UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

NOBIEMBRE 2021 – ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

ESTUDIO COMPARATIVO DE TECNOLOGÍAS DE LA SEGURIDAD INFORMÁTICA PHISHING Y SPOOFING PARA LA DETECCIÓN DE UN ATAQUE INFORMATICO.

EGRESADO:

TORRES LOPEZ NELSON IVAN

TUTOR:

ING. LEÓN ACURIO JOFFRE VICENTE

AÑO 2022

RESUMEN

En el presente estudio comparativo de tecnologías de la seguridad informática phishing y spoofing para la detección de un ataque informático se ha ido detallando de manera específica cuales han sido las características, tipos, diferencias y herramientas a utilizar para contrarrestar estos dos métodos que emplean los ciberdelincuentes como es el phishing y spoofing para el robo de la información.

Por ello se realizó una investigación bibliográfica en la que se ha citado de diferentes sitios web las diferentes metodologías que emplean los ciberdelincuentes para cometer sus actos delictivos y en la que se pudo encontrar que el phishing es uno de los más usados en los últimos años ya que implementa métodos muy convincente en la que utilizan la ingeniería social para lograr su cometido.

Además, se sugirió diferentes tipos de herramientas informáticas que ayudan a contrarrestar estos tipos de amenazas cibernéticas.

Palabras claves: ciberdelincuentes, herramientas informáticas, phishing, spoofing, tecnologías de la seguridad, ataques cibernéticos, ingeniería social.

ABSTRACT

In this comparative study of phishing and spoofing computer security technologies for the detection of a computer attack, the characteristics, types, differences and tools to be used to counteract these two methods used by cybercriminals have been specifically detailed. such as phishing and spoofing for information theft.

For this reason, a bibliographical investigation was carried out in which the different methodologies used by cybercriminals to commit their criminal acts have been cited from different websites and in which it was found that phishing is one of the most used in recent years. that implements very convincing methods in which they use social engineering to achieve their goal.

In addition, different types of computer tools were suggested that help counteract these types of cyber threats.

Keywords: cybercriminals, computer tools, phishing, spoofing, security technologies, cyber attacks, social engineering.

INTRODUCCIÓN

En la actualidad las tecnologías específicamente en el ámbito de la seguridad han ido en avance y se han convertido en algo muy común e importantes en los últimos años, una de las ramas que más se ha beneficiado es el comercio electrónico ya que es uno de los temas más discutidos y más implementados en los diferentes tipos de organizaciones a nivel mundial y por supuesto es uno de los más relevantes en el mercado.

Por lo tanto existe una gran variedad de información con respecto al manejo de diversas herramientas informáticas; Aquí es donde los ciberdelincuentes se aprovechan de cualquier descuido no solo de las empresas sino también de las personas físicas, y utilizan técnicas como la ingeniería social con sus métodos fraudulentos para cometer este tipo de delitos, conocido en el mundo de la informática como phishing y spoofing que en términos conceptuales se conoce como la pesca informática o suplantación de identidad.

El objetivo de este estudio comparativo que corresponde a las tecnologías de seguridad como lo es el phishing y el spoofing es conocer por medio de una investigación sus diferencias, prevenciones, como identificarlas y contrarrestarlas, etc. Se procederá a obtener información mediante páginas web, libros, como estos tipos de tecnologías de seguridad funcionan y efectuarían un ataque en una empresa o persona y así ir destacando cuál de estos tipos de ataques son los más comunes y cómo prevenirlo o evitar estar expuesto a ese riesgo.

En el presente proyecto investigativo que se está redactando se utilizara la siguiente línea de investigación de sistemas de información y comunicación, emprendimiento e innovación y su sublínea de investigación redes y tecnologías inteligentes de software y hardware en la que

ayudará con el desarrollo del Estudio comparativo de tecnologías de la seguridad informática phishing y spoofing para la detección de un ataque informático.

El phishing y el spoofing para muchas empresas o personas son difíciles en detectar, pero no imposible ya que la mayoría de los que implementan estos tipos de ataques dejan pistas mínimas de cómo identificar cuando es un ataque cibernético, es por eso que esta investigación será de citas, fuentes bibliográficas y páginas web relacionados a los ataques cibernéticos.

