Ataques de phishing y cómo prevenirlos

Phishing attacks and how to prevent them

Javier Guaña-Moya
Pontificia Universidad Católica del Ecuador (PUCE)
Quito, Ecuador
eguana953@puce.edu.ec

Marco Chiluisa-Chiluisa
Universidad Central del Ecuador (UCE)
Quito, Ecuador
machiluisa@uce.educ.ec

Paulina del Carmen Jaramillo-Flores
Instituto Superior Tecnológico Japón (ISTJ)
Quito, Ecuador
pjaramillo@itsjapon.edu.ec

Darwin Naranjo-Villota
Ministerio de Educación
Bolívar- Ecuador
darwin.naranjo@educacion.gob.ec

Eugenio Rafael Mora-Zambrano
Instituto Superior Tecnológico Japón (ISTJ)
Quito, Ecuador
gmora@itsjapon.edu.ec

Lenin Gerardo Larrea-Torres
Instituto Ecuatoriano de Seguridad Social
Quito-Ecuador
lenin.larrea@iess.gob.ec

Resumen — **El vertiginoso avance tecnológico relacionado con la globalización y la nueva era digital ha propiciado el diseño de técnicas y herramientas novedosas que hacen frente a los riesgos de la tecnología y la información. Destacan términos como "ciberseguridad" que corresponde a aquella área de las ciencias de computación que se encarga del desarrollo e implementación de los mecanismos de protección de la información y de la infraestructura tecnológica, con el fin de hacerle frente a ataques cibernéticos. El phishing, es un delito que emplea ingeniería social y subterfugios técnicos sobre esto para robar datos de identidad personal y credenciales de cuentas financieras de los usuarios, representando un alto riesgo económico y financiero a nivel mundial, tanto para los individuos como para las grandes organizaciones. El objetivo de la presente investigación es determinar las formas de prevenir el phishing, mediante el análisis de las características de este fraude informático, las diversas modalidades existentes y las principales estrategias de prevención, con el fin de incrementar el conocimiento de los usuarios acerca de este tema, resaltando la importancia de una formación adecuada que permita establecer mecanismos eficientes para detectar y bloquear el phishing.**

Palabras Clave – phishing; delitos cibernéticos; ataques informáticos; ciberseguridad.

Abstract — **The vertiginous technological advance related to globalization and the new digital era has led to the design of new techniques and tools that deal with the risks of technology and information. Terms such as "cybersecurity" stand out, which corresponds to that area of computer science that is responsible for the development and implementation of information protection mechanisms and technological infrastructure, in order to deal with cyberattacks. Phishing is a crime that uses social engineering and technical subterfuge to steal personal identity data and financial account credentials from users, representing a high economic and financial risk worldwide, both for individuals and for large organizations. The objective of this research is to determine the ways to prevent phishing, by analyzing the characteristics of this computer fraud, the various existing modalities and the main prevention strategies, in order to increase the knowledge of users about this. subject, highlighting the importance of adequate training that allows establishing efficient mechanisms to detect and block phishing.**

Keywords – phishing; cybercrimes; computer attacks; cyber security.

I. INTRODUCCIÓN

El uso de tecnologías cada vez más novedosas para cometer ataques cibernéticos contra gobiernos, negocios e individuos, ha fomentado el empleo de palabras y frases, tal como ataques cibernéticos o ciberdelitos, que una década atrás apenas se conocían, formando en la actualidad parte del vocabulario diario. Estos delitos no se limitan con fronteras físicas, ni virtuales, y poseen la capacidad de ocasionar importantes daños, suponiendo un riesgo real para las víctimas de todo el mundo [1].

Entre estos ciberataques se encuentran los ataques de phishing que representan actualmente uno de los desafíos de seguridad más comunes que enfrentan tanto las personas como las empresas para mantener la información segura. Los piratas informáticos utilizan el correo electrónico, las redes sociales, las llamadas telefónicas y cualquier forma de comunicación que les permita tener acceso a datos valiosos, bien sea para obtener contraseñas, tarjetas de crédito u otra información confidencial, constituyendo las organizaciones objetivos particularmente valiosos [2].

