará un análisis en profundidad de la situación actual de estas amenazas a nivel global y local, indagando sobre las tendencias, patrones y casos más comunes reportados específicamente por la entidad en cuestión.

Como parte del estudio se consultarán fuentes secundarias que permitan caracterizar el panorama de riesgos enfrentado por el sector, así como informes internos disponibles para identificar las modalidades de fraude más recurrentes.

Con base en la información recolectada y mejores prácticas, se formularán recomendaciones dirigidas a reforzar los controles y capacidades de detección y neutralización de sitios maliciosos.

Este proyecto se enfocará en el análisis e identificación de medidas de mejora, buscando proveer insumos para fortalecer la protección contra ataques de phishing y suplantación de identidad en el sector bancario.

1.5 Metodología:

Se define el modelo de trabajo que se llevará para la propuesta de mejora y eficiencia en la detección y neutralización de sitios de phishing y suplantación que puede presentar una institución bancaria colombiana, con al finalidad de evitar las pérdidas generadas a raíz de ataques cibernéticos, como base guía se presentan las siguientes etapas:

Etapa 1:Se llevará a cabo un análisis de la situación actual de los ataques cibernéticos dirigidos al sector bancario a nivel mundial. Es fundamental comprender qué métodos y técnicas están siendo empleados por los ciberdelincuentes, así como el incremento de ataques en los últimos años. Esto proporcionará una visión clara de las amenazas emergentes y

permitirá anticipar posibles ataques que podrían dirigirse hacia el sector bancario en Colombia. Para la realización de esta etapa se necesitan las siguientes actividades:

a. Identificación y análisis de los ataques cibernéticos más frecuentes dirigidos a las instituciones financieras a nivel mundial.
b. Identificación de conceptos relacionados con el malware y sus distintos tipos, así como la identificación de conceptos sobre el phishing y sus variantes.

Etapa 2: Después de completar la Etapa 1, que les ha proporcionado una comprensión detallada de los diversos tipos de ataques cibernéticos y su creciente incidencia a nivel global en los últimos años, se procede a la siguiente fase: El análisis detallado de los ataques cibernéticos más frecuentes que impactan a las instituciones financieras en Colombia..

En esta etapa, se enfocan en examinar detenidamente las técnicas de infiltración utilizadas para la inyección de malware, así como las estrategias de suplantación empleadas. Esto implica un análisis exhaustivo de cada caso, incluyendo el método de distribución de cada amenaza. Para la realización de esta etapa se necesitan las siguientes actividades:

a. Identificación y análisis de los ataques cibernéticos más frecuentes dirigidos a las instituciones financieras a nivel Colombia.
b. Identificación y análisis de los métodos de suplantación dirigida a los clientes de las instituciones financieras con la búsqueda de poder inyectar algún tipo de malware.
c. Descubrimientos a raíz de los análisis e identificaciones en a y b.

Etapa 3: Una vez se hayan definido claramente las identificaciones de la etapa 1 y 2, se procederá a presentar propuestas de mejora que incorporen nuevas tecnologías o estrategias de mercado. Estas propuestas estarán dirigidas a fortalecer la capacidad de las instituciones financieras para prevenir ataques cibernéticos distribuidos mediante métodos de suplantación. Para la realización de esta etapa se necesitan las siguientes actividades:

a. Estrategias destinadas a fortalecer la eficacia en la detección y erradicación de sitios de phishing o suplantación en la institución financiera de Colombia con el fin de evitar la inyección de malware o robo de información confidencial.

2.Ataques cibernéticos más populares dirigidos a las instituciones financieras a nivel global.

En el vasto panorama digital de hoy en día, las instituciones financieras son pilares fundamentales que sostienen la economía global. Sin embargo, esta importancia las convierte en blancos irresistibles para una amplia gama de ataques cibernéticos como se puede evidenciar en la imagen 1. La creciente interconexión de sistemas financieros a nivel mundial y la constante evolución de la tecnología han dado lugar a un escenario en el que las amenazas a la ciberseguridad representan un desafío constante y en constante cambio.

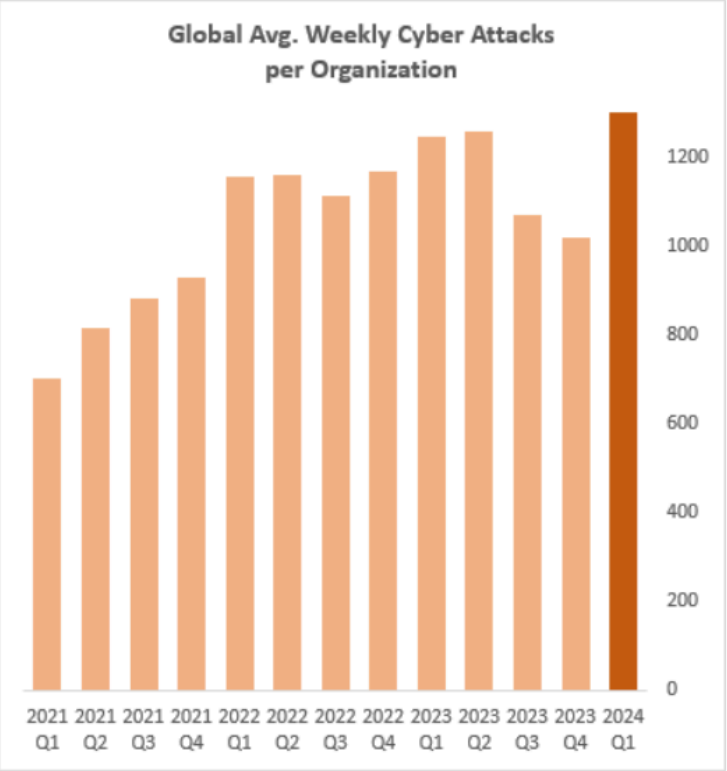

Imagen 1. Promedio global de ataques cibernéticos por Q[7].

Los ataques cibernéticos contra instituciones financieras no solo representan una grave amenaza para la estabilidad económica, sino que también plantean serias preocupaciones en términos de seguridad y privacidad de los datos de los clientes. Desde el robo de información confidencial hasta la interrupción de servicios críticos, los ataques cibernéticos pueden tener repercusiones devastadoras en la confianza del público y en la integridad de los sistemas financieros.

En este contexto, es crucial comprender las diversas formas en que se llevan a cabo estos ataques cibernéticos. Desde malware hasta ataques de denegación de servicio (DDoS), cada técnica tiene sus propias características y métodos de ejecución. Al examinar detenidamente cada uno de estos tipos de ataques, podemos obtener una visión más clara de las amenazas a las que se enfrentan las instituciones financieras y las medidas que deben tomar para protegerse. En este sentido, exploraremos en detalle los siguientes ataques cibernéticos: Malware, Gusanos, Adware, Troyanos, Bombas lógicas, Ransomwares, DDoS y Phishing.

2.1 Malware:

Es una abreviatura de "software malicioso", y se refiere a cualquier tipo de software diseñado con el propósito de dañar, robar información o causar molestias en un sistema informático, dispositivo electrónico o red[8]. Los malware pueden tener una amplia variedad de formas y funciones, algunos de los tipos más comunes incluyen:

2.1.1 Gusanos:

Un gusano informático es un tipo de malware diseñado para propagarse por diferentes dispositivos, permaneciendo activo en todos ellos sin necesidad de ser activado por una acción humana. Un gusano informático puede infiltrarse en un sistema de varias maneras, aprovechando vulnerabilidades como software desactualizado, contraseñas débiles o puertos de red desprotegidos. También puede ingresar a través de dispositivos externos infectados, como unidades USB[9]. Una vez dentro, el gusano comienza a multiplicarse, buscando otros sistemas vulnerables en la misma red o accesibles desde la máquina infectada mediante el escaneo de direcciones IP o la exploración de puertos abiertos. Lleva consigo una carga útil, que puede ser un componente malicioso o un conjunto de instrucciones diseñadas para realizar acciones específicas en el sistema infectado. Para expandirse, el gusano se replica y busca infectar más sistemas, utilizando técnicas de autorreplicación para generar copias de sí mismo y luego distribuirlas mediante la explotación de recursos compartidos en red o el envío de archivos adjuntos de correo electrónico infectados[10].

A medida que el gusano se propaga de un sistema a otro, utiliza activamente varias técnicas para maximizar su propagación de forma autónoma. Una de estas técnicas es explotar vulnerabilidades en protocolos y servicios de red comúnmente usados, con el objetivo de alcanzar nuevos sistemas y objetivos de manera eficaz[11].

Por ejemplo, los gusanos pueden aprovechar fallos de seguridad en programas de correo electrónico populares para enviar automáticamente mensajes infectados a todos los contactos de la libreta de direcciones del usuario, sin necesidad de interacción humana[12]. Esto permite que el gusano se propague de forma encubierta a través de la red de contactos de la víctima.

Además de buscar constantemente nuevos objetivos, los gusanos son capaces de evolucionar y adaptarse con el tiempo para garantizar su supervivencia a largo plazo. Incorporan de forma autónoma nuevas técnicas de propagación basadas en vulnerabilidades recién descubiertas. También actualizan sus cargas útiles (payloads) para sortear mecanismos de detección[12].

Esta capacidad de propagación, evolución y adaptación de forma continua es lo que garantiza el éxito de los gusanos a la hora de infectar de manera sostenida un elevado número de sistemas durante periodos prolongados de tiempo, causando serios problemas de seguridad[13].

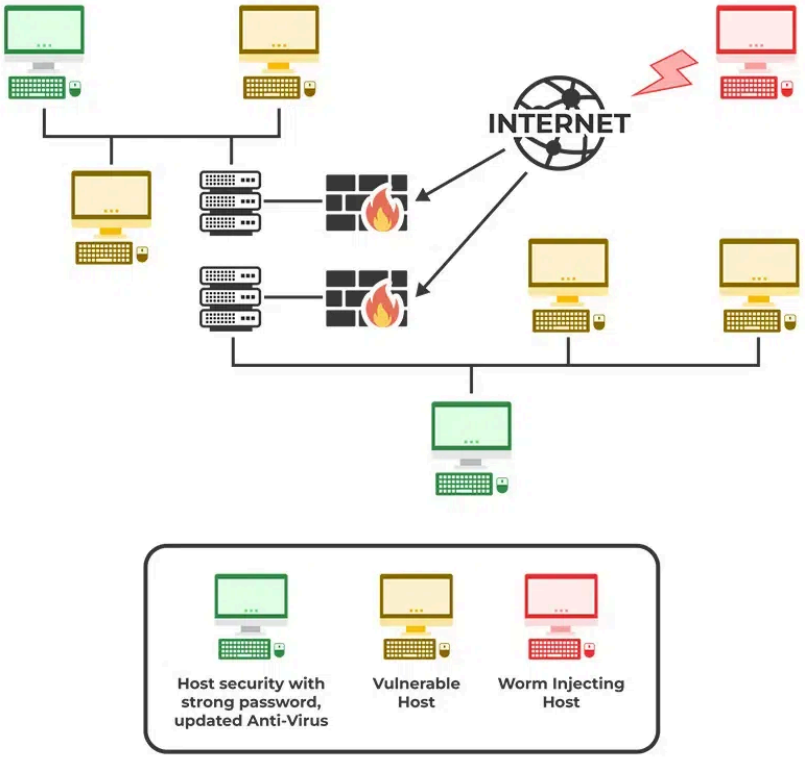

Imagen 2. Forma de distribución de un ataque de gusano[14].

Existen varios tipos de gusanos informáticos, que se pueden clasificar según la forma de propagación:

2.1.1.1. Gusanos de internet:

Se propagan a través de conexiones a Internet, explotando vulnerabilidades en los navegadores o en las aplicaciones web.

2.1.1.2. Gusanos de mensajería instantánea:

Se propagan a través de aplicaciones de mensajería instantánea, aprovechando las vulnerabilidades en estas aplicaciones.

2.1.1.3. Gusanos de correo electrónico:

Se propagan a través de correos electrónicos, aprovechando las vulnerabilidades en los clientes de correo electrónico o en los servidores de correo.

2.1.1.4. Gusanos que comparten archivos:

Se propagan a través de redes de intercambio de archivos, aprovechando las vulnerabilidades en estas redes.

2.1.1.5. Criptogusanos:

Son una variante de gusanos que se propagan a través de la criptografía, aprovechando las vulnerabilidades en los algoritmos de cifrado [11].

La propagación de los gusanos informáticos puede ocurrir de manera autónoma, sin necesidad de intervención humana. Los gusanos pueden propagarse a través de medios físicos, como unidades flash USB, o de manera electrónica, a través de correo electrónico, servicios de mensajería instantánea y redes de intercambio de archivos [15].

Para identificar un gusano informático en una máquina, es necesario buscar signos de actividad anormal, como un aumento en el uso de recursos del sistema, conexiones a sitios web desconocidos, o archivos descargados sin autorización. También es importante mantener actualizado el software antivirus y realizar análisis regulares para detectar y eliminar cualquier malware presente [10][11].

2.1.2 Adware:

El adware es un software no deseado diseñado para mostrar anuncios en la pantalla del usuario, normalmente en un navegador web. Se considera un precursor de los programas potencialmente no deseados (PUP) y puede ser introducido en el sistema de varias maneras, como a través de programas freeware o shareware que incluyen adware sin el consentimiento

del usuario, o mediante la explotación de vulnerabilidades en el navegador del usuario para iniciar descargas involuntarias [15][16].

El adware puede realizar tareas no deseadas, como analizar la ubicación y los sitios web visitados por el usuario, mostrar anuncios relacionados con los bienes y servicios que se muestran en esos sitios, y recopilar información sobre los hábitos de navegación del usuario para personalizar los anuncios. Aunque no es una amenaza de seguridad informática directa, puede ser molesto y, si los creadores del adware venden la información recopilada a terceros, puede resultar en un bombardeo de anuncios personalizados [17].