En este presente proyecto se utilizó el método descriptivo que servirá para recolectar, resumir, organizar y presentar información que se ha podido recopilar en diferentes sitios web o fuentes bibliográficas. Que consiste en explicar y evaluar características, diferencias y prevenciones de los ciberataques. El fin de este método descriptivo es ir seleccionando información que existe sobre el estudio de estas tecnologías en comparación.

DESARROLLO

En la actualidad muchas empresas y personas en general han sido víctimas de ataques cibernéticos y una de las más comunes es el phishing y spoofing, denominada pesca informática o suplantación de identidad que se dan mediante la ingeniería social.

La gran mayoría que son víctimas de estos ataques tienden hacer fáciles de manipular ya que no poseen un sistema de seguridad actualizado, programas sin parches ni licencias de seguridad y a páginas a las que se visitan sin restricciones y por ende para los atacantes son más fáciles de vulnerar.

"Ilustración 1. Phishing vs Spoofing "Tecnología de la Informática"

Fuentes: (Velazquez, 2021)

Los ciberdelincuentes que generalmente practican el phishing y el spoofing comúnmente lo realizan en su mayoría por medio de correos electrónicos falsos, SMS, redes sociales, creando sitios web falsos o incluso en llamadas telefónicas utilizando tácticas como la ingeniería social en la que el atacante se hace pasar por alguna entidad pública en general, tratando así de poder obtener información y a su vez utilizar la misma para beneficios maliciosos.

Las víctimas de estos ciberataques tienden a caer fácilmente ya que el atacante los manipula psicológicamente enviando correos electrónicos o creando sitios web similares a los de una entidad bancaria, proveedor de internet, o cualquier empresa en la que este afiliado su víctima, y que poseen estos correos o sitios web que los pueden hacer vulnerables a un ciberataque es el contenido, en el que la mayoría de los casos pide el cambio de actualización personal de sus cuentas bancarias, envían archivos adjunto con contenidos maliciosos o URL que al darles clic traen archivos descargables no autorizados conocido como ransomware que infectan a los sistemas del computador con malware mediante códigos maliciosos que codifican la información del computador dejando así a la víctima sin acceso a sus datos y programas y pudiendo obtener toda la información posible que por consiguiente utilizan para beneficio propio mediante la extorción para demandar un rescate por la información robada y lucrarse económicamente de la misma. (ESET., 2022).

Muchos piensan que el phishing y el spoofing son lo mismo porque ambas se basan generalmente en el delito informático, por eso cabe recalcar que se pueden usar ambas para realizar un acto informático fraudulenta, así como también no se podrían usarlas si así desea el atacante ya que no son dependientes (Lima., 2022).

Por ende se ha optado por realizar un cuadro en el que se detallará las diferencias más importantes que tienen estas tecnologías de la seguridad informática de la que estamos tratando en la presente investigación.

Diferencias entre el Phishing y Spoofing	
Phishing 	❖ Su objetivo es obtener y robar la información privada del usuario. ❖ Utiliza la Ingeniería social para la equivocación humana basada en el engaño y así acceder a sus datos e información personal.
Spoofing 	❖ El objetivo es robar la identidad del usuario para actuar como otro individuo. ❖ Utiliza herramientas informáticas la cual se basan en la suplantación de identidad a través de plataformas web o canales de comunicación falsos. ❖ Causa daño sin la necesidad de llegar a robar la información. ❖ Se puede incluir o no se puede incluir en ataques de phishing.

Tabla 1. Cuadro comparativo de diferencias entre el Phishing y Spoofing.

Elaborado por: Nelson Torres

Los sitios web (Nodored., 2022) y (SoftwareLab., 2022) brindan información para identificar los tipos de phishing y spoofing que existen y que utilizan los ciberdelincuentes para robar información sensible a los usuarios.

Por eso a continuación mediante cuadros se especifica los tipos de phishing y spoofing más comunes:

Tipos de Phishing	
Fraude del CEO / Cuenta empresarial comprometida	❖ Este tipo de ataque se emplea cuando el atacante envía un correo electrónico a algún empleado, específicamente a los del área contable o finanza, en la que suplanta la identidad de la empresa u algún ejecutivo en la que trabaja la víctima, con el objetivo de que este le brinde información sensible o le transfiera dinero a una cuenta falsa.
Fraude del CEO / Cuenta empresarial comprometida	❖ El clone phishing no es nada más que la creación o clonación de mensajes existentes ya antes recibidos pero en una versión maliciosa.