Especialmente en tiempos de crisis, como la pandemia de coronavirus, los ciberdelincuentes aprovechan el momento para atraer a las víctimas a que muerdan el anzuelo de phishing, debido que las personas están nerviosas y desean información

continua, buscando orientación de empleadores, gobiernos y autoridades pertinentes, por lo que un correo electrónico que supuestamente proviene de alguna de estas fuentes, que ofrece nueva información e indica a los destinatarios que completen una tarea rápidamente, probablemente recibirá menos desconfianza que antes de la crisis, resultando un clic impulsivo en un dispositivo infectado o una cuenta comprometida [3].

Por tanto, entender los riesgos de los ataques de phishing y conocer las modalidades más comunes es un primer paso importante para protegerse contra ellos.

II. PHISHING

A. *Fraudes informáticos*

Desde mediados de la década anterior han aparecido múltiples tipos de fraudes informáticos, por medio de sistemas o redes informáticas de transmisión e intercambio de datos por Internet, que forman parte de lo que se conoce como "cibercriminalidad", que tiene como objetivo apoderarse de información personal de los usuarios de Internet, accediendo a cuentas de correo y/o redes sociales, buscando obtener también datos de los contactos virtuales.

La finalidad de estos fraudes es comerciarlos ilícitamente, así como tener acceso a claves de banca electrónica para de este modo ingresar a las cuentas bancarias de los titulares y disponer del dinero que en ellas se encuentra, modalidad que se conoce como phishing [4].

B. *Definición de phishing*

El phishing es un tipo de ataque de ciberseguridad por medio del cual los expertos informáticos (phisher), de manera malintencionada, envían mensajes haciéndose pasar por una persona o entidad de confianza, con la finalidad de manipular a los usuarios, propiciando que realice acciones como instalar un archivo malicioso, hacer clic en un enlace falso o divulgar información confidencial como credenciales de acceso.

El phishing representa el tipo más común de ingeniería social, término general que describe los intentos de manipular o engañar a los usuarios de computadoras. La ingeniería social es un vector de amenazas cada vez más común que se utiliza en casi todos los incidentes de seguridad, que, generalmente, combina el phishing con otras amenazas, como malware, inyección de código y ataques a la red [5].

De acuerdo a lo anterior, el phishing se puede definir como la pesca de datos personales a través de Internet que se realiza, generalmente, por medio del envío masivo de correos electrónicos con enlaces a páginas "web" falsas que imitan el contenido o la imagen de un determinada entidad financiera o bancaria, engañando al destinatario del mensaje con la finalidad de sustraer la información personal que posibilita el acceso a las cuentas personales.

Lo anterior permite a los ciberdelincuentes hacer retiros de dinero o bien realizar compras no consentidas por Internet, siendo estos ataques de phishing, especialmente en la actualidad, efectivos por la dificultad para ser detectados, ya que el correo electrónico o mensaje malicioso es convincente y se hace pasar por una fuente confiable conocida por el usuario [6].

C. *Tipos de ataque de phishing*

Los ciberdelincuentes elaboran comunicaciones, fundamentalmente por medio de SMS, correos electrónicos, contenido basado en voz y cuentas de redes sociales, que crean una sensación de urgencia, pánico o infunden miedo en los destinatarios y/o usuarios, encontrando que las líneas de asunto y los subtítulos son llamativos y atraen a la víctima para que realice la acción necesaria.

En los ataques menos sofisticados, los usuarios no son redirigidos a otro sitio web, en estos casos plantean a las victimas acciones simples como hacer clic en un enlace, mientras que, en ataques más sofisticados, se utilizan los kits de phishing fácilmente disponibles, los cuales permiten a los phishers con habilidades técnicas mínimas orquestar fácilmente ataques de phishing, desde recopilar listas de correo hasta falsificar marcas legítimas y configurar sitios web falsos [7].