Imagen 3. Demostración gráfica de un Adware[18].

Existen diferentes tipos de adware, incluyendo secuestradores de navegador, que modifican la configuración del navegador sin el consentimiento del usuario, cambiando la página de inicio, la configuración de búsqueda por defecto, y más. Otros tipos de adware pueden modificar la página de inicio, el motor de búsqueda, o incluso cambiar los atajos de teclado del ordenador para abrir el navegador. Además, el adware puede variar según el dispositivo y el sistema operativo, incluyendo versiones para móviles Android, Mac, y Windows [19].

Para identificar el adware en una máquina, se pueden buscar signos como la aparición de anuncios no deseados, cambios misteriosos en la página de inicio del navegador,

problemas con la visualización de sitios web frecuentados, redirecciones a sitios web no deseados, lentitud en el navegador, aparición de nuevas barras de herramientas, extensiones o plugins, instalaciones automáticas de aplicaciones no deseadas, y bloqueos del navegador [20].

El adware ha evolucionado desde su creación inicial en 1995, considerado parte del spyware, hasta convertirse en una forma de PUP con un nivel de amenaza por debajo de la categoría de malware. A pesar de que el adware sigue existiendo, ha experimentado un resurgimiento, siendo responsable de un alto porcentaje de detecciones por parte de los usuarios de Malwarebytes[21]. Esto se debe en parte a la proliferación de dispositivos móviles, que facilita la introducción de adware en aplicaciones móviles, y a la consolidación de los creadores de adware, que recurren a técnicas más agresivas para evitar su eliminación [15].

2.1.3 Troyanos:

Un troyano es un tipo de malware que se disfraza de software legítimo para engañar a los usuarios y permitir a los cibercriminales acceder a sus sistemas, un ejemplo de esto es en la Imagen 4. A diferencia de los virus, los troyanos no se autorreplican, sino que se propagan simulando ser un software o contenido útil, mientras que en secreto contienen instrucciones maliciosas [22][23].

Los troyanos se crean utilizando técnicas de ingeniería social para engañar a los usuarios y hacer que descarguen o ejecuten el malware. Esto puede ocurrir a través de ataques de phishing, donde se envían correos electrónicos fraudulentos que parecen ser de confianza; mediante la instalación de programas antivirus falsos que sugieren que el equipo está infectado; o mediante la descarga de software de sitios web no confiables o desconocidos [23][24].

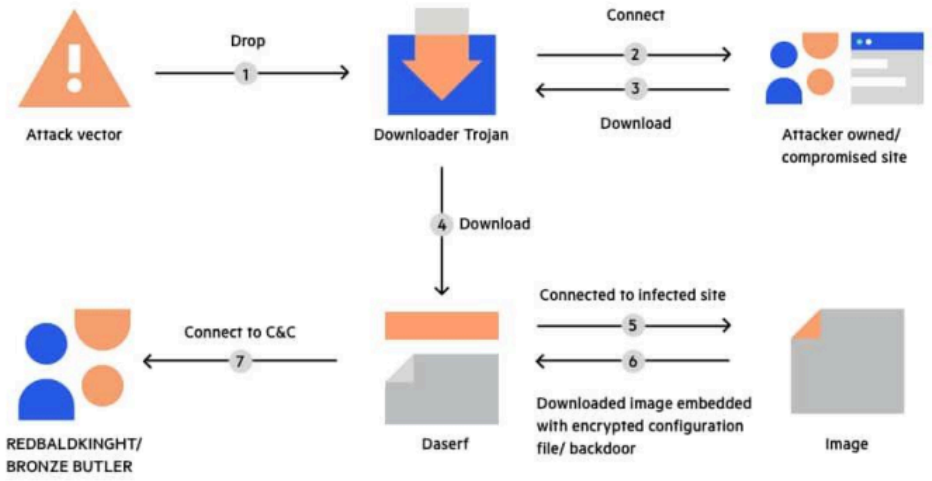

Imagen 4. Manera de ataque del método troyano encriptado por medio de un archivo multimedia[25].

Existen varios tipos de troyanos, pero todos comparten la característica de disfrazarse de software legítimo para engañar a los usuarios. Algunos ejemplos comunes incluyen:

2.1.3.1 Troyanos de phishing:

Estos se envían a través de correos electrónicos que parecen ser de remitentes legítimos, pero que contienen archivos adjuntos o enlaces maliciosos.[27]

2.1.3.2 Scareware:

Programas antivirus falsos que sugieren que el equipo está infectado y ofrecen una solución, pero en realidad descargan un troyano.[28]

2.1.1.3.3 Troyanos de descarga oculta:

Software que se descarga automáticamente sin el consentimiento del usuario, a menudo disfrazado como un programa útil.[26]

2.1.3.4 Troyanos de red Wi-Fi falsa:

Redes falsas que se hacen pasar por redes Wi-Fi legítimas para engañar a los usuarios y redirigirlos a sitios web maliciosos.

Los troyanos funcionan al ser ejecutados por el usuario, ya sea a través de la descarga de un archivo malicioso, la ejecución de un programa infectado o la conexión a una red Wi-Fi falsa. Una vez activados, pueden permitir a los cibercriminales espiar, robar información confidencial y obtener acceso de puerta trasera al sistema del usuario [29][30].

Para identificar un troyano en una máquina, es importante estar atento a comportamientos sospechosos, como redirecciones no solicitadas a sitios web desconocidos, programas de inicio inesperados o archivos adjuntos de correo electrónico sospechosos. Además, utilizar software antivirus y mantenerlo actualizado puede ayudar a detectar y eliminar troyanos. En algunos casos, reiniciar el dispositivo en modo seguro y desactivar programas de inicio no confiables puede ser útil para eliminar troyanos sin afectar el funcionamiento del sistema [31][32].

2.1.4 Bombas lógicas:

Una bomba lógica es un código malicioso que se inserta en una red informática, sistema operativo o aplicación de software, y permanece inactiva hasta que se cumple una condición específica (Imagen 5). Al activarse, puede causar daños significativos al sistema, como borrar archivos, limpiar discos duros, o incluso enviar correos electrónicos de spam desde el sistema infectado [33][34].

Las bombas lógicas pueden activarse mediante condiciones positivas (cuando se cumple una condición específica) o negativas (cuando no se cumple una condición). Un ejemplo de activación positiva sería la apertura de un archivo específico, mientras que una activación negativa podría ser el no desactivar la bomba a tiempo [34][35].

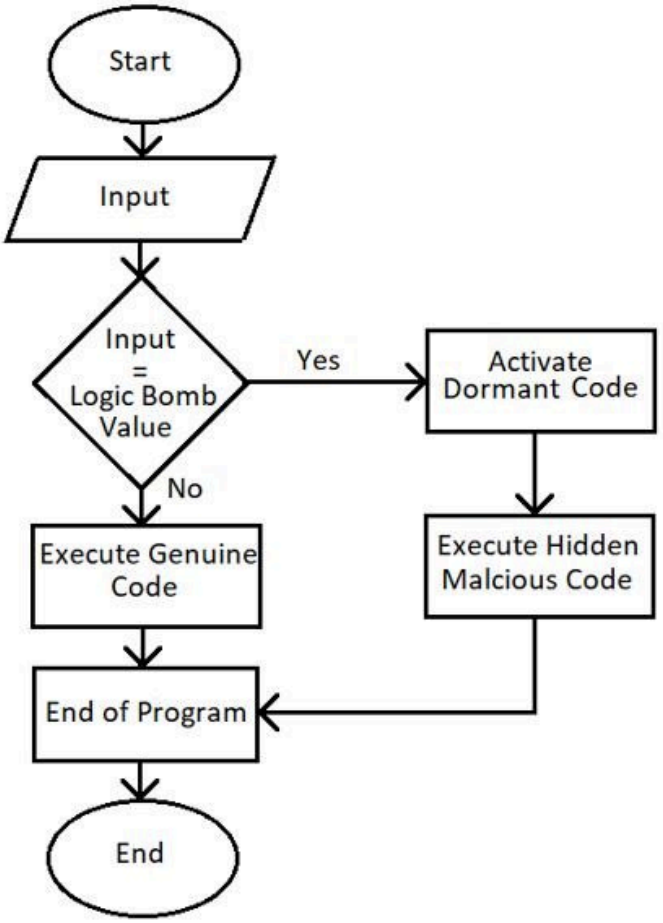

Imagen 5. Funcionamiento de una bomba lógica[36].

Existen diferentes tipos de bombas lógicas, incluyendo las bombas de tiempo, que se activan en una fecha o hora específica. Estas bombas utilizan una condición lógica basada en el tiempo para detonar [37].

Para identificar una bomba lógica en una máquina, es crucial estar atento a cambios inusuales en el comportamiento del sistema, como la pérdida inexplicada de datos, el funcionamiento lento, o la aparición de mensajes o correos electrónicos no deseados. Además, la presencia de archivos o programas desconocidos, o la detección de actividad de red inusual, pueden ser indicativos de una bomba lógica. En algunos casos, las bombas lógicas pueden pasar años sin ser detectadas, lo que hace que su identificación sea un desafío [38][39].

Para prevenir ataques de bombas lógicas, es esencial mantener el software actualizado, utilizar software de seguridad confiable, y educar a los usuarios sobre las prácticas seguras de navegación y uso de software. Además, realizar copias de seguridad regulares de los datos importantes puede ayudar a mitigar los daños causados por una bomba lógica [40].

2.1.5 Ransomwares:

Los ataques de ransomware dirigidos al sector financiero han sido un problema creciente en los últimos años, afectando a instituciones de todo el mundo. Un ejemplo notable es el ataque al Industrial and Commercial Bank of China (ICBC) en Estados Unidos, donde los atacantes utilizaron el método de ransomware para cifrar los datos del banco, exigiendo un rescate para desbloquearlos (para un mejor entendimiento de los procesos del ataque se puede observar la imagen 6). Aunque el ataque no afectó la operación general del banco en China ni en Nueva York, sí causó interrupciones y preocupaciones sobre la seguridad cibernética en el sector financiero [41].

Además, el sector financiero ha enfrentado amenazas cibernéticas significativas, como la dependencia de terceros proveedores de servicios informáticos, lo que puede aumentar la vulnerabilidad a ataques cibernéticos[42]. Un ejemplo de esto es el incidente de 2023, donde un ataque de ransomware contra un proveedor de servicios informáticos en la nube afectó a 60 cooperativas de crédito en Estados Unidos, demostrando cómo los ataques pueden tener efectos devastadores en el sector financiero [43].

En América Latina, el sector financiero también ha sido objetivo de ataques de malware, como el caso de un ataque de malware conocido como Carioca, que afectó a 70 bancos e instituciones financieras en la región[44]. Este ataque demostró la vulnerabilidad de las instituciones financieras a los ataques cibernéticos, especialmente en un contexto donde la digitalización y la dependencia de la nube han aumentado [45].

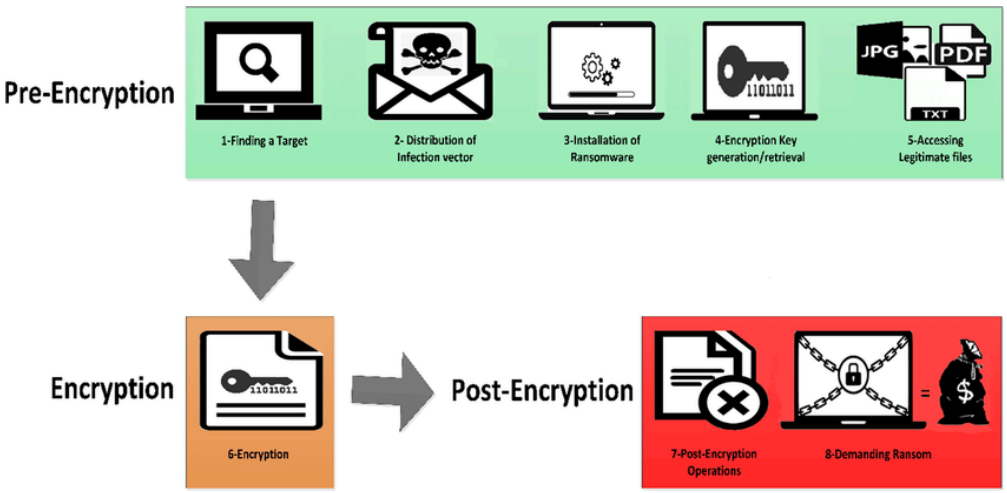

Imagen 6. Fases de un ataque ransomware[46].

Con base a lo anterior se puede concluir que el ransomware es un tipo de software malicioso que cifra los archivos de un usuario, haciéndolos inaccesibles, y luego exige un rescate para desbloquearlos. Se crea mediante el desarrollo de kits de ransomware, que son herramientas utilizadas por los ciberdelincuentes para distribuir fácilmente los ataques de ransomware[47]. Estos kits aprovechan vulnerabilidades en sistemas operativos, aplicaciones o redes para infectar dispositivos y realizar el ataque. Los pagos por ransomware pueden ser muy lucrativos para los atacantes, lo que aumenta los incentivos para llevar a cabo estos ataques [48]. Existen varios tipos de ransomware, entre los que se incluyen:

2.1.5.1 Filecoders:

Son los más comunes y representan aproximadamente el 90% de las cepas de ransomware. Cifran y bloquean los archivos de los dispositivos infectados, exigiendo un pago por la clave de descifrado [49].

2.1.5.2 Screenlockers:

Bloquean completamente el dispositivo, haciéndolo parecer que es controlado por instituciones oficiales como el FBI o el Departamento de Seguridad Interior de Estados Unidos, y exigiendo un pago para desbloquearlo [50].

2.1.5.3 Doxxing:

Aunque no es técnicamente ransomware, es una amenaza digital que puede conllevar la petición de un rescate. Los atacantes acceden a datos privados del usuario y amenazan con publicarlos si no se realiza un pago [51][52].