Suplantación de dominio (Spoofing de Dominio)	❖ El spoofing de dominio se basa en la falsificación del dominio de correos electrónicos y sitios web de alguna empresa o persona en general para robar información. Ejemplo: Apple.com vs Apple.co
Gemelo malvado	❖ Este se efectúa mediante una red Wi-fi maliciosa haciéndose pasar por una legítima para que así el ciberdelincuente recopile y obtenga información personal o empresarial sin el consentimiento de la víctima.
Smishing (SMS phishing)	❖ Es una forma de atraer al usuario por medio de mensajes de textos asiéndose pasar por fuentes legítimas, que contienen enlaces que al darles clic los dirige a sitio web o les descarga archivos malicioso.
Vishing	❖ Vishing o phishing se emplea mediante una llamada de telefónica con el fin de intentar manipular a la víctima utilizando la ingeniería social con el fin de que este le brinde información personal o financiera.

Tabla 2. Tipos de Phishing.

Elaborado por: Nelson Torres

Tipos de Spoofing	
Spoofing con Emails	❖ Este tipo de spoofing es las más utilizada por los ciberdelincuentes ya que por medio del envío masivo de correos electrónicos falsos utilizan logotipos y cabeceras oficiales de bancos, compañías y agencias del orden público suplantando sus identidades para el robo de información.
Spoofing de DNS	❖ Conocida como falsificación de DNS (Sistema de Nombre de Dominio), los ciberdelincuentes usan este método para enviar datos DNS maliciosos a las terminales de las víctimas para impedirles que ingresen a sitios web que deseen visitar lo cual sean redirigidos a sitios web con contenido falso.
Spoofing de IP	❖ Como su nombre lo indica trata sobre la falsificación de IP, este método ayuda a que los ciberdelincuentes falsifique una IP existente valida y tome posesión de ella con el fin de enviar múltiples paquetes de IPs hacia redes a las que tendrá acceso.

Tabla 3. Tipos de Spoofing.

Elaborado por: Nelson Torres

El sitio web (Carballar, 2020) nos menciona las herramientas que suelen usar los cibercriminales para hacer este tipo de ciberataques, pueden ser de fabricación propia o también software que se pueden encontrar en internet, estas herramientas informáticas no son fáciles de utilizar ya que se debe de tener el conocimiento necesario y experiencia para poder manejarlas y sacarle un mayor provecho.

Las herramientas más usadas por estos ciberdelincuentes son:

- ✓ **Exploradores de puertos**

  Estos buscan los ordenadores más vulnerables de internet que contengan sus puertos abiertos, es decir, sus vías de comunicación por las que los programas de un ordenador brindan sus comunicaciones, con el fin de acceder a los mismos.

- ✓ **Gusano**

  Este es un programa cuya habilidad es transmitirse de ordenador en ordenador utilizando la información contenida que posee cada una de ellos, también permite averiguar cualquier tipo de información que contenga el ordenador infectado.

- ✓ **Caballo de Troya**

  Es un programa que mediante la ingeniería social o utilizando correos electrónicos ayudan a los ciberdelincuentes a tomar el control del ordenador de la víctima, ayudando así al atacante a ocultar sus acciones maliciosas dentro del ordenador.

- ✓ **Buscador de claves**

  Este tipo de programa es conocido como ataque de fuerza bruta porque se basa en la realización de intentos repetitivos, ya que posee de una lista de las combinaciones de claves más utilizadas.

Así como existen herramientas para realizar ataques como el phishing y spoofing también existen para contrarrestarlos y ayudar a la detección y prevención de este tipo de amenazas cibernéticas, especialmente para lo que con hoy en día se trabaja como lo es el negocio en línea. Según (Geekflare., 2021) es imposible prevenir el 100% de un fraude, pero utilizando múltiples capas como es la práctica de la seguridad utilizando las herramientas necesarias se puede reducir el riesgo de estas actividades ilegales.

Las capacidades que deben de tener las herramientas de detección y prevención para este tipo de ataques es el:

- ✓ Monitoreo de toda transacción que contenga alto riesgo o actividades fraudulentas.
- ✓ Capacidad para detectar riesgos digitales.
- ✓ Bloquear automáticamente toda actividad fraudulenta.
- ✓ Cumplir con los estándares y regular la privacidad.
- ✓ Dar aviso a los equipos sobre cualquier acto riesgoso.