La susceptibilidad al phishing varía entre individuos de acuerdo a los atributos y nivel de conciencia, por lo que, en la mayoría de los ataques, los phishers explotan la naturaleza humana para piratear, en lugar de utilizar tecnologías sofisticadas. Por otra parte, los ciberdelincuentes siempre aprovechan situaciones de desastres y eventos mundiales para su propio beneficio, tal es el caso de la pandemia por COVID-19, donde los phishers diseñaron una variedad de ataques temáticos de phishing y malware contra trabajadores, instalaciones de atención médica e incluso el público en general, basado en la incertidumbre y poca información que existía en el inicio[8].

Inicialmente, los phisher se valían de la curiosidad y la urgencia como factores desencadenantes más comunes que influenciaban a las personas a responder a este tipo de ataques. Posteriormente, reemplazaron estos factores por el entretenimiento, las redes sociales y la recompensa como los principales motivadores emocionales, por lo que, en el escenario de los ataques de los phishers, los factores psicológicos frecuentemente superan las decisiones conscientes de las personas [9].

Entre los diversos tipos de phishing se puede mencionar:

- **Estafas de phishing por correo electrónico**: Corresponde a mensajes fraudulentos enviados de forma masiva a usuarios aleatorios por medio del correo electrónico, generalmente registran nombres de dominio falsos que imitan organizaciones reales y envían miles de solicitudes comunes a las víctimas.
- **Spear phishing**: Modalidad de phishing altamente dirigido, que ataca a usuarios específicos, con frecuencia el phisher ya tiene parte o toda la información de la víctima, tal como: nombre, lugar de trabajo, profesión, dirección de correo electrónico, información específica sobre el puesto de trabajo, colegas de confianza, familiares u otros contactos.
- **Whaling**: Ataques dirigidos específicamente a directores ejecutivos u otros ejecutivos de alto nivel en función de perfiles detallados, en este caso suelen tener acceso a la información de los empleados senior quienes poseen mucha información de dominio público, usando los atacantes esta información para diseñar ataques altamente efectivos.

- **Smishing**: Corresponde a alertas fraudulentas de SMS, por lo general se trata de mensajes que aparentemente provienen de una institución bancaria de confianza para el usuario, donde solicitan información personal o financiera, como el número de cuenta o claves de cajero automático.
- **Vishing**: Suplantación de identidad organizada por medio de llamadas telefónicas u otros medios basados en voz que puede implicar también llamadas telefónicas automáticas que fingen ser de una entidad de confianza y le solicitan a la víctima que escriba detalles personales usando el teclado del teléfono.
- **Pharming**: En este caso los usuarios son redirigidos a sitios web fraudulentos mediante la manipulación técnica de las direcciones DNS que son utilizadas por un determinado usuario, reconduciendo la navegación que este realiza a sitios web que presentan un aspecto idéntico, sin embargo, son falsos y han sido creados con fines de estafa.
- **Phishing en redes sociales**: Se emplean las plataformas de redes sociales, como Instagram, Facebook, LinkedIn, y Twitter para organizar este tipo de ataques. En estos casos los atacantes se aprovechan de la tendencia de los consumidores a presentar quejas y solicitar asistencia a las marcas a través de los canales de las propias redes sociales. Sin embargo, en lugar de contactar a la marca real, el consumidor contacta a la cuenta social falsa del atacante.

D. Phishing en cifras

De acuerdo a las estadísticas publicadas por Security Boulevard [10] referente al phishing, se destaca que, desde la mitad del año 2020, este tipo de ataques se ha incrementado vertiginosamente, particularmente porque son muy creativos y explotan la pandemia global de Covid-19, indicando, además, que las víctimas objetivo son objeto de phishing con regularidad.