2.1.5.4 Scareware:

Es un software falso que simula encontrar problemas en el equipo del usuario y demanda un pago para "solucionarlos". Algunas variantes pueden comportarse como screenlockers, bloqueando el dispositivo hasta que se realice el pago [51][52].

Para identificar el ransomware en una máquina, es crucial mantener el software actualizado, realizar copias de seguridad regulares, utilizar un bloqueador de anuncios para protegerse de malvertising y descargas drive-by, y emplear un antivirus confiable. Estas medidas ayudan a prevenir la infección por ransomware y a detectar y eliminar cualquier malware presente [53].

2.1.6 DDoS:

Los ataques DDoS (Distributed Denial-of-Service) son ciberataques que buscan interrumpir, de forma temporal o permanente, el acceso a diversos servicios online como sitios web, aplicaciones, redes, APIs, etc., inundando la máquina o recurso de red objetivo con solicitudes superfluas que provienen de muchas fuentes distintas (Imagen 7). Esto hace que sea imposible parar el ataque bloqueando una única fuente, resultando en una sobrecarga de tráfico indeseado que impide que los servicios estén disponibles para los usuarios finales[54].

Los ataques DDoS funcionan aprovechando redes de dispositivos conectados a Internet que están infectados para perturbar la red o servidor objetivo con una inundación de solicitudes indeseadas. Los ciberatacantes infectan dispositivos utilizando vulnerabilidades de seguridad y malware, convirtiéndolos en "bots" que amplifican el tamaño del ataque. Estos

dispositivos infectados forman una "botnet" que envía solicitudes a la dirección IP objetivo, causando una denegación de servicio e impidiendo que el tráfico normal acceda al servicio que está siendo atacado [55].

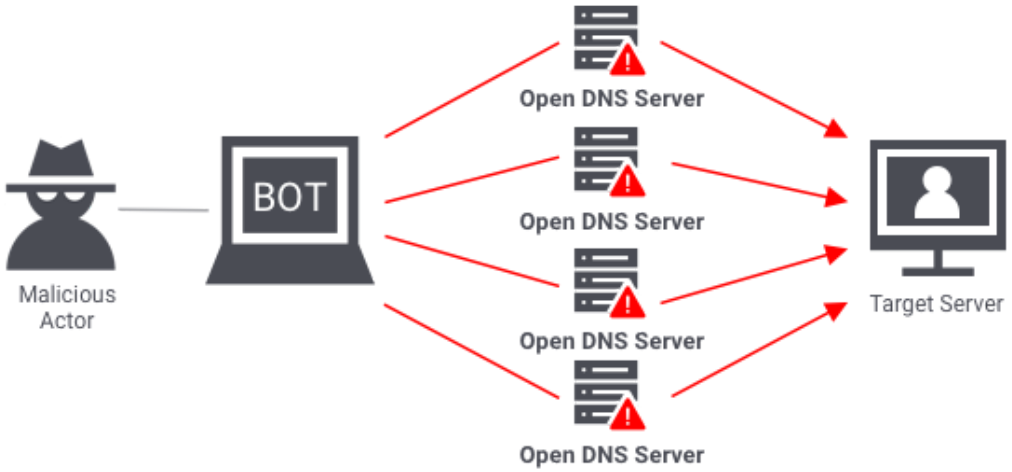

Imagen 7. Funcionamiento ataque DDoS[56].

Los ataques DDoS han afectado significativamente al sector financiero, específicamente en el sector de banca, instituciones financieras y seguros (BFSI). Se destaca que el sector de BFSI ocupó la tercera posición entre los sectores más afectados por ataques DDoS en el contexto de sitios web israelíes, según el informe de Cloudflare [57]. Esto sugiere que las instituciones financieras y de seguros en Israel han sido objetivos de ataques DDoS, aunque no se proporcionan detalles específicos sobre los bancos afectados.

En términos generales, los ataques DDoS se han vuelto más sofisticados y volumétricos, con un aumento significativo en el volumen de tráfico de ataque en el cuarto trimestre de 2023. Los ataques DDoS pueden tomar varias formas, incluyendo inundaciones de solicitudes HTTP, inundaciones de paquetes IP y ataques de inundación de bits, con el objetivo de sobrecargar los servidores y servicios en línea para interrumpir su funcionamiento normal [58].

El informe de Cloudflare también destaca que la mayoría de los ataques DDoS son breves y pequeños en relación con la escala de Cloudflare, pero los sitios web y las redes

desprotegidos pueden sufrir interrupciones debido a ataques breves y pequeños sin una protección automatizada en línea adecuada. Esto subraya la importancia de que las organizaciones adopten una postura de seguridad sólida para mitigar los riesgos asociados con los ataques DDoS [58][59].

Existen tres tipos principales de ataques DDoS:

2.1.6.1 Ataques volumétricos o basados en volumen:

Se caracterizan por el envío de una gran cantidad de tráfico a la red o servidor objetivo, sobrecargándolo[60].

2.1.6.2 Ataques de protocolo:

Se enfocan en explotar vulnerabilidades en los protocolos de red o de aplicación para interrumpir el servicio[60].

2.1.6.3 Ataques a la capa de aplicación:

Dirigidos a aplicaciones específicas, buscan explotar vulnerabilidades en el software de la aplicación para interrumpir su funcionamiento [61].

Además, a veces se utilizan múltiples ataques juntos para atacar varias capas al mismo tiempo, conocidos como "ataques DDoS multivector" [61].

La prevención y mitigación de ataques DDoS es un desafío debido a la dificultad de detección y la sofisticación creciente de las técnicas utilizadas por los atacantes. Es crucial que las organizaciones planifiquen una respuesta adecuada para cuando se produzcan estos ataques [62].

2.2 Phishing:

Los ataques de phishing dirigidos al sector financiero han evolucionado significativamente en los últimos años, adoptando tácticas más sofisticadas y efectivas. Estos

ataques han aumentado en número y sofisticación, con un enfoque creciente en la explotación de vulnerabilidades de día cero y en la recolección de datos confidenciales que pueden ser muy valiosos para los atacantes. Los servicios financieros son un sector esencial que desempeña un papel importante en la economía global, y cualquier interrupción o tiempo de inactividad en estos servicios puede tener graves consecuencias. Además, los datos confidenciales que poseen las organizaciones de este sector pueden convertirse en una mercancía muy valiosa para los atacantes [63].

Los ataques de phishing contra los servicios financieros y sus clientes son altamente rentables, con pérdidas estimadas de 17,700 dólares por minuto. Los ciberdelincuentes pueden recaudar una cantidad significativa de dinero al atacar a una serie de clientes, ya que el precio de los datos de las tarjetas de crédito oscila entre los 17 y los 120 dólares. Con kits de phishing fácilmente disponibles en el mercado clandestino a precios económicos, los ciberdelincuentes pueden lanzar fácilmente ataques a sus objetivos previstos [64][65].

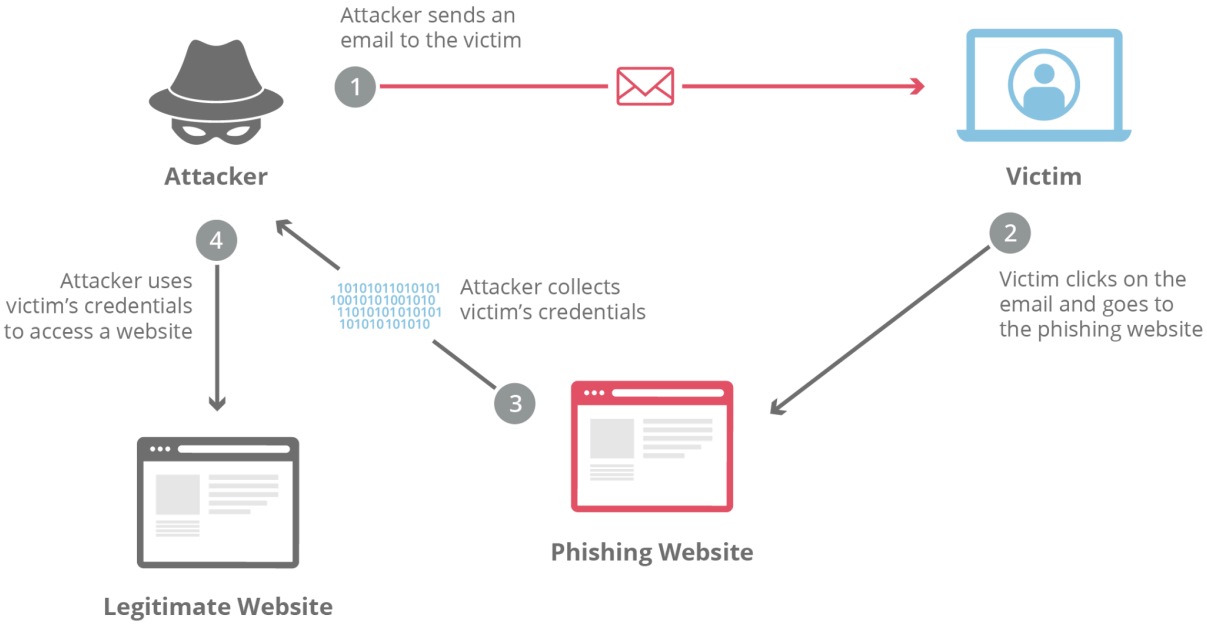

Imagen 8. Funcionamiento ataque de phishing[66].

Aunque los ataques de phishing van dirigidos principalmente a los clientes de las instituciones financieras en lugar de a las propias instituciones, el daño podría extenderse más allá del impacto individual. Los ciberdelincuentes que suplantan servicios financieros podrían dañar la marca y la reputación del banco, erosionando la confianza de los clientes y haciéndole perder su negocio durante el proceso (Ejemplo del funcionamiento de phishing).

Los recursos necesarios para corregir y gestionar los efectos de los ataques de phishing también podrían costar caro a los bancos[67].

El robo de cuentas es una de las amenazas más preocupantes para el sector financiero, con la mayoría de las IP de ataques a instituciones financieras asociadas al robo de cuentas (42%). Los bancos podrían perder ingresos si los clientes experimentan transacciones no autorizadas debido a ataques de robo de cuentas. El coste estimado del fraude por robo de cuentas es de 11,400 millones de dólares al año [68].

En resumen, los ataques de phishing en el sector financiero han cambiado significativamente, adoptando tácticas más sofisticadas y efectivas, con un enfoque en la explotación de vulnerabilidades de día cero y en la recolección de datos confidenciales. Estos ataques representan una amenaza significativa para las instituciones financieras y sus clientes, con implicaciones financieras y de reputación significativas. No es un tipo de malware en sí mismo, sino un método de distribución de este. ¿cómo funciona y dónde se encuentra dentro del espectro de amenazas cibernéticas?:

- Phishing como técnica: El phishing implica el envío de mensajes fraudulentos que parecen provenir de fuentes legítimas para engañar a los usuarios y hacerles realizar acciones dañinas, como hacer clic en enlaces maliciosos o proporcionar información personal[69].

- Phishing como malware: Cuando el phishing conduce a la instalación de malware, se convierte en una forma indirecta de distribución de malware. Por ejemplo, un usuario puede hacer clic en un enlace falso que instala malware en su dispositivo o descargar un archivo adjunto que contiene malware[69].

Existen varios tipos de phishing, cada uno con características y objetivos específicos:

2.2.1 Phishing por Correo Electrónico:

Este es el tipo más común de phishing, donde se envían correos electrónicos que parecen provenir de fuentes legítimas, como bancos o proveedores de servicios, con el fin de engañar a los destinatarios para que revelen información personal o financiera[69].

2.2.2 Spear Phishing:

Los ataques de Spear Phishing se diferencian de los ataques de phishing generales en que son dirigidos a un objetivo específico, utilizando información recopilada sobre el destinatario para hacer que el mensaje parezca más legítimo. Esto puede incluir detalles sobre el campo de especialización, la función en la organización, los intereses personales, y la información pública disponible sobre el destinatario. Esta personalización aumenta la probabilidad de que el destinatario haga clic en un vínculo malicioso o descargue un archivo adjunto, permitiendo al atacante acceder a la red o plataforma objetivo o robar datos confidenciales [69][70].

2.2.3 Whaling:

El whaling es un tipo de ataque cibernético que se dirige específicamente a individuos de alto nivel dentro de una organización, como directores ejecutivos (CEOs) o gerentes financieros, con el objetivo de robar dinero, obtener información confidencial o acceder a sistemas informáticos con fines delictivos. Este ataque se realiza mediante la simulación de una persona de alto nivel dentro de la organización, utilizando técnicas de ingeniería social para engañar a la víctima y hacer que revele información confidencial o realice transferencias de dinero. A diferencia del phishing y el spear phishing, que son ataques más generales, el whaling se enfoca en objetivos específicos y utiliza tácticas para hacer que las comunicaciones fraudulentas parezcan provenir de una persona influyente dentro de la organización[69][71].

2.2.4 Vishing:

El vishing es una práctica fraudulenta que se realiza a través de llamadas telefónicas con el objetivo de engañar a las personas para que revelen información personal y bancaria. Este tipo de estafa se basa en la ingeniería social, donde los delincuentes se hacen pasar por empleados de entidades bancarias u otras organizaciones, utilizando datos obtenidos sobre la víctima para establecer una comunicación aparentemente legítima. Además de las llamadas telefónicas, los estafadores pueden utilizar mensajes de texto (smishing) y servicios digitales para intensificar la ilusión de comunicación legítima. La estrategia incluye la suplantación de identidad, la creación de problemas ficticios para generar una sensación de urgencia y la solicitud de información confidencial bajo el pretexto de resolver el problema[68][72].