Por ello se realizó un cuadro donde se menciona a 3 de las herramientas disponibles para proteger específicamente del fraude en línea a empresas.

<table>
<tr><th colspan="2">Herramientas para la prevención y detección de fraudes.</th></tr>
<tr><td>SEON(Fraud Fighters)
 

Es una herramienta de prevención y detección de fraude que permite a las empresas establecer las huellas digitales se sus clientes</td><td>Características
❖ Su motor de datos de tiempo real brida datos actualizados.
❖ Busca, identifica y bloquea cuentas falsas automáticamente.</td></tr>
</table>

con el fin de detectar transacciones fraudulentas y eliminar cuentas ilegitimas, ayudando así a reducir la perdida de dinero y tiempo.	❖ Filtra y crea una lista de cuentas de dispositivos ilegales y de riesgo.
ADJUST Es una herramienta que bloquea de manera proactiva los fraudes antes que ocurran, monitorea, detecta y previene el fraude publicitario en tiempo real.	**Características** ❖ Detecta y bloquea a los atacantes. ❖ Usa filtros automatizados para permitir solo instalaciones genuinas. ❖ Rechaza el spam y fraudes de enlaces de páginas falsas.
FRAUD.NET Es un conjunto de productos de seguridad especialmente para las industrias financieras protegiéndolas de fraudes como es el comercio electrónico y el marketing ilícito.	**Características** ❖ Utiliza inteligencia artificial para obtener información sobre actividades sospechosas la cual identifica y a la vez detiene de manera rápida. ❖ Detecta cualquier tipo de transacción fraudulenta verificando las cuentas de los clientes. ❖ Controla y detecta anomalías para identificar el fraude en tiempo real. ❖ Evita que las personas caigan en el marketing digital ilícito.

Tabla 4. Herramientas para la prevención y detección de fraudes.

Elaborado por: Nelson Torres

Así como existen estas herramientas anthiphishing también existen antivirus que dan la talla contrarrestando estos tipos de ataques cibernéticos ayudando con la seguridad de estos ataques como son los ransomware, malware, troyanos y gusanos informáticos.

Por ello el sitio web (Digitalguide, 2022) brinda información muy detalla sobre los antivirus más convincentes y los peligros que puede ocasionar no poseer un escudo contra los ataques cibernéticos, por tal razón se realizó una tabla haciendo mención de los tres mejores software:

<table>
<tr><th colspan="2">3 de los mejores Antivirus para la protección contra amenazas cibernéticas</th></tr>
<tr><td>BITDEFENDER
 

Es un software de seguridad que ofrece protección antimalware avanzada y muchas protecciones de seguridad online que ayudan al usuario a tener una mejor y segura navegación contra ataques de phishing.</td><td>Características
❖ Posee protección antiphishing ya que rastrea y bloquea sitios web no confiables.
❖ Posee protección multicapas que ayudan a mantener documentos, imágenes y videos a salvo de cualquier amenaza contra malware y ransomware conocido.
❖ Es rápido, actúa de manera anónima y segura mientras navega por la web cifrando todo el tráfico de internet protegiendo toda la información cuando utilice una conexión Wifi.
❖ Compatible con Windows, Mac iOS.</td></tr>
</table>

KASPERSKY ANTIVIRUS	Características
Es un antivirus que nos brinda una excelente protección contra todo tipo de programas maliciosos ayudándole así también en la protección de los registros de la computadora y todo el sistema.	❖ Brinda un análisis rápido y completo. ❖ Protección antiphishing que ayuda a protegerse de los intentos de robos de información. ❖ Posee un sistema de protección cuando se realizan compras online. ❖ Cifrado de sitios web. ❖ Analiza en tiempo real y de manera rápida las descargas realizadas. ❖ Su interfaz es intuitiva y sencilla de usar. ❖ Da un informe detallado sobre el rendimiento y el comportamiento de los programas.
NORTON 360  Un antivirus que ofrece una protección muy rigurosa contra virus y malware utilizando motores de análisis que escanean, rastrean y eliminan todo tipo de amenazas de malware.	**Características** ❖ Fácil de usar, sencilla, sólida y muy fiable. ❖ Posee un motor antimalware sofisticado y potente que analiza de manera completa el sistema. ❖ Navegación segura contrarrestando los ataques de phishing y spoofing. ❖ Brinda protección de la webcam. ❖ Compatible con Windows, Android, Mac, iOS.