Entre los puntos que más destacan de este informe se pueden mencionar:

- El Informe de Investigaciones de violación de datos (DBIR) de 2019 de Verizon [11] afirma que en los ataques que involucran phishing de una forma u otra evidenciaron un incremento del 32%, cubriendo aproximadamente un tercio de todas las violaciones de datos.
- Alrededor del 86% de los ataques de correo electrónico involucraron correos electrónicos “sin malware”; en lugar de malware, utilizando cada vez más nuevos ataques sofisticados, como el phishing selectivo, fraude CEO, el fraude del director ejecutivo o tácticas de suplantación de identidad, según datos de abril a junio del 2019 de FireEye [12].
- Igualmente, en el 2019 el 88% de las organizaciones informaron haber enfrentado ataques de phishing selectivo, lo que resultó en que el 46% recibiera demandas de ransomware y el 25% de las pequeñas y medianas empresas sufrieran ataques de phishing, de acuerdo a los datos del Informe de Estado del Phish, publicado por Proofpoint en 2020 [13].
- El 57% de las organizaciones reportaron ataques de phishing móvil a través de SMS y WhatsApp, así como llamadas telefónicas de voz usando mensajería, redes sociales e incluso aplicaciones de juegos.
- Aproximadamente el 74% de los ataques de phishing involucraron el protocolo HTTPS, usando certificados SSL/TLS, en comparación con el 54% registrado en el segundo trimestre de 2019 y el 68% del tercer trimestre de 2019, destacando que, de estos, el correo web o el software como servicio estuvieron involucrados en el 31% de los ataques de phishing [14].
- Un estudio realizado donde se accedieron a 800 páginas de phishing con los navegadores web usados con más frecuencia determinó que los que presentaron la mejor protección son Mozilla Firefox y Microsoft Edge de Windows demostrando que fueron capaces de bloquear más del 80% de las amenazas, mientras que Google Chrome, que es el navegador más usado por los usuarios de habla hispana, bloqueó solamente el 28% de las páginas fraudulentas en el sistema operativo Windows y el 25% en el sistema operativo Mac, representando la mitad de la capacidad de bloqueo con respecto al año anterior [15].
- Respecto a la pandemia, el Informe de Panorama de Amenazas Móviles de 2020 de RiskIQ [16], señala que aparece un sitio nuevo de phishing cada 20 segundos, lo cual significa que cada minuto, tres nuevos sitios de phishing diseñados para apuntar a los usuarios aparecen en Internet, especialmente de temas relacionados con el Covid-19.
- Entre enero y marzo de 2020, se registraron 51 mil dominios con temática de coronavirus en todo el mundo y en abril del mismo año, los ciberdelincuentes enviaron 18 millones de correos electrónicos de phishing relacionados con el Covid-19, razón por la cual Google informó que bloqueó más de 250 millones de correos electrónicos no deseados y de phishing relativos a la pandemia [17].

En lo relativo a las empresas tecnológicas y las diversas redes sociales, hasta el 2020 se evidenció que Apple fue la organización comercial más imitada para sitios web clonados y de phishing, mientras que Facebook el portal emulado número uno entre los sitios de redes sociales.

Para finales del 2021, de acuerdo a los datos de Check Point [18] las redes sociales consolidan la posición entre los tres sectores más suplantados, con WhatsApp y LinkedIn entre las marcas más plagiadas (Fig. 1).