2.2.5 Smishing:

El Smishing es un tipo de ciberataque que se realiza a través de mensajes de texto (SMS) o mensajes de texto, combinando las palabras "SMS" y "phishing". Este tipo de ataque se basa en la ingeniería social y se utiliza para engañar a las víctimas haciéndose pasar por entidades de confianza, como bancos o empresas de servicios, con el objetivo de obtener información personal o financiera, hacer clic en enlaces malintencionados o descargar software o aplicaciones dañinas. Los mensajes de smishing suelen parecer urgentes, creando una sensación de miedo o curiosidad para inducir al destinatario a realizar acciones no deseadas, como compartir datos personales o financieros[73].

Los atacantes de smishing pueden adoptar diversas estrategias, incluyendo estafas de verificación de cuenta, premios o loterías, soporte técnico, alertas de fraude bancario, estafas fiscales, cancelación de servicios y descargas de aplicaciones malintencionadas. Estas tácticas buscan aprovechar la confianza de los usuarios en los mensajes de texto y la falta de conciencia sobre los riesgos asociados con hacer clic en enlaces o proporcionar información personal a través de medios digitales[74].

2.2.6 Phishing por Motores de Búsqueda:

Los atacantes manipulan los resultados de búsqueda de motores como Google para que los enlaces a sitios web maliciosos aparezcan como los primeros resultados. Al hacer clic en estos enlaces, los usuarios son dirigidos a sitios web fraudulentos diseñados para robar información [75].

2.2.7 Pharming:

Consiste en redirigir el tráfico de navegación a un sitio web falso, haciendo parecer el sitio web legítimo. Esto se puede lograr a través de correos electrónicos, sitios web infectados o DNS cache poisoning [76].

2.2.8 Whishing:

Utiliza WhatsApp como plataforma para enviar mensajes rápidos que parecen estar de marcas conocidas, con el objetivo de inducir a los usuarios a interactuar con el contenido y posiblemente revelar información personal [77].

2.2.9 Phishing basado en malware:

En este caso, el correo electrónico en sí mismo es un malware. No es necesario abrir un enlace o descargar un archivo; simplemente abrir el correo electrónico ya es suficiente para activar el malware [78].

2.2.10 QRishing:

El QRishing es una técnica de phishing que utiliza códigos QR para engañar a los usuarios y obtener información confidencial, instalar malware, o redirigirlos a sitios web maliciosos. Los códigos QR, que fueron creados en 1994, se han vuelto omnipresentes en la vida cotidiana, utilizados para una variedad de propósitos, desde compartir información hasta acceder a servicios digitales. Sin embargo, esta versatilidad también la convierte en una

herramienta ideal para los atacantes, quienes pueden crear códigos QR maliciosos y colocarlos en lugares estratégicos para que los usuarios los escanee, creyendo que acceden a información legítima o a servicios seguros.[79]

2.3 Ingeniería Social y Spoofing:

Los ataques de ingeniería social y spoofing han tenido un impacto significativo en el sector financiero. La pandemia de coronavirus ha revelado un nuevo nivel de sofisticación en los ataques de phishing, donde los temas de phishing se alinean con catástrofes globales para abordar las ansiedades de la sociedad moderna [80].

En el primer trimestre de 2020, se registró un aumento en ataques cibernéticos dirigidos a instituciones financieras de un 238%. El costo medio de una filtración de información en el sector financiero en 2021 registró cantidades de hasta 5,72 millones de dólares, y se espera que estas cifras continúen aumentando en 2022. Esto indica una gran posibilidad de que el sector financiero sea víctima de ciberataques avanzados con consecuencias costosas [80][81].

3. Identificación de los ataques cibernéticos más recurrentes en una institución financiera colombiana.

El aumento de los casos de phishing en el sector bancario en Colombia ha sido notable en los últimos años. Según un informe de TransUnion, los intentos de fraude digital en los servicios financieros en Colombia aumentaron un 243%1. El fraude digital es un problema creciente a nivel mundial, con un crecimiento del 80% en los últimos tres años[82].

El principal tipo de fraude digital en los servicios financieros en Colombia es la suplantación de identidad, donde una persona utiliza una cuenta robada y suplanta a su víctima para cometer un fraude. Otros tipos de fraude digital reportados por los clientes de servicios financieros de TransUnion son el fraude de primera persona y la toma de la cuenta [83].

En términos de inversiones en ciberseguridad, las de la banca en Colombia aumentaron casi 400% desde 2018, pasando de $88.000 millones en ese año a $315.000 millones en 20203[84].

Las entidades financieras en Colombia recibieron 1.362 millones de ataques cibernéticos en 2021, solo 21 resultaron en algún incidente y no impactaron los recursos de los clientes o la prestación del servicio. Las entidades invirtieron 341.000 millones de pesos para protegerse y 75.000 millones de pesos para responder por incidentes que sufrieron sus clientes debido a operaciones no autorizadas [84][85].

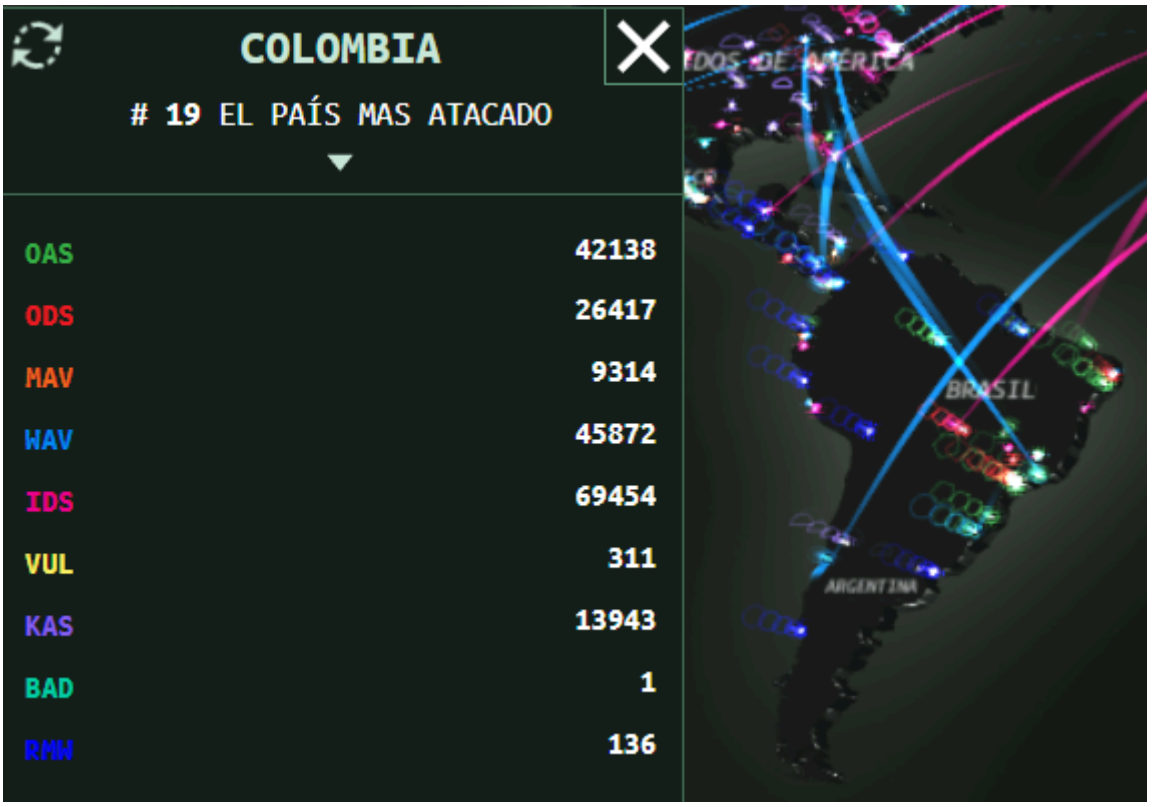

Imagen 9. Mapa global de ataques cibernéticos a tiempo real de Kaspersky[86].

Para protegerse contra estas amenazas, las instituciones financieras deben implementar una serie de medidas de seguridad. Esto incluye la estimación de las medidas de seguridad actuales, la delegación de los servicios de ciberseguridad en socios externos, el uso de la autenticación multifactor, la consideración del ciberseguro como un elemento obligatorio de todo su plan de ciberseguridad, la formación de su personal sobre las amenazas y riesgos actuales, y la comunicación a los clientes sobre los métodos que utilizan los

ciberatacantes para robar su información personal y su dinero[87][88]. Por ejemplo, Davivienda ha implementado herramientas para la detección temprana de ataques. Además, Asobancaria y Certicámara están avanzando en un programa de biometría dactilar del sector, que ha reducido el 99% la suplantación en oficinas [89].

Además, es crucial que las instituciones financieras compartan información entre ellas y generen inteligencia sobre lo que está sucediendo, lo que ayuda a desarrollar el "músculo" contra los ataques cibernéticos más rápidamente y a mejorar la preparación y respuesta ante los incidentes [90].

En resumen, el aumento de los casos de phishing en el sector bancario en Colombia es una preocupación creciente.

Los bancos, presentan este tipo de ataques dirigido a sus usuarios el cual pueden presentarse de diferentes maneras como lo es:

3.1 Apertura de correos electrónicos o SMS con links a sitios externos:

Los ataques de suplantación a través de correos electrónicos o SMS con enlaces a sitios externos son un problema global que afecta a empresas e individuos en todo el mundo. Sin embargo, algunos países son más afectados que otros. Según un informe de la firma de seguridad cibernética Kaspersky, Colombia es uno de los países más afectados por este tipo de ataques en América Latina [91].

Los ataques de suplantación a través de correos electrónicos o SMS con enlaces a sitios externos funcionan de la siguiente manera:

- Los ciberdelincuentes envían correos electrónicos o SMS que parecen provenir de una fuente legítima, como un banco o una empresa conocida.
- Estos correos electrónicos o SMS contienen enlaces que llevan a una página web que visualmente es idéntica a la del banco o la empresa, pero que en realidad es una página falsa.

- Si el cliente hace clic en el enlace y accede a la página falsa, puede ser engañado para ingresar sus datos bancarios o personales, como su número de tarjeta de crédito, contraseña o número de identificación.
- Esta información es recopilada y utilizada por los ciberdelincuentes para realizar transacciones fraudulentas en nombre del cliente.

Los ataques de suplantación a través de correos electrónicos o SMS con enlaces a sitios externos han tenido un impacto significativo en las instituciones financieras colombianas. Estas instituciones han tenido que invertir en medidas de seguridad para proteger a sus clientes de estos ataques, lo que ha supuesto un aumento de los costes operativos. Además, los ataques de suplantación han dañado la reputación de las instituciones financieras colombianas y han generado una pérdida de confianza entre los clientes[92].

Las pérdidas económicas causadas por los ataques de suplantación a través de correos electrónicos o SMS con enlaces a sitios externos son significativas. Según un informe de la firma de seguridad cibernética Symantec, las pérdidas globales causadas por este tipo de ataques ascendieron a 1.300 millones de dólares en 2021. En Colombia, las pérdidas económicas causadas por este tipo de ataques se estiman en 100 millones de dólares en 2021[93].

3.2 Ingreso a páginas de suplantación dirigidas a una institución financiera a través de los buscadores de internet:

En este caso, el cliente puede ser redirigido a un sitio falso que se parece al sitio del banco. Al igual que en el primer caso, el cliente puede ser engañado para ingresar sus datos bancarios en el sitio falso[94].

Los bancos tienen la responsabilidad de proteger a sus clientes contra estos tipos de ataques. Esto incluye la educación de los usuarios sobre cómo protegerse de los fraudes electrónicos, la implementación de medidas de seguridad como firewalls y criptografía de datos, y la monitorización y detección de transacciones fraudulentas [95].

3.3 Websites de suplantación dirigidos a una Institución Financiera.

IMPORTANTE:

Debido a la relevancia de la información contenida en las páginas de suplantación dirigidas al Banco Davivienda, se ha tomado la medida de censurar ciertas secciones de las imágenes mostradas. Esta acción ha sido adoptada con el objetivo principal de salvaguardar la seguridad tanto de los usuarios como de los lectores del documento.

El propósito de esta medida es evitar cualquier compromiso o daño a la reputación de la marca, así como también prevenir potenciales riesgos para aquellos que puedan sentir curiosidad por examinar detalladamente las páginas afectadas.

Se entiende la importancia de proteger la integridad y confianza de los clientes y del público en general frente a posibles intentos de suplantación o fraudes. Por lo tanto, se ha aplicado esta medida de censura de manera diligente y responsable, con el fin de mitigar cualquier posible impacto negativo derivado de la exposición de información sensible o engañosa.

Se agradece la comprensión y colaboración de todos los implicados en este proceso, y se reafirma el compromiso continuo con la seguridad y el bienestar de la comunidad de usuarios.

3.3.1 Suplantación Website de una Institución Financiera:

En este caso de suplantación dirigida a la plataforma principal del Banco Davivienda, se revela un sofisticado intento de engaño perpetrado por ciberdelincuentes. La imagen 10 muestra una página falsa que imita de manera casi idéntica la apariencia y funcionalidades de la página oficial del banco. Sin embargo, una inspección minuciosa permite identificar discrepancias significativas que delatan su carácter fraudulento.