Tabla 5. 3 de los mejores Antivirus para la protección contra amenazas cibernéticas.

Elaborado por: Nelson Torres

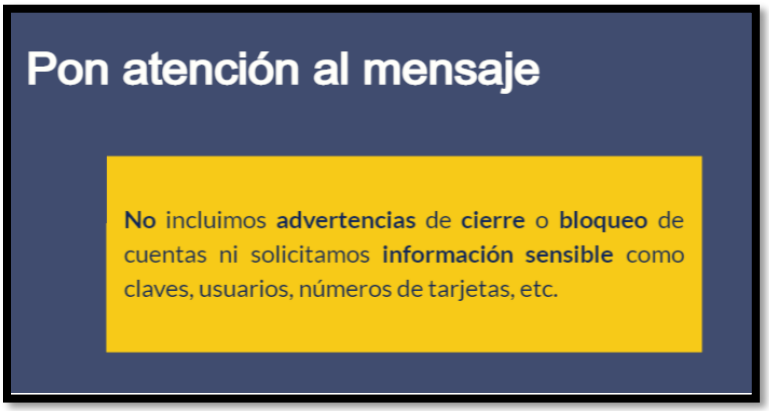
Según el sitio web (Cardozo, 2018) las recomendaciones para prevenir los ataques cibernéticos es tener siempre actualizados los sistemas operativos del computador, contar con un antivirus certificado, software con parches de seguridad y en caso de los correos maliciosos asegurándose de sus dominios, no acceder a los enlaces citados en él, no descargar documentos adjuntos o llamar a la empresa en general para verificar su credibilidad.

Uno de los ejemplos claros de cómo detectar o autentificar un correo electrónico o sitio web es la que nos brinda la página oficial del banco (Pichincha., 2020) y nos muestra en la primera ilustración la que nos hace mención de cómo identificar sus direcciones de correo electrónicos haciendo referencia a que deben terminar en: **@pichincha.com o comunicados@bancopichincha.com.ec**

"Ilustración 2. Verificación de autentificación de correo banco pichincha

Fuente: (Pichincha., 2020)

En la siguiente nos menciona que debemos de prestar sumamente atención y darle siempre la importancia necesaria al tipo de mensaje que emite la empresa, ya que esta no bloquea, no hace cierres, ni solicita información sensible de sus cuentas.



"Ilustración 3. Verificación de autentificación de correo banco pichincha

Fuente: (Pichincha., 2020)

Esta última ilustración hace énfasis a los requisitos que debe contener su enlace y su barra de navegación.

1. **Candado de seguridad.**

   Significa que la información que se visualiza en los sitios web está segura y contiene un certificado SSL legítimo que hace que tu información navegue por internet de manera encriptada y sin inconvenientes de que sea interceptada por los ciberdelincuentes.

2. **http con "S"**

   El https le permite al sitio web tener comunicación de forma segura, protegiendo la integridad y confidencialidad de los datos que posee la página.

3. **Dominio**

El dominio es único y exclusivo que se les da a los sitios web con el fin de identificar y visitar los mismos, en este ejemplo el dominio del sitio web del banco pichincha es **pichincha.com** que le hace referencia e identifica a la empresa misma.

"Ilustración 4. Verificación de autentificación de página banco pichincha

Fuente: (Pichincha., 2020)

Otro de los consejos que brinda el sitio web (Tapia, 2021) para evitar ser víctima de este tipo de ataques como es la suplantación de identidad o en especial el robo de datos bancarios es:

- Nunca compartir claves y usuarios de canales digitales u otros a terceros.
- No entre a sus bancas virtual estando conectado a una red Wifi de algún cibercafé o de algún parque porque pueden estar expuestos a contraer virus o troyanos que roban su información.
- Evite descargar aplicaciones de páginas no oficiales en especial las que no poseen el candado de seguridad.
- Instale antivirus con licencia.