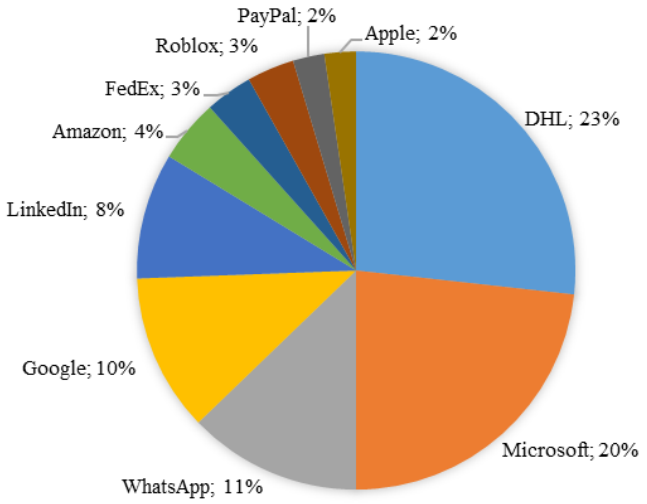

Figura 1. Phishing de marcas en el 4to trimestre de 2021

Por otra parte, los archivos de Microsoft Office y Adobe Acrobat representaron en el 2020 el 94% de los archivos adjuntos de malware en los correos electrónicos, lo que significa un aumento del 15% en 2018 y de 25% en 2019 [6].

E. Tendencia mundial

Desde el punto de vista global, Kaspersky Labs en el Informe Spam and Phishing de 2019 [19], señala que entre algunas de las principales estadísticas de phishing relacionadas con los diferentes países se encuentra que Venezuela ocupó el puesto número 1 con el 31,16% de las víctimas de ataques de phishing, seguido de Brasil con el 30,26%, Grecia con el 25,96%, Australia con el 25,24%, Argelia con 23,93%, Chile con 23,84%, Reunión 23,82%, Ecuador 23,53% y Guayana Francesa con el 22,94% (Fig. 2).

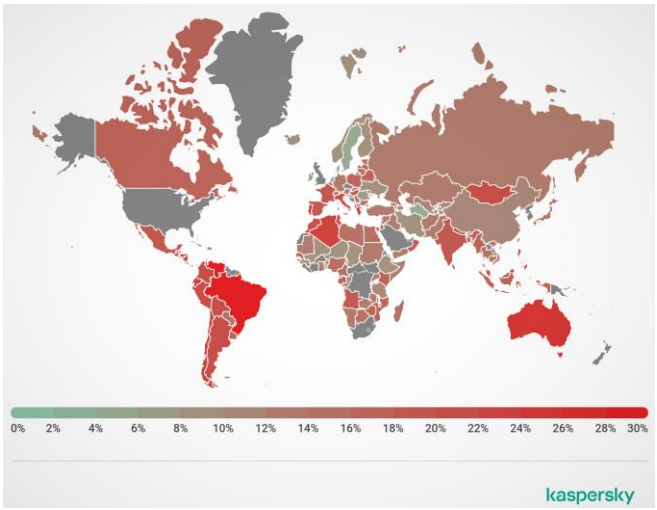

Figura 2. Países por porcentaje de usuarios atacados

Resaltan algunos casos como el de Brasil, donde los ataques de phishing aumentaron un 232% entre febrero y diciembre de 2019, es decir, un lapso de solamente 10 meses y Puerto Rico donde el gobierno perdió más de 2,6 millones de dólares luego que uno de los empleados fuera víctima de un ataque de phishing por correo electrónico.

Por otra parte, la mayor fuente de spam se originó en China con un 21,26%, ubicándose por delante de EE. UU y Rusia con 14,39% y 5,21%, respectivamente, le siguen Brasil con 5,02%, Francia con 3%, India con 2,84%, Vietnam el 2,62%, completando el top 10 Alemania con el 2,61%, Turquía con 2,15% y Singapur con el 1,72% [19] (Fig. 3).