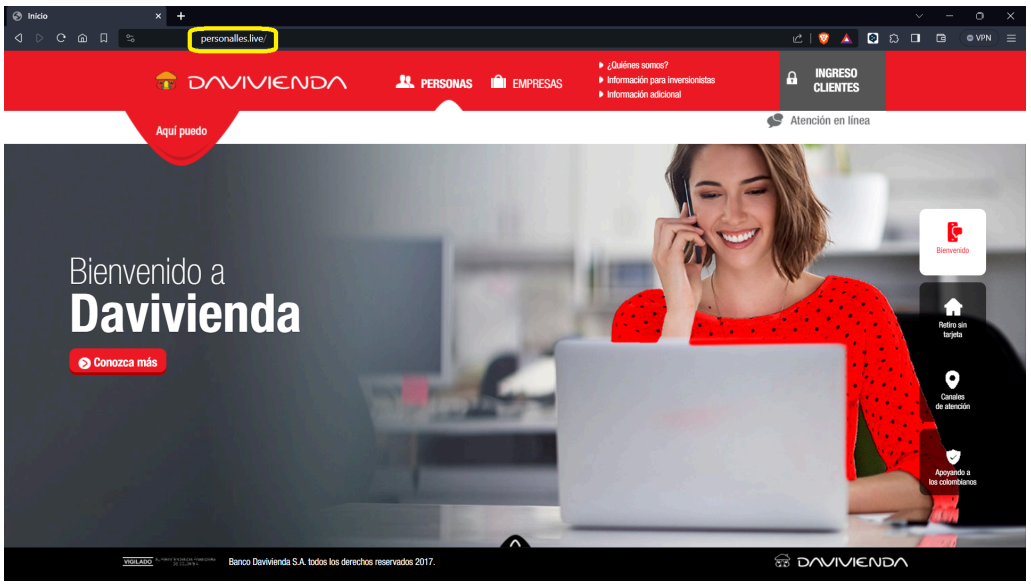

Imagen 10. Suplantación website Banco Davivienda

La primera señal de alerta se evidencia en el dominio utilizado. Mientras que el dominio legítimo del Banco Davivienda es Davivienda.com, la cabecera de la página falsa muestra un dominio completamente diferente. Esta discrepancia constituye una clara indicación de que se trata de un intento de phishing, generando la primera alerta para los usuarios.

Además de la falsificación del dominio, la página falsa presenta una funcionalidad adicional diseñada para capturar información confidencial de los usuarios. La imagen 11 muestra cómo los ciberdelincuentes solicitan datos sensibles, como el tipo y número de documento, así como la contraseña de ingreso a la plataforma. Este tipo de tácticas son comúnmente empleadas por los estafadores para obtener acceso a cuentas bancarias y cometer fraudes financieros.

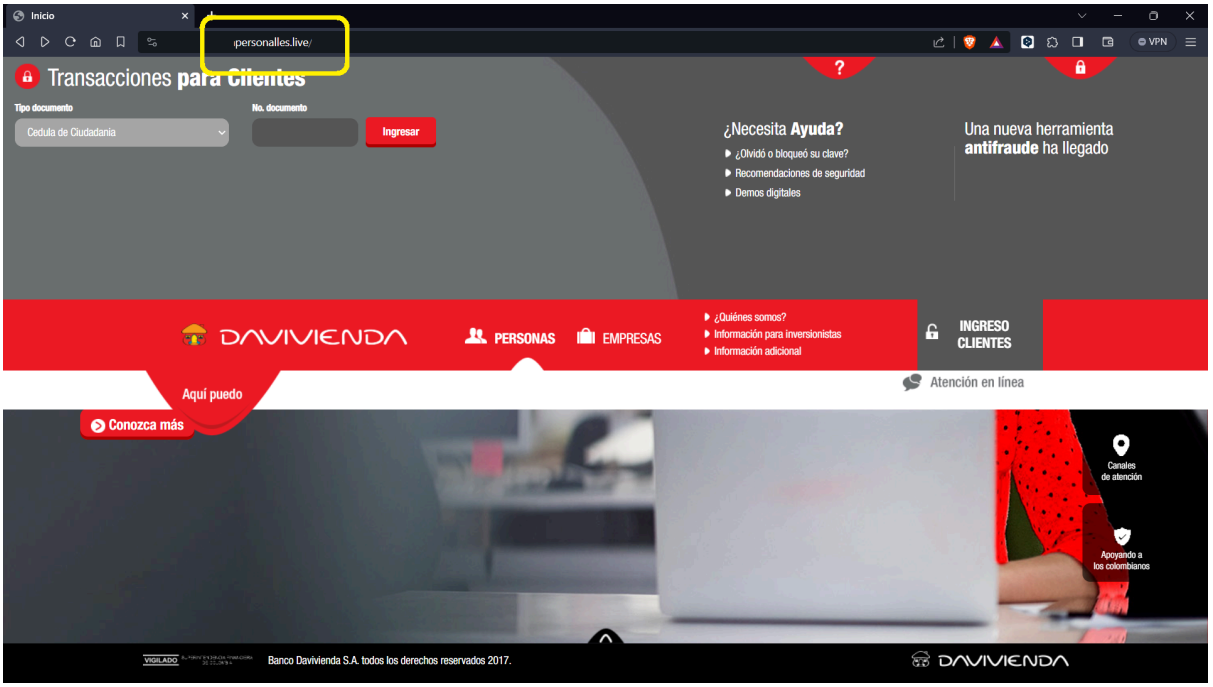

Imagen 11. Suplantación website Banco Davivienda,Solicitud de información

Lo preocupante es que, además de capturar información relevante de los usuarios, los ciberdelincuentes realizan un análisis detallado de la actividad en la página falsa. Registran el número de personas que acceden al sitio fraudulento, la duración de la visita de cada usuario, el número de clicks realizados y su ubicación en la página, así como el porcentaje de usuarios que completan parcial o totalmente el formulario falso.

Esta información recopilada permite a los estafadores entender el comportamiento de los usuarios y ajustar sus estrategias de ataque para futuras campañas de phishing. Es evidente que esta operación criminal es altamente sofisticada y representa un grave riesgo para la seguridad financiera y personal de los usuarios del Banco Davivienda.

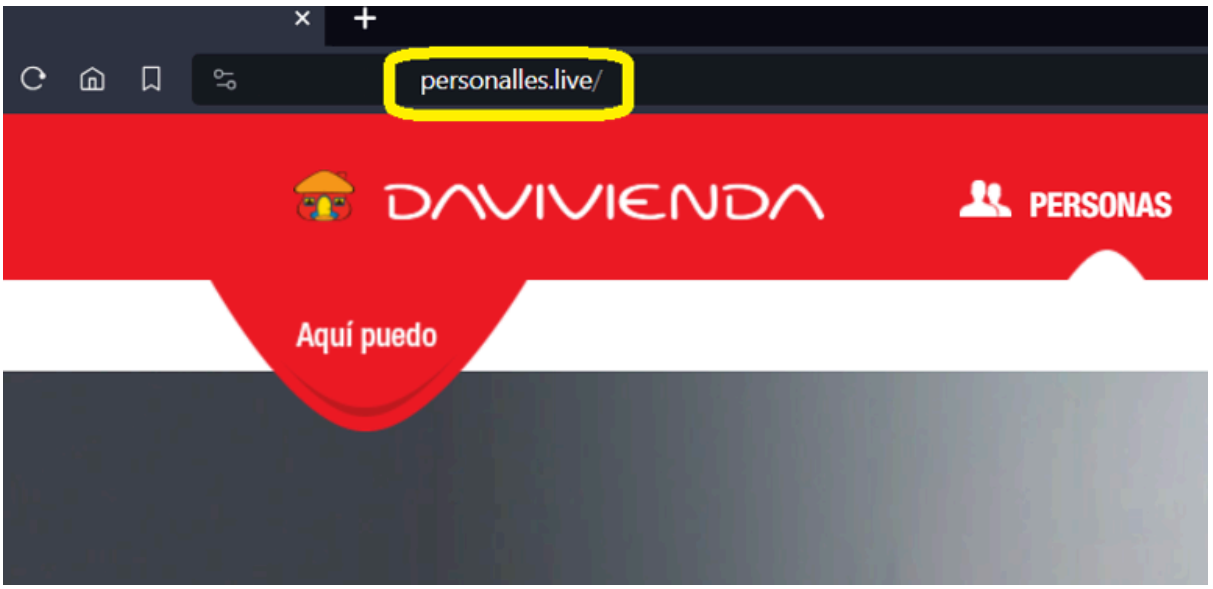

Imagen 12. Parte del dominio usado para la suplantación de la web de Banco Davivienda

3.3.2 Suplantación Website Aplicativo:

Para la suplantación de la plataforma Daviplata, se identifican dos modalidades de diseño utilizadas comúnmente por los ciberdelincuentes, ambas enfocadas en la obtención fraudulenta de información personal y financiera de los usuarios. En primer lugar, en la imagen número 13 se muestra un ejemplo de suplantación de Daviplata destinado a dispositivos móviles. Esta variante suele ser distribuida a través de mensajes de texto o aplicaciones de mensajería instantánea como WhatsApp.

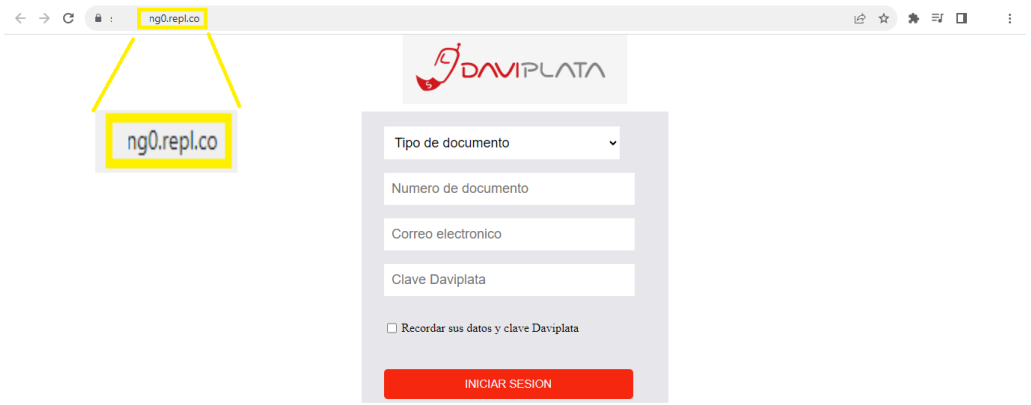

Imagen 13.Suplantación website Daviplata, visualización móvil.

Por otro lado, la imagen número 14 exhibe un caso de suplantación de Daviplata orientado a sitios web falsos. Estos sitios fraudulentos suelen utilizar dominios diferentes al legítimo de la marca, y pueden ser promocionados a través de correos electrónicos fraudulentos o en portales web donde los usuarios pueden ser atraídos a través de diversos métodos engañosos.

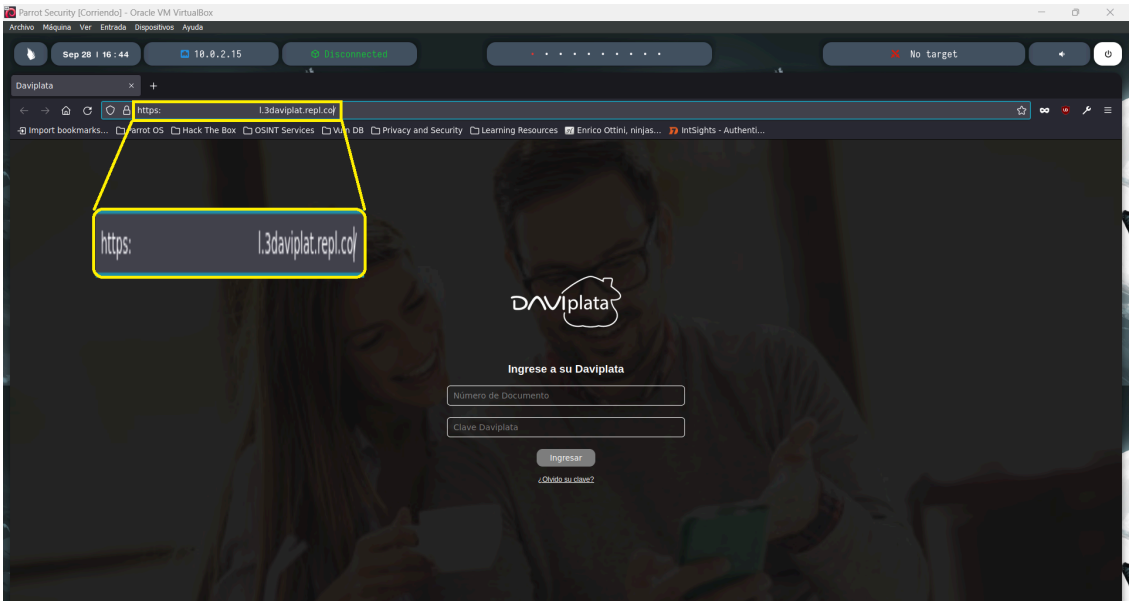

Imagen 14. Suplantación website Daviplata, visualización escritorio.

Es importante destacar que estos casos de phishing, ya sea dirigidos a dispositivos móviles o a sitios web, comparten similitudes fundamentales con los casos de suplantación de la plataforma principal del Banco Davivienda, como se detalló anteriormente en el numeral 3.3.1. En todos estos escenarios, los ciberdelincuentes buscan engañar a los usuarios para que divulguen información confidencial, aprovechándose de la confianza y la familiaridad que los usuarios tienen con la marca Davivienda.

4. Descubrimientos y tendencias de los ataques cibernéticos más recurrentes en una institución financiera Colombiana.

4.1 Detección por parte de los browsers:

Varios navegadores web incorporan herramientas internas diseñadas para detectar y prevenir la interacción con páginas utilizadas para la realización de ataques de phishing. En el

caso particular de la imagen 15, se presenta un ejemplo de una página de suplantación destinada a Daviplata. Sin embargo, es importante destacar una problemática recurrente: la disparidad en los parámetros de detección de phishing entre distintos navegadores.

Esta disparidad puede resultar en bloqueo de sitios maliciosos en algunos navegadores mientras que en otros no. Esto se debe a que cada navegador implementa sus propios algoritmos y metodologías para identificar y clasificar las páginas potencialmente peligrosas. Como resultado, los usuarios pueden encontrarse con inconsistencias en la protección contra phishing según el navegador que utilicen.