- No responda a correos que le soliciten información personal.
- Asegúrese que los sitios web en los que ingresa sean los oficiales, fijándose que contenga el https y su ya antes mencionado candado de seguridad.
- No ingrese a los link de correos sospechosos.
- En caso de recibir correos o comunicación sospecha de aviso a su respectiva institución por medio de sus canales oficiales.

Los ciberataques cada vez son más comunes y mucho más rigurosos por lo que las empresas tendrán que tomar más en serio su seguridad y luchar contra estos ataques utilizando software antiphishing y spoofing con sus respectivas licencias y capacitando a sus empleados contra estas amenazas a las que se enfrentan día a día teniendo en cuenta que la parte más vulnerable para los atacantes son los usuarios (Consultores., 2021).

CONCLUSIÓN

Los ciberdelincuentes cada vez están implementando ataques y métodos phishing o spoofing más robustos la cual para las empresas es difíciles de contrarrestar y prevenir, pero a su vez el avance de las tecnologías de seguridad informática en general también ha ido en aumento presentando software que ayudan a la detección y prevención a estos tipos de ciberataques.

Mediante la investigación que se ha realizado se obtuvo los métodos y diferentes tipos de ataques que usan los ciberdelincuentes para cometer sus actos ilícitos y uno de los más comunes fue él envió masivo de correos electrónicos en la que utilizan la ingeniería social manipulando a los usuarios o empresas haciéndolos caer en sitios web maliciosos para así obtener información sensible.

Las personas que desconocen sobre estos tipos de ataques cibernéticos creen que son lo mismo porque ambos se basan en el delito informático, pero existen grandes diferencias que dicen lo contrario, en cuanto a las más específicas son que el phishing se basa en el robo de la información utilizando la ingeniería social y el spoofing es suplantar la identidad de painas web, empresas o usuarios con ayuda de herramientas informáticas, también puede causar daño sin la necesidad de robar información.

Una de las mayores prevenciones que tienen que tener los usuarios para navegar y cuidar cualquier información sensible es contar con software robustos y legítimos como son los antivirus o también llamados antiphishing o antispoofing lo cual mencionamos en la presente investigación

ya que tienen muy buena aceptación y están certificados a la hora de blindar la información que posee un ordenador.

Una de las herramientas que ayudo con la investigación fue Google Trends esta es un motor de búsqueda que pertenece a Google que contiene una gigantesca base de datos la cual ayudo a la obtención de información con respecto a los posicionamientos a nivel mundial de estos dos sistemas de seguridad de la información.

Esta herramienta como es Google Trends ayudo a saber que el phishing es la metodología más aplicada a nivel mundial en los últimos 12 meses arrojando una alza muy elevada, pero en la actualidad por el avance de los distintos tipos de software que brinda seguridad informática ha ayudado a que disminuyan estos ataques informáticos.

Estos dos ataques cibernéticos como son el phishing y el spoofing han ido avanzando con los pasos de los años, creando diferentes métodos para vulnerar y robar cualquier información posible, pero a su vez el mundo también lo ha ido haciendo, mejorando sus seguridades y blindando cada vez más su información sensible dándole así mayor importancia al mundo de la seguridad informática y asiendo que a estos ciberdelincuentes se les haga mucho más complicado realizar cualquier tipo de ataque para robar información.

BIBLIOGRAFÍA

Carballar, J. A. (19 de Octubre de 2020). *Herramientas de los ciberdelincuentes.* Obtenido de Herramientas de los ciberdelincuentes.: http://carballar.com/herramientas-de-los-ciberdelincuentes

Cardozo, R. (4 de Octubre de 2018). *'Phishing' y 'smishing', ¿qué son y cómo evitarlos?* Obtenido de 'Phishing' y 'smishing', ¿qué son y cómo evitarlos?: https://www.bbva.com/es/phishing-y-smishing-que-son-y-como-evitarlos/

Consultores., G. A. (18 de Febrero de 2021). *Qué es Spoofing y Phishing: Ciberseguridad en la Empresa.* . Obtenido de Qué es Spoofing y Phishing: Ciberseguridad en la Empresa. : https://www.grupoacms.com/blog/ciberseguridad-empresa-medidas-proteccion-contra-spoofing-phishing

Digitalguide, I. (13 de Marzo de 2022). *Antivirus: ¿cuál es el software más convincente?* Obtenido de Antivirus: ¿cuál es el software más convincente?: https://www.ionos.es/digitalguide/servidores/seguridad/cuales-son-los-mejores-antivirus/