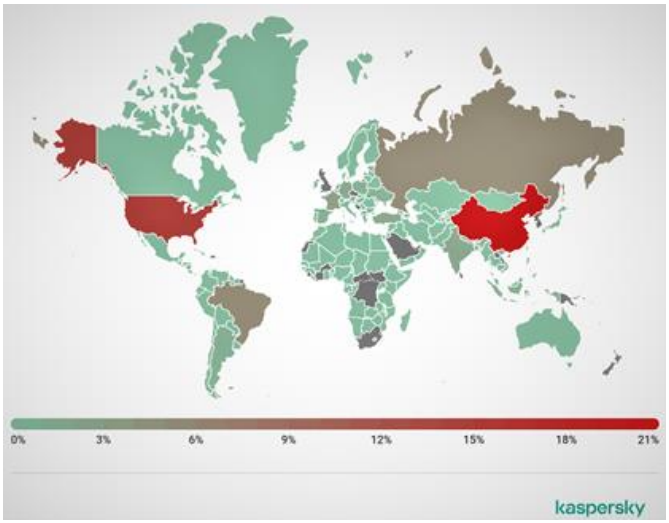

Figura 3. Fuente de spam por país

F. Prevención de los ataques de phishing

Es fundamental que las organizaciones eduquen a los empleados para prevenir ataques de phishing, particularmente en aquellas técnicas que sirvan para reconocer correos electrónicos, enlaces y archivos adjuntos sospechosos, considerando que los delincuentes cibernéticos se encuentran constantemente refinando técnicas, razón por la cual la educación continua es vital [20], tomando en cuenta que, de acuerdo al Data Breach Investigation Report de Verizon [11], ocho de cada diez ataques efectivos por phishing implicaron una falla en el factor humano.

Es importante conocer que un ataque de phishing posee tres componentes básicos:

1. Se realiza por medio de comunicaciones electrónicas, bien sea por correo electrónico o a través de las redes sociales.
2. El delincuente informático suplanta la identidad de una persona u organización de confianza empleando herramientas de ingeniería social con los que intenta manipular a los usuarios, siendo cada vez más sofisticados y elaborados los engaños, como crear perfiles falsos, elaborar diseños idénticos a los que emplean las organizaciones reales, etc.
3. El objetivo del phishing es tener acceso a la información confidencial de las personas, es decir, usuarios y contraseñas de banca digital, números de tarjeta de crédito, entre otros [21].

Asimismo, entre los principales signos indicativos acerca de mensajes y correos electrónicos de phishing se tiene:

- Ofertas consideradas demasiado buenas para ser verdad.
- Remitente inusual o desconocido.
- Errores de ortografía y gramática.
- Amenazas, tal como el cierre de cuenta o eliminación de usuarios, entre otros, particularmente cuando transmiten un sentido de urgencia.
- Enlaces desconocidos, especialmente cuando la URL de destino es diferente a la que aparece en el contenido del correo electrónico.
- Archivos adjuntos inesperados, especialmente aquellos archivos con la extensión .exe.

Por tanto, algunas de las medidas o técnicas de seguridad fundamentales pueden incluir:

- Autenticación mediante dos factores, incorporando dos métodos de confirmación de identidad, tal como pueden ser una contraseña y un código o clave enviado a un teléfono inteligente.
- Filtros de correo electrónico que utilizan aprendizaje automático y procesamiento de lenguaje natural para marcar mensajes de correo electrónico de alto riesgo. También el protocolo DMARC puede ser útil para prevenir la suplantación de identidad por correo electrónico.
- Inicios de sesión con contraseña aumentada empleando imágenes personales, señales de identidad, máscaras de seguridad, entre otras medidas de seguridad.

Este conocimiento es importante, tomando en cuenta que los propios usuarios representan el mejor canal por medio del cual es posible detectar, informar y defenderse de los ataques de phishing, debido que no importa qué tan segura sea la plataforma de seguridad informática de una empresa, esta será tan segura como su base de usuarios lo permita.

Se puede aplicar el enfoque de prevención del phishing desde cinco ópticas, que son:

1. Educación extensa y continua del usuario

Las mejores prácticas de prevención del phishing determinan que todos los usuarios, bien sean empleados, clientes, usuarios finales, socios, etc., deben ser educados de manera continua y exhaustiva a través de un programa estructurado, considerando que la concientización y el entrenamiento humano son el enfoque primario de defensa en la metodología antiphising, al permitir que los usuarios sean conscientes de las señales que deben buscar y las formas de protegerse, incluyendo herramientas atractivas que permitan cometer errores y aprender de ellos [8].