Esta situación subraya la importancia de la actualización constante de las medidas de seguridad por parte de los desarrolladores de navegadores, así como la necesidad de que los usuarios estén al tanto de las diferencias en la eficacia de las herramientas de protección entre plataformas. Además, resalta la necesidad de una mayor colaboración entre los proveedores de navegadores y las entidades de seguridad cibernética para mejorar la detección y prevención de ataques de phishing en línea.

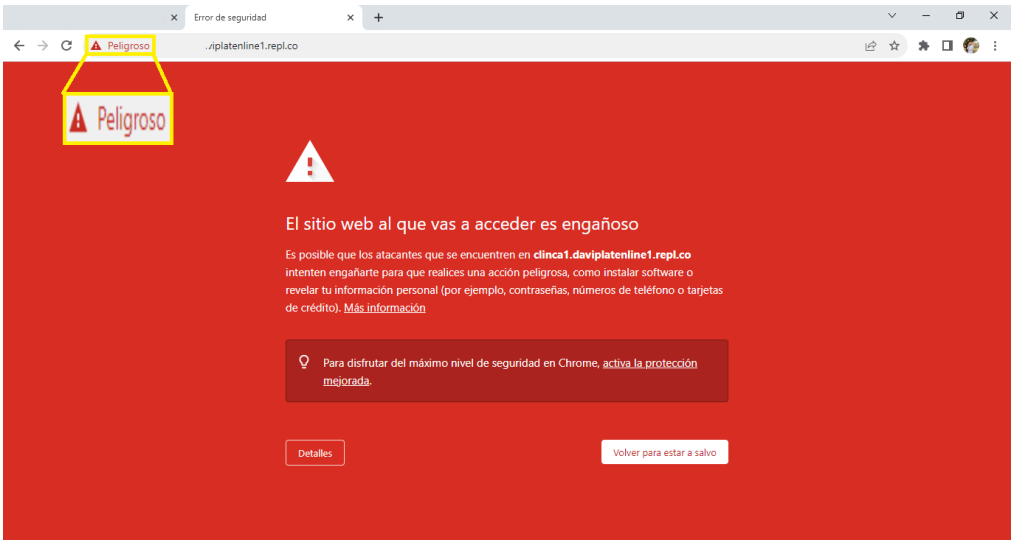

Imagen 15. Detección de parte del browser.

4.2 Desactivación del servicio y lectura de errores de los sitios de suplantación:

En el contexto de las campañas de phishing, es común que los atacantes alojen páginas de suplantación durante períodos prolongados o en base a la cantidad de información

recopilada antes de desactivar el servicio en la web. Esta táctica tiene como objetivo primordial eludir la detección por parte del navegador, que constituye la última barrera de defensa en la identificación de sitios web cómo fra|udulentos o maliciosos.

La función del navegador en este caso es crucial, ya que utiliza una variedad de mecanismos de seguridad, como la evaluación del comportamiento del usuario, el análisis de firmas de malware conocidas y la valoración de la reputación del dominio, para determinar la autenticidad de un sitio web. Por lo tanto, los atacantes procuran mantener activas estas páginas de suplantación durante el mayor tiempo posible con el fin de evitar la detección y baja del sitio por parte del navegador.

En el análisis de la imagen 16, se identificó un error 522 al intentar establecer la comunicación con la página de suplantación. El error 522, un código de estado HTTP, señala una desconexión entre el servidor web y el servidor. Este incidente puede surgir debido a varios factores, como congestión en la red, tiempo de espera excedido o problemas de enrutamiento. Es crucial señalar que también es posible encontrar el error 526 en situaciones similares. El error 526 está vinculado a la comunicación a través de HTTPS e indica un problema con el certificado SSL o TLS del servidor web.

Esto sugiere que algunas plataformas de suplantación emplean estos protocolos de seguridad para garantizar la integridad de la comunicación. Estos certificados proporcionan una capa adicional de protección, perceptible para el usuario mediante un ícono de candado en la barra de direcciones del navegador, lo que puede llegar a inducir que el sitio web es seguro. Esta tendencia refleja la evolución hacia páginas web de suplantación más robustas.

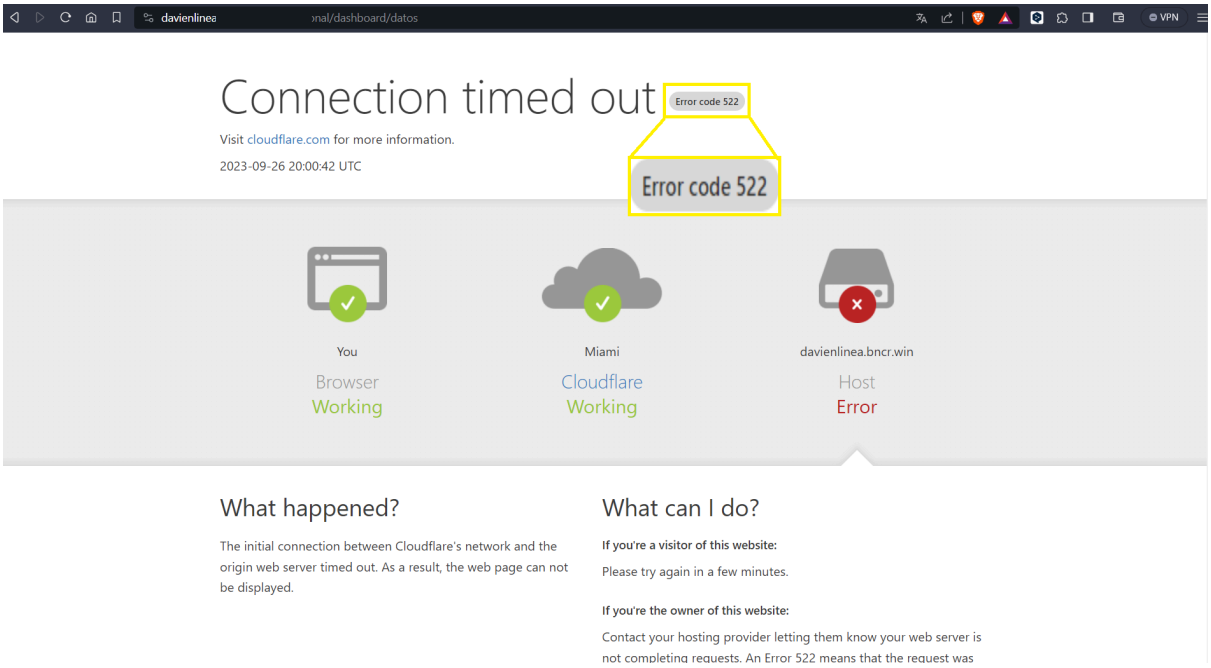

Imagen 16. Desactivación del servicio del phishing.

4.3 Uso de plataformas IDE (Entorno de desarrollo integrado):

Las plataformas de desarrollo en la nube ofrecen a los usuarios un entorno de programación accesible desde cualquier lugar con conexión a internet. Esto puede hacer que sea más fácil para los delincuentes crear y distribuir código malicioso, ya que no necesitan instalar ningún software en sus propios dispositivos y pueden trabajar de manera remota. Por ejemplo, podrían usar un IDE en la nube para desarrollar scripts o aplicaciones que simulan sitios web de inicio de sesión legítimos, con el objetivo de robar credenciales de usuario.

Además, estas plataformas suelen permitir compartir fácilmente el código desarrollado, lo que podría facilitar la distribución de páginas de phishing entre los usuarios. Los delincuentes pueden compartir enlaces a sus proyectos maliciosos a través de correos electrónicos, mensajes de texto o en foros en línea, intentando engañar a las víctimas para que proporcionen información confidencial.

4.4 Uso de smishing como metodo de distribucion de campañas de phishing:

Imagen 17. Ejemplo de smishing.

Se observó que uno de los principales métodos de distribución del phishing era mediante el smishing, una técnica que implica el envío masivo de mensajes de texto a diversos números de contacto, independientemente de si pertenecen a usuarios de la marca o no. En estos mensajes de texto, se empleaba la ingeniería social en el cuerpo del mensaje para inducir a la persona receptora a creer que se había llevado a cabo una transferencia en alguna de las cuentas del usuario como se puede notar en la imagen 17. Este enfoque tenía como objetivo captar la atención del usuario. Además, estos mensajes contenían enlaces URL que redirigen al usuario a páginas de suplantación previamente mencionadas en los apartados 6.1 y 6.2, o hacia otras páginas maliciosas.

4.5 Uso de pharming:

Tras la detección de la interacción del usuario con un enlace malicioso, ya sea a través de un navegador web o mediante smishing, y llevando a cabo investigaciones exhaustivas junto con un monitoreo riguroso de las URL y dominios involucrados, se ha podido observar

que una parte significativa de los casos de phishing recurre a la técnica conocida como pharming.

El pharming implica la manipulación de los sistemas de nombres de dominio (DNS) o la configuración del servidor para redirigir al usuario a una dirección URL diferente de la solicitada originalmente. Este método operaba de la siguiente manera: los ciberdelincuentes empleaban páginas de comercio electrónico, ya fueran vulneradas o creadas por ellos mismos, con el fin de utilizar temporalmente la técnica de pharming. Posteriormente, desactivaban los servicios de la página de suplantación utilizando la técnica detallada en el numeral 4.2.

Es importante destacar que, a diferencia de otras técnicas, esta modalidad de pharming no genera un error, sino que vuelve a enfocar la funcionalidad de la URL hacia la plataforma de comercio electrónico legítima. Este enfoque tiene como objetivo evitar que los navegadores web generen sospechas, así como prevenir que el dominio utilizado en el phishing sea eliminado o dado de baja.

5. Estrategias para fortalecer la eficiencia en la detección y neutralización de sitios de phishing o suplantación en la institución financiera colombiana.

5.1.Capacitación de usuarios:

Las capacitaciones de ciberseguridad para usuarios internos y externos son fundamentales para las instituciones financieras debido a la naturaleza sensible de la información que manejan, incluyendo datos de clientes y propios datos confidenciales. Estas capacitaciones ayudan a prevenir y mitigar los riesgos asociados con ciberataques, que pueden tener consecuencias devastadoras tanto para la reputación como para la seguridad financiera de la institución.

Es ampliamente reconocido en el sector financiero que estas iniciativas contribuyen significativamente al fortalecimiento de la ciberseguridad. Algunas de las formas en que estas capacitaciones pueden mejorar la seguridad de las instituciones financieras incluyen:

- Concientización sobre amenazas: Las capacitaciones ayudan a los empleados a entender las principales amenazas de ciberseguridad, como phishing, malware, y ataques de ransomware, y cómo identificar y evitar estos riesgos.
- Adopción de buenas prácticas: Capacitar a los usuarios en el uso seguro de tecnologías y plataformas puede reducir la superficie de ataque y minimizar el impacto de cualquier incidente de seguridad.
- Respuesta a incidentes: La formación en procedimientos de respuesta a incidentes de seguridad puede acelerar la recuperación y minimizar el daño en caso de un ataque.
- Cumplimiento normativo: Las capacitaciones también pueden asegurar que las instituciones financieras cumplan con las regulaciones y normativas de ciberseguridad, evitando multas y sanciones.

A pesar de la falta de estadísticas específicas, la evidencia empírica sugiere que las instituciones financieras que invierten en capacitaciones de ciberseguridad experimentan una disminución en los incidentes de seguridad y mejoran su capacidad para responder de manera efectiva a los incidentes que ocurren. Además, la concienciación y la educación de los usuarios son componentes clave en la estrategia de defensa en profundidad de cualquier organización, especialmente en el sector financiero donde la protección de la información es crítica.

5.2 Uso de doble factor de autenticación:

Implementar el uso de un OTP (One-Time Password, o Contraseña de un solo uso) es una medida esencial para proteger las credenciales bancarias de los usuarios. Esta estrategia implica requerir no solo una contraseña para iniciar sesión en una cuenta ya sea Daviplata o Banco Davivienda, sino también un segundo factor de autenticación, como un código único enviado al teléfono móvil del usuario o correo electrónico.

El uso del OTP actúa como una barrera adicional contra los ciberdelincuentes que han obtenido las credenciales bancarias de los usuarios de manera fraudulenta. Aunque puedan ingresar las contraseñas, no podrán realizar ninguna acción sin el código único de autenticación generado en tiempo real.

Esta capa adicional de seguridad reduce significativamente el riesgo de que los ciberdelincuentes puedan llevar a cabo transacciones no autorizadas o acceder a información confidencial incluso si han comprometido las credenciales de inicio de sesión de los usuarios.

5.3 Pruebas de phishing controlados dentro de la organización:

Considerando que la protección de la información de los usuarios es un factor crucial, es necesario salvaguardar internamente a la empresa contra diversos métodos de acceso por parte de ciberdelincuentes, como el phishing, que puede infectar los equipos de los empleados descargando malware. Para evaluar la preparación y previsión de las personas, así como identificar áreas de mejora en ciberseguridad, se sugiere la realización de pruebas simuladas masivas de phishing en diferentes departamentos de la empresa.

Para llevar a cabo estas pruebas, se pueden emplear herramientas como GoPhish, que permite la ejecución de campañas de phishing controladas y a gran escala. Esta plataforma otorga a los administradores, especialmente al equipo de ciberseguridad, la capacidad de diseñar y analizar exhaustivamente las pruebas, obteniendo datos como el número de personas que recibieron la campaña, cuántas hicieron clic en los enlaces proporcionados, el tiempo que pasaron en la plataforma de prueba y las horas de acceso a los enlaces.

Con base en el análisis de esta información, y considerando que los empleados de Davivienda también son usuarios de la misma marca, se pueden desarrollar estrategias de capacitación interna y externa para fortalecer la seguridad contra el phishing, tanto dentro como fuera de la empresa. Estas estrategias no solo sirven para mejorar la conciencia y habilidades de los empleados en ciberseguridad, sino también para reforzar la protección interna de la compañía ante posibles casos de phishing.

5.4 Convenio con los browsers más importantes del mercado:

Considerando la abundancia de casos de phishing que se encuentran diariamente, se propone establecer convenios con los principales navegadores web del mercado. Estos acuerdos facilitarían la rápida desactivación de las páginas fraudulentas que intentan suplantar la identidad de Banco Davivienda y Daviplata. El proceso estaría respaldado por

una serie de pruebas proporcionadas por el equipo de ciberseguridad y seguridad de la información de la empresa.

Una estrategia adicional sería compartir información relevante sobre los casos de phishing identificados con los navegadores web. Esto permitiría a los proveedores de navegación mejorar sus sistemas de detección de suplantación web, al comprender mejor las tecnologías, los proveedores de alojamiento, la infraestructura y la estructura utilizadas por los phishers.

En última instancia, esta colaboración mejoraría la seguridad de los usuarios que utilizan estos navegadores al tiempo que fortalecería sus capacidades de detección de amenazas de manera general.

5.5 Convenio con empresas de telecomunicaciones más importantes del mercado:

Ante los casos de smishing, se plantea la posibilidad de establecer convenios con empresas de telecomunicaciones que cuenten con una infraestructura tecnológica sólida. Estas empresas deberían tener la capacidad de realizar un escaneo en tiempo real de los mensajes salientes, ya que su función principal como proveedores implica la distribución de mensajes mediante un modelo de comunicación punto a punto.

La estrategia propuesta funciona de la siguiente manera: la compañía enviaría a su proveedor los mensajes SMS de campaña que utiliza, y cualquier variante de campaña distinta a las originales de la marca serían retenidas. Este enfoque proporciona una ventaja significativa al proteger a los usuarios en gran medida contra el smishing casi en su totalidad.

5.6.Segmentación de red y RBAC:

La implementación de medidas de segmentación de red y control de acceso basado en roles (RBAC) permite sectorizar las operaciones bancarias en diferentes dominios lógicos según el tipo de actividad y perfiles de usuarios. Al dividir físicamente la red de la institución en múltiples subredes independientes con listas de control de acceso (ACLs) bien definidas, se limita el alcance de las amenazas y se aíslan posibles sectores comprometidos, impidiendo

la propagación masiva de malware o la exposición de toda la información a sitios maliciosos de suplantación. Del mismo modo, asignar niveles de permisos diferenciados según el rol específico de cada usuario agiliza la detección precoz y el bloqueo posterior de cuentas comprometidas, reduciendo su capacidad de daño.

Gracias a esta infraestructura segmentada y con roles específicos, se simplifica enormemente la identificación de anomalías en el tráfico y el comportamiento frente a los sitios de phishing, permitiendo a los equipos de seguridad reaccionar con mayor celeridad y eficacia ante posibles incidentes que pongan en riesgo los datos bancarios.

5.7. Pruebas de vulnerabilidades:

Las pruebas de vulnerabilidades en ciberseguridad en instituciones financieras son cruciales para fortalecer la seguridad de estas entidades. Estas pruebas permiten identificar y corregir debilidades en los sistemas y procesos antes de que puedan ser explotadas por actores malintencionados. Aunque las estadísticas específicas de mejora pueden variar dependiendo de la institución y el tipo de prueba realizada, hay varios indicadores generales que muestran el impacto positivo de estas pruebas:

- Reducción de Incidentes de Ciberseguridad: Las pruebas de vulnerabilidades ayudan a identificar y corregir vulnerabilidades antes de que sean explotadas, lo que reduce significativamente la incidencia de ataques cibernéticos exitosos. Esto se traduce en menos pérdidas financieras, daños a la reputación y multas regulatorias.
- Mejora en la Concienciación y Formación de Empleados: La capacitación periódica y la educación en ciberseguridad mejoran la conciencia de los empleados sobre las amenazas y cómo abordarlas. Esto resulta en un personal más consciente y preparado para identificar y mitigar vulnerabilidades, fortaleciendo así la defensa de la organización.
- Cumplimiento Normativo Mejorado: Las pruebas de vulnerabilidades y la implementación de medidas de seguridad basadas en las recomendaciones de estas pruebas contribuyen al cumplimiento de las regulaciones y estándares de ciberseguridad, como la Ley Gramm-Leach-Bliley, la Ley Sarbanes-Oxley y el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS).

- Adopción de Tendencias Emergentes en Ciberseguridad: Las pruebas de vulnerabilidades pueden revelar áreas donde las instituciones financieras pueden beneficiarse de las últimas tecnologías y prácticas en ciberseguridad, como la inteligencia artificial (IA) y el aprendizaje automático (ML), para mejorar la detección y respuesta a amenazas.
- Preparación para el Futuro: Al adoptar un enfoque de confianza cero, implementar una arquitectura de seguridad en capas y monitorear y actualizar continuamente los controles de ciberseguridad, las instituciones financieras se preparan para enfrentar los desafíos futuros en ciberseguridad. Esto incluye la creciente sofisticación de los ciberataques y la importancia de la seguridad de los datos.

Las pruebas de vulnerabilidades en ciberseguridad son una herramienta esencial para mejorar la seguridad de las instituciones financieras. A través de la identificación y corrección de vulnerabilidades, la mejora de la conciencia y formación de los empleados, el cumplimiento normativo, la adopción de tendencias emergentes y la preparación para el futuro, estas pruebas contribuyen significativamente a fortalecer la ciberseguridad de estas entidades.

Conclusiones

Sin lugar a dudas, el sector financiero, con especial énfasis en el ámbito de BFSI, ha surgido como un enclave primordial para las incursiones perpetradas por agentes malintencionados. En este contexto, resulta imperativo que las entidades financieras y aseguradoras desplieguen una estrategia integral de defensa, respaldada por medidas de seguridad de vanguardia y una filosofía de seguridad proactiva. Este enfoque no solo asegurará la protección de los activos críticos y la confidencialidad de los datos sensibles, sino que también fortalecerá la resiliencia del sector ante las crecientes amenazas cibernéticas.

Es esencial recalcar que los ataques de phishing representan una amenaza persistente, que evoluciona en paralelo con los avances en las infraestructuras tecnológicas y las defensas cibernéticas de las empresas. En este sentido, la constante mejora de las estrategias perpetradas por los ciberdelincuentes busca eludir las salvaguardas implementadas por las organizaciones, comprometiendo tanto a usuarios individuales como a entidades corporativas. Destacadamente, el sector bancario se erige como uno de los principales blancos de estos ataques de ingeniería social, dada su considerable rentabilidad y el potencial impacto que pueden generar en la estabilidad financiera y la confianza del público. Ante esta realidad, la adopción de medidas proactivas, como la concientización de los usuarios y la implementación de sistemas de detección avanzados, se torna indispensable para mitigar los riesgos asociados a esta amenaza en constante evolución.

Para abordar de manera efectiva la evolución constante de las amenazas cibernéticas, resulta imperativo contemplar la instauración de una entidad especializada en ciberinteligencia. Dicha instancia estaría dedicada a la meticulosa investigación de los ataques y suplantaciones dirigidos específicamente hacia la entidad, desentrañando sus estructuras y tácticas subyacentes. Este análisis de alto calibre facultaría a la organización para anticiparse a las maniobras de los ciberdelincuentes, reduciendo significativamente la probabilidad de verse sorprendida y mitigando el riesgo de incidentes o brechas de seguridad que pudieran materializarse. De esta manera, se fortalecería la postura defensiva de la empresa, elevando su capacidad para prevenir y neutralizar potenciales amenazas en el ámbito digital.

Es de vital trascendencia mantener una diligente vigilancia sobre las noticias y tendencias en el ámbito de la ciberseguridad. En este sentido, ninguna entidad corporativa puede considerarse inmune a la eventualidad de un ataque cibernético, y la familiarización con las más recientes modalidades de intrusión posibilita la formulación de controles de seguridad más sofisticados y efectivos. La perpetua actualización de los sistemas de seguridad preexistentes emerge como una premisa fundamental para la adaptación dinámica y la respuesta proactiva ante las amenazas emergentes, consolidando así la capacidad de la organización para salvaguardar sus activos críticos y preservar la integridad de sus operaciones en un entorno digital en constante cambio.

La implementación de soluciones antivirus y antimalware actualizadas, junto con la educación del personal sobre prácticas seguras de navegación, son pilares fundamentales para la prevención efectiva de infecciones por malware. La utilización de listas de control de aplicaciones complementa estas medidas al limitar la ejecución de software no autorizado, fortaleciendo así la postura de seguridad de la organización frente a amenazas potenciales..

La implementación de filtros de correo electrónico, la capacitación del personal y la utilización de soluciones de autenticación de múltiples factores son medidas fundamentales para prevenir ataques de phishing. Al adoptar un enfoque multifacético que aborde tanto la tecnología como el factor humano, la organización puede reducir significativamente el riesgo de comprometer sus credenciales y datos sensibles, fortaleciendo así su postura de seguridad cibernética teniendo en cuenta que este tipo de solución no es tan costosa teniendo en cuenta otras posibles soluciones frente a la prevención de malware.

Bibliografía

[1] “Intentos de fraude digital en servicios financieros llegaron a 243% desde Colombia”. Diario La República. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.larepublica.co/finanzas/intentos-de-fraude-digital-en-servicios-financieros-aumentaron-243-desde-colombia-3183292

[2] Colprensa. “Los intentos de fraude digital en Colombia han crecido 859% en los Ãºltimos tres aÃ±os”. www.elcolombiano.com. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.elcolombiano.com/negocios/aumenta-el-fraude-digital-en-colombia-2023-MG21143168

[3] “Fraude cibernético en bancos solo afecta $5 de cada $100.000, según Asobancaria”. Diario La República. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.larepublica.co/finanzas/el-fraude-cibernetico-en-los-bancos-solo-afecta-5-de-cada-100-000-segun-asobancaria-3245661

[4] “¿Qué están haciendo los bancos para protegerse de los ataques cibernéticos?” Semana.com Últimas Noticias de Colombia y el Mundo. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.semana.com/mejor-colombia/articulo/que-estan-haciendo-los-bancos-para-protegerse-de-los-ataques-ciberneticos/202200/

[5] “¿Qué dice Davivienda sobre los casos de fraude y cómo puede proteger su cuenta?” ELESPECTADOR.COM. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.elespectador.com/economia/finanzas-personales/que-dice-davivienda-sobre-los-casos-de-fraude-y-como-puede-proteger-su-cuenta/

[6] D. R. Filho. “A responsabilidade dos bancos pelos prejuízos resultantes do "phishing"”. Jus.com.br | Jus Navigandi - Tudo de Direito e Justiça. accedido el 9 de marzo de 2024. [En línea]. Disponible:

https://jus.com.br/artigos/11481/a-responsabilidade-dos-bancos-pelos-prejuizos-resultantes-do-phishing/4

[7]Shifting Attack Landscapes and Sectors in Q1 2024 with a 28% increase in cyber attacks globally. (s.f.). Check Point. https://blog.checkpoint.com/research/shifting-attack-landscapes-and-sectors-in-q1-2024-with-a-28-increase-in-cyber-attacks-globally/

[8] I. Belcic. "¿Qué es el malware y cómo protegerse de los ataques?" ¿Qué es el malware y cómo protegerse de los ataques? accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.avast.com/es-es/c-malware

[9] "Qué es un gusano informático y cuáles son sus características". Award-winning news, views, and insight from the ESET security community. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.welivesecurity.com/la-es/2021/11/05/que-es-gusano-informatico-caracteristicas/

[10] I. Belcic. "¿Qué es un gusano informático?" ¿Qué es un gusano informático? Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.avast.com/es-es/c-computer-worm

[11] "Qué es un gusano informático y cómo funciona | NordVPN". NordVPN. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://nordvpn.com/es/blog/que-es-un-gusano-informatico/

[12] "¿Qué es un gusano informático? Los 9 ejemplos más terribles". SoftwareLab. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://softwarelab.org/es/blog/que-es-un-gusano-informatico/

[13] "¿Qué es un gusano informático y cómo funciona?" EasyDMARC. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://easydmarc.com/blog/es/que-es-un-gusano-informatico-y-como-funciona/

[14]"What is Computer Worm? - GeeksforGeeks". GeeksforGeeks. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.geeksforgeeks.org/what-is-computer-worm/

[15] N. Latto. “¿Qué es el adware y cómo puede prevenirlo?” ¿Qué es el adware y cómo puede prevenirlo? Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.avast.com/es-es/c-adware

[16] “Adware - ¿Qué es y cómo eliminarlo? | Malwarebytes”. Malwarebytes. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://es.malwarebytes.com/adware/

[17] “Que es un adware: definición, causas, peligros y soluciones para este tipo de malware”. N26 The Mobile Bank | Voted 'Best bank in the world 2023'. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://n26.com/es-es/blog/adware

[18]“What Is Adware and How Do You Prevent It in 2024?” Security.org. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.security.org/antivirus/adware/

[19] “Tipos de malware y ejemplos”. www.kaspersky.es. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.kaspersky.es/resource-center/threats/types-of-malware

[20] “Guía para la Implementación de Seguridad de la Información en una MIPYME”. MinTic. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf

[21] “¿Cuáles son los virus informáticos más conocidos?” Universidad Online a Distancia | Universidad Isabel I. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.ui1.es/blog-ui1/cuales-son-los-virus-informaticos-mas-conocidos

[22] “¿Qué es un virus troyano? Tipos y cómo eliminarlo”. latam.kaspersky.com. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://latam.kaspersky.com/resource-center/threats/trojans

[23] “¿Qué es un virus troyano? Tipos y cómo eliminarlo”. www.kaspersky.es. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.kaspersky.es/resource-center/threats/trojans

[24] I. Belcic. “¿Qué es un malware troyano? Guía definitiva”. ¿Qué es un malware troyano? Guía definitiva. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.avast.com/es-es/c-trojan