2. Autenticación multifactorial

La autenticación multifactor, también conocida como MFA, es una barrera técnica simple que agrega capas adicionales de verificación, así se tiene que además del nombre de usuario y la contraseña se debe ingresar, por ejemplo, un código OTP enviado a un número de móvil registrado, un token físico y datos biométricos, evitando así que los phishers utilicen credenciales comprometidas para obtener acceso no autorizado [8].

3. Políticas efectivas de administración de contraseñas y acceso

Además de MFA, todas las organizaciones deben aplicar políticas efectivas de gestión de acceso y contraseñas, tal como roles y privilegios de usuario claramente definidos, cambios frecuentes de contraseñas o barreras para reutilizar contraseñas, entre otros [8].

4. Firewalls de aplicaciones web (WAF) de próxima generación

Los WAF de próxima generación, como AppTrana WAF, están perfectamente equipados para filtrar solicitudes maliciosas en el perímetro antes de que lleguen a la aplicación. Aunque un WAF no se puede emplear para eliminar el canal de phishing y señuelos que envía el pirata informático para que un usuario haga clic en un enlace, aún se puede considerar una capa de defensa para proporcionar otra barrera al atacante si el objetivo del phishing es la aplicación misma, en estos casos el WAF puede identificar y prevenir inyecciones de malware, desfiguraciones y otros ataques causados, como XSS reflejado; además, AppTrana WAF también analiza las solicitudes y decide de manera inteligente si marcar, permitir, bloquear o desafiar a los usuarios [8].

5. Pruebas de seguridad

Representa una medida importante de prevención de ataques de phishing el realizar pruebas de seguridad y pruebas de penetración, debido que permite a las organizaciones detectar puntos débiles del departamento de seguridad de TI, empleando los resultados para mejorar las herramientas de seguridad, educar a los empleados, así como también conocer qué tan conscientes y equipados están los usuarios para evitar y prevenir el phishing [8].

III. CONCLUSIONES

Existen varias medidas de protección que los individuos y las organizaciones pueden aplicar para protegerse contra ese fraude, pero fundamentalmente lo más importante es mantenerse informado acerca de las estrategias actuales de phishing, de tal manera que se pueda confirmar que las políticas y soluciones de seguridad aplicadas pueden eliminar las amenazas a medida que evolucionan.

Es igualmente vital para las organizaciones que los empleados entiendan los tipos de ataques que pueden enfrentar, los riesgos y cómo abordarlos, considerando que mantener empleados informados y sistemas debidamente asegurados son clave para protegerse de estos ciberataques, por tanto, se reitera la importancia de la capacitación a todos los empleados, gerentes y terceros para detectar correos electrónicos de phishing y asegurarse de que sean plenamente conscientes de sus responsabilidades en lo relacionado a la seguridad de la información que manejan, considerando que si los usuarios conocen cómo detectar un posible ataque de phishing, será mucho menos probable que caigan en la trampa.

Finalmente, es fundamental la atención continua para evitar el acceso indebido a la información personal, considerando que a diario surgen estrategias novedosas y sofisticadas de fraude cibernético, por lo que la desconfianza y el cuidado que se tenga para analizar los sitios web en los que se depositan los datos de identidad son la mejor protección.

REFERENCIAS BIBLIOGRÁFICAS

[1] Interpol, «Ciberdelincuencia», Ciberdelincuencia, 2022. https://www.interpol.int/es/Delitos/Ciberdelincuencia.

[2] J. De Groot, «Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2021», Digital Guardian, 9 de septiembre de 2021. https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams.

[3] J. Fruhlinger, «What is phishing? How this cyber attack works and how to prevent it», CSO Online, 4 de septiembre de 2020. https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.