[25]“How the attacker used the Trojan horse to attack”. ResearchGate. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://www.researchgate.net/figure/How-the-attacker-used-the-Trojan-horse-to-attack_fig2_357553876

[26] “Todo lo que debes saber sobre un troyano: Qué es, qué hace y cómo eliminarlo | Blog de McAfee”. Blog de McAfee. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.mcafee.com/blogs/es-mx/internet-security/que-son-los-virus-troyanos-y-como-librarse-de-ellos/

[27] “Qué son los virus troyanos y cómo deshacernos de ellos | McAfee”. McAfee. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.mcafee.com/learn/es/que-son-los-virus-troyanos-y-como-deshacernos-de-ellos/

[28] “¿Qué hacen los troyanos y cómo eliminarlos? | Blog de McAfee”. Blog de McAfee. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.mcafee.com/blogs/es-es/privacy-identity-protection/que-son-los-virus-troyanos-y-como-deshacernos-de-ellos/

[29]“¿Qué es un troyano? Cómo eliminarlo y mantenerse seguro | ESET”. Malware Protection & Internet Security | ESET. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.eset.com/centro-america/troyano/

[30] “What is a Trojan? Is it a virus or is it malware?” Sitio oficial | Norton™: Programas antivirus contra software malicioso. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://mx.norton.com/blog/malware/what-is-a-trojan

[31] “Troyanos - Definición, detección, eliminación y protección”. Hornetsecurity – Servicios de seguridad en nube para empresas. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.hornetsecurity.com/es/knowledge-base/troyanos/

[32] G. Julián. “¿Qué es un troyano, cómo funciona y cómo podemos protegernos?” Genbeta - Software, internet y productividad. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.genbeta.com/seguridad/que-es-un-troyano-como-funciona-y-como-podemos-protegernos

[33] D. Ghimiray. “¿Qué es una bomba lógica? Cómo impedir los ataques de bomba lógica”. ¿Qué es una bomba lógica? Cómo impedir los ataques de bomba lógica. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.avast.com/es-es/c-what-is-a-logic-bomb

[34] Colaboradores de los proyectos Wikimedia. “Bomba lógica - Wikipedia, la enciclopedia libre”. Wikipedia, la enciclopedia libre. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://es.wikipedia.org/wiki/Bomba_lógica

[35] “Bomba lógica: características, tipos, usos... - MSMK University”. MSMK. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://msmk.university/ciberseguridad/bomba-logica

[36]“Working of Logic Bomb.” ResearchGate. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://researchgate.net/figure/Working-of-Logic-Bomb_fig1_342761639

[37] “¿Qué Hace una Bomba Lógica?” Master en Ciberseguridad Online. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://masterenciberseguridadonline.es/internet/que-hace-una-bomba-logica/

[38] “One moment, please...” One moment, please... Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://brianur.info/conociendo-y-creando-una-bomba-logica/

[39] “Bomba Lógica”. Asperis Security. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.asperis.es/glosario-ciberseguridad/bomba-logica/

[40] “¿Qué es una bomba lógica? | TecnoNautas”. TecnoNautas. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://tecnonautas.net/que-es-una-bomba-logica/

[41] “El banco chino ICBC sufre un ciberataque a sus servicios financieros en Estados Unidos”. El País. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://elpais.com/economia/2023-11-10/el-banco-chino-icbc-sufre-un-ciberataque-a-sus-servicios-financieros-en-estados-unidos.html

[42] “Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera”. IMF BLOG. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[43] “Hackeo a oleoducto enciende alarmas sobre bancos y bolsa”. CNN. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://cnnespanol.cnn.com/2021/05/13/hackers-oleoducto-bancos-bolsas-objetivos-eeuu-trax/

[44] “En el sector de servicios financieros, Brasil encabeza lista de objetivos para ataques”. Cointelegraph. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://es.cointelegraph.com/news/crypto-lender-genesis-allegedly-owes-900m-to-gemini-s-clients-report

[45] “Las instituciones financieras de América Latina son uno de los principales objetivos de los ciberdelincuentes”. GlobalSign. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.globalsign.com/es/blog/Las-instituciones-financieras-de-america-latina

[46]“Ransomware attack phases.” ResearchGate. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://www.researchgate.net/figure/Ransomware-attack-phases_fig2_357310118

[47]“Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe”. sectorbancariospa. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

[48] “Gobierno y banca, los más afectados por los ataques de ransomware en 2020 | Ventas de Seguridad”. Ventas de Seguridad - El portal para la seguridad electrónica. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.ventasdeseguridad.com/2021042712649/noticias/empresas/gobierno-y-banca-los-mas-afectados-por-los-ataques-de-ransomware-en-2020.html

[49] “Panorama de amenazas que afectan al sector financiero”. Threat_Intelligence. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/933/

[50] “Evaluación de la Ciberseguridad en el Sistema Financiero Mexicano”. Banxico, banco central, Banco de México. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/recuadros/%7B92F809D6-8F09-D3A7-3E81-1D800CEDAEAD%7D.pdf

[51] “Ransomware: qué es y cómo eliminarlo | Malwarebytes”. Malwarebytes. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://es.malwarebytes.com/ransomware/

[52] “Ransomware: qué es y cómo funciona”. Award-winning news, views, and insight from the ESET security community. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.welivesecurity.com/la-es/2021/05/21/que-es-ransomware/

[53] “¿Qué es el ransomware? | IBM”. IBM in Deutschland, Österreich und der Schweiz. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.ibm.com/es-es/topics/ransomware

[54] “Informe sobre las amenazas DDoS en el 4º trimestre de 2023”. cloudflare. [En línea]. Disponible: https://blog.cloudflare.com/ddos-threat-report-2023-q4-es-es/

[55] “Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera”. IMF BLOG. Accedido el 9 de mayo de 2024. [En línea]. Disponible:

https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[56]“What is a DDoS Attack: Types, Prevention & Remediation | OneLogin”. OneLogin: Market-Leading Identity and Access Management Solutions. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.onelogin.com/learn/ddos-attack

[57] J. L. Reus. “Reconoce Banxico 16 hackeos a bancos”. El Financiero. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.elfinanciero.com.mx/economia/2021/06/04/reconoce-banxico-16-hackeos-a-bancos/

[58] “Panorama de amenazas que afectan al sector financiero”. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/933/

[59] Y. Fernández. “Qué es un ataque DDoS y cómo puede afectarte”. Xataka - Tecnología y gadgets, móviles, informática, electrónica. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.xataka.com/basics/que-es-un-ataque-ddos-y-como-puede-afectarte

[60] “¿Qué es un ataque DDoS? Significado, definición y tipos | Fortinet”. Fortinet. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.fortinet.com/lat/resources/cyberglossary/ddos-attack

[61] “Ataques DDoS: tipos, protección y mitigación”. Stackscale. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.stackscale.com/es/blog/ataques-ddos/

[62] “Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera”. IMF BLOG. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[63] “Ciberseguridad en el sector bancario: Principales amenazas y prevención”. PowerDMARC. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://powerdmarc.com/es/cyber-security-in-banking/

[64] “Tipos de malware y ejemplos”. www.kaspersky.es. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.kaspersky.es/resource-center/threats/types-of-malware

[65] “¿Qué es spear phishing? | IBM”. IBM in Deutschland, Österreich und der Schweiz. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.ibm.com/mx-es/topics/spear-phishing#:~:text=IBM-,¿Qué%20es%20spear%20phishing?,pagos%20de%20autorización%20al%20atacante.

[66]“¿Qué es un ataque de phishing?” CLOUDFLARE. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://www.cloudflare.com/es-es/learning/access-management/phishing-attack/

[67]Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.incibe.es/aprendeciberseguridad/spear-phishing

[68] “What is phishing? Examples, types, and techniques”. CSO Online. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html.

[69] E. Sardanyés. “Todos los tipos de ataques de Phishing”. ESED | Ciberseguridad | Servicios informáticos. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.esedsl.com/blog/todos-los-tipos-de-ataques-de-phishing

[70] “¿Qué es Spear Phishing?” Hornetsecurity – Servicios de seguridad en nube para empresas. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.hornetsecurity.com/es/knowledge-base/spear-phishing/

[71]“¿Qué es el whale phishing? | IBM”. IBM in Deutschland, Österreich und der Schweiz. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.ibm.com/mx-es/topics/whale-phishing#:~:text=IBM-,¿Qué%20es%20el%20whale%20phishing?,de%20texto%20o%20llamadas%20telefónicas.

[72]“Phishing, Vishing, Smishing, Â¿quÃ© son y cÃ³mo protegerse?” BBVA NOTICIAS. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/#:~:text=El%20término%20deriva%20de%20la,información%20previamente%20obtenida%20desde%20internet.

[73]“¿Qué es Smishing (SMS Phishing)? | IBM”. IBM in Deutschland, Österreich und der Schweiz. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.ibm.com/mx-es/topics/smishing#:~:text=¿Qué%20es%20el%20smishing?,envíen%20dinero%20a%20delincuentes%20cibernéticos.

[74]“¿Qué es Smishing (phishing por SMS)? | IBM”. IBM in Deutschland, Österreich und der Schweiz. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.ibm.com/es-es/topics/smishing

[75]“¿Cuáles Son los Distintos Tipos de Phishing?” Trend Micro. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.trendmicro.com/es_mx/what-is/phishing/types-of-phishing.html#:~:text=El%20phishing%20por%20motores%20de,el%20sitio%20web%20del%20hacker.

[76]“Qué es el pharming y cómo protegerte”. latam.kaspersky.com. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://latam.kaspersky.com/resource-center/definitions/pharming

[77]R. Badillo. “Así quiere acabar WhatsApp con las estafas: cómo podrás bloquear el 'spam' sin abrirlo”. elconfidencial.com. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.elconfidencial.com/tecnologia/2024-02-12/whatsapp-bloquear-contactos-desde-notificacion_3828779/#:~:text=El%20phishing%20es%20una%20práctica,acceder%20a%20sus%20cuentas%20bancarias.

[78]“Ransomware, malware y phishing. ¿Cuál es la diferencia?” Skysnag. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.skysnag.com/es/blog/ransomware-vs-malware-vs-phishing-what-is-the-difference/

[79]Á. G. M. “Qrishing, las estafas con códigos QR que pueden llevar a infectar tu móvil de virus e incluso robarte dinero”. Xataka Android - Sistema operativo móviles Google, Play store, Apps. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.xatakandroid.com/seguridad/qrishing-estafas-codigos-qr-que-pueden-llevar-a-infectar-tu-movil-virus-e-incluso-robarte-dinero

[80] “LAS 3 AMENAZAS CIBERNÉTICAS QUE MÁS AFECTAN AL SECTOR FINANCIERO EN 2022”. Grupo Smartekh Blog. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://blog.smartekh.com/las-3-amenazas-cibernéticas-que-más-afectan-al-sector-financiero-en-2022

[81] “ANÁLISIS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL QUE AMENAZAN LA SEGURIDAD INFORMÁTICA DE USUARIOS DE ENTIDADES FINANCIERAS”. Universidad Nacional Abierta y a Distancia UNAD. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://repository.unad.edu.co/bitstream/handle/10596/55080/jcmalagonl-.pdf?sequence=3&isAllowed=y

[82] “Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe”. sectorbancariospa. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

[83] CyberSecurity News. “CyberSecurity News on LinkedIn: 5 ataques de ingeniería social que las empresas deben conocer y prevenir -…”. LinkedIn: Log In or Sign Up. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.linkedin.com/posts/cybersecuritynews_5-ataques-de-ingeniería-social-que-las-empresas-activity-7029449048839401472-rJJg?trk=public_profile_like_view

[84] “Estadísticas y datos sobre el phishing para 2019–2022”. Comparitech. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.comparitech.com/es/blog/vpn-privacidad/phishing-estadisticas-datos/

[85] “Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe”. sectorbancariospa. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

[86]“MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky”. MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://cybermap.kaspersky.com/es

[87] “Ataques de ingeniería social con IA generativa – Nationwide”. Compañía de servicios financieros y seguros – Nationwide. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://espanol.nationwide.com/lc/resources/cyber-resource-center/articles/social-engineering-attacks-using-generative-ai

[88] C. Lamberti. “Hay 544 ataques de phishing por minuto en América Latina: cómo protegerse”. El Cronista. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.cronista.com/infotechnology/actualidad/hay-544-ataques-de-phishing-por-minuto-en-america-latina-como-protegerse/

[89] “NUEVAS CIBERAMENAZAS DESAFÍAN AL SECTOR DE SERVICIOS FINANCIEROS EN 2024”. PR Newswire: press release distribution, targeting, monitoring and marketing. Accedido el 9 de mayo de 2024. [En línea]. Disponible: https://www.prnewswire.com/mx/comunicados-de-prensa/nuevas-ciberamenazas-desafian-al-sector-de-servicios-financieros-en-2024-302101863.html

[90]“Cyber Attacks on Financial Institutions | Why Banks Are Caught in the Crosshairs”. SentinelOne. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.sentinelone.com/blog/a-cyberwar-on-financial-institutions-why-banks-are-caught-in-the-crosshairs/#:~:text=As%20of%20December%202022,%20finance,the%2034%%20reported%20in%202021.

[91]accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

[92]“The 6 Biggest Cyber Threats for Financial Services in 2024 | UpGuard”. Third-Party Risk and Attack Surface Management Software | UpGuard. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

[93]E. Sayegh. “Potential For Devastation: The Impact Of A Cyberattack On The Banking System”. Forbes. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.forbes.com/sites/emilsayegh/2023/06/06/potential-for-devastation-the-impact-of-a-cyberattack-on-the-banking-system/

[94]M. Gross. “Phishing Attacks Target the Financial Industry”. 403 Forbidden. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.rbadvisoryllc.com/phishing-attacks-target-the-financial-industry

[95]“Types of Cyberattacks on Financial Institutions | Fortinet”. Fortinet. accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.fortinet.com/solutions/industries/financial-services/types-of-cyberattacks-on-financial-institutions