[4] N. Oxman, «Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"», Revista de derecho (Valparaíso), n.o 41, pp. 211-262, dic. 2013, doi: 10.4067/S0718-68512013000200007.

[5] CheckPoint, «¿Qué es el phishing? Tipos de ataques de phishing - Software de Check Point», What is Phishing? Types of Phishing Attacks, 2020. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/#.

[6] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, y S. Arthi, «Why is phishing still successful?», Computer Fraud & Security, vol. 2020, n.o 9, pp. 15-19, sep. 2020, doi: 10.1016/S1361-3723(20)30098-1.

[7] R. Singh, «What are Phishing Attacks And How To Prevent Them? | Indusface Blog», Indusface, 16 de octubre de 2020. https://www.indusface.com/blog/phishing-attacks-what-are-they-and-how-to-prevent-them/.

[8] Z. Alkhalil, C. Hewage, L. Nawaf, y I. Khan, «Phishing Attacks: A Recent Comprehensive Study and a New Anatomy», Frontiers in Computer Science, vol. 3, 2021, Accedido: 6 de abril de 2022. [En línea]. Disponible en: https://www.frontiersin.org/article/10.3389/fcomp.2021.563060

[9] PhishMe, «Enterprise Phishing Resiliency and Defense Report - Cofense», 2017. https://cofense.com/whitepaper/enterprise-phishing-resiliency-and-defense-report/.

[10] C. Crane, «Phishing Statistics: The 29 Latest Phishing Stats to Know in 2020», Security Boulevard, 22 de abril de 2020. https://securityboulevard.com/2020/04/phishing-statistics-the-29-latest-phishing-stats-to-know-in-2020/.

[11] Verizon Business, «2021 DBIR Master's Guide», Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/.

[12] FireEye, «The 3 Ts of Email Attacks: Tactics, Techniques, Targets», FireEye. https://content.fireeye.com/one-email/ig-the-3-ts-of-email-attacks.

[13] G. Egan, «2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike | Proofpoint US», Proofpoint, 23 de enero de 2020. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical.

[14] APWG, «Phishing Activity Trends Report, 4th Quarter 2019». 2020. Accedido: 11 de febrero de 2022. [En línea]. Disponible en: https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

[15] OCU, «Phishing: cómo evitarlo y prevenirlo», www.ocu.org, 2022. https://www.ocu.org/tecnologia/internet-telefonia/consejos/evitar-ataque-phishing.

[16] RisklQ, «2020 Mobile App Threat Landscape Report», 2021. Accedido: 6 de abril de 2022. [En línea]. Disponible en: https://www.riskiq.com/wp-content/uploads/2021/01/RiskIQ-2020-Mobile-App-Threat-Landscape-Report.pdf

[17] D. Zumerle y R. Smith, «Market Guide for Mobile Threat Defense», Market Guide for Mobile Threat Defense, 2021. https://www.jamf.com/resources/white-papers/gartner-market-guide-for-mobile-threat-defense/.

[18] Group IT Digital Media, «Estas son las marcas más suplantadas en los ataques de phishing | Seguridad», IT User, 20 de enero de 2022. https://www.itdigitalsecurity.es/actualidad/2022/01/dhl-supera-a-microsoft-como-la-marca-mas-imitada-por-los-ciberdelincuentes.

[19] Kaspersky Labs, «Spam and phishing in 2019», Spam and phishing in 2019, 2020. https://securelist.com/spam-report-2019/96527/.

[20] Forcepoint, «What is Phishing?», Forcepoint, 9 de agosto de 2018. https://www.forcepoint.com/cyber-edu/phishing-attack.

[21] Asobanca, «Los ataques de phishing alcanzaron su máximo histórico por la pandemia. ¿Cómo huir de ellos?», Asobanca, 13 de octubre de 2021. https://asobanca.org.ec/innovacion-y-tecnologia/los-ataques-de-phishing-alcanzaron-su-maximo-historico-por-la-pandemia-como-huir-de-ellos/.