ESET. (22 de Marzo de 2022). *SECURITY REPORT*. Obtenido de SECURITY REPORT: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Geekflare. (3 de abril de 2021). *Herramientas de detección y prevención de fraudes para negocios en línea.* Obtenido de Herramientas de detección y prevención de fraudes para negocios en línea.: https://geekflare.com/es/fraud-prevention-tools/

Lima., A. (9 de Marzo de 2022). *DIFERENCIA ENTRE SPOOFING Y PHISHING*. Obtenido de DIFERENCIA ENTRE SPOOFING Y PHISHING: https://es.acervolima.com/diferencia-entre-spoofing-y-phishing/

Nodored., A. c. (13 de Marzo de 2022). *10 tipos de ataques y estafas de phishing*. Obtenido de 10 tipos de ataques y estafas de phishing: https://aprende.nodored.com/10-tipos-de-ataques-y-estafas-de-phishing/

Pichincha., B. (8 de Diciembre de 2020). *¿Qué es el phishing? Cómo reconocerlo y evitarlo*. Obtenido de ¿Qué es el phishing? Cómo reconocerlo y evitarlo: https://www.pichincha.com/portal/blog/post/que-es-phishing

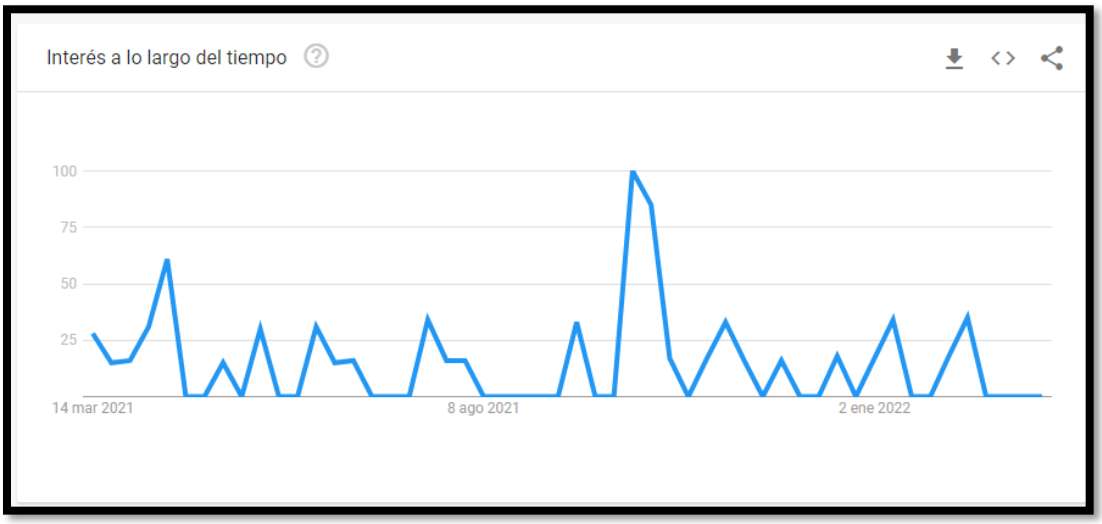
SoftwareLab. (13 de Marzo de 2022). *¿Qué es spoofing? Los 5 tipos: DNS, Email, IP, DDoS y ARP*. Obtenido de ¿Qué es spoofing? Los 5 tipos: DNS, Email, IP, DDoS y ARP.: https://softwarelab.org/es/que-es-spoofing/

Tapia, E. (13 de Octubre de 2021). *Los ataques de phishing alcanzaron su máximo histórico por la pandemia. ¿Cómo huir de ellos?* . Obtenido de Los ataques de phishing alcanzaron su máximo histórico por la pandemia. ¿Cómo huir de ellos? : https://asobanca.org.ec/innovacion-y-tecnologia/los-ataques-de-phishing-alcanzaron-su-maximo-historico-por-la-pandemia-como-huir-de-ellos/

Velazquez, N. (26 de Octubre de 2021). *¿Cuál Es La Diferencia Entre PHISHING Y SPOOFING?* Obtenido de ¿Cuál Es La Diferencia Entre PHISHING Y SPOOFING?: https://trustnet.com.mx/cual-es-la-diferencia-entre-phishing-y-spoofing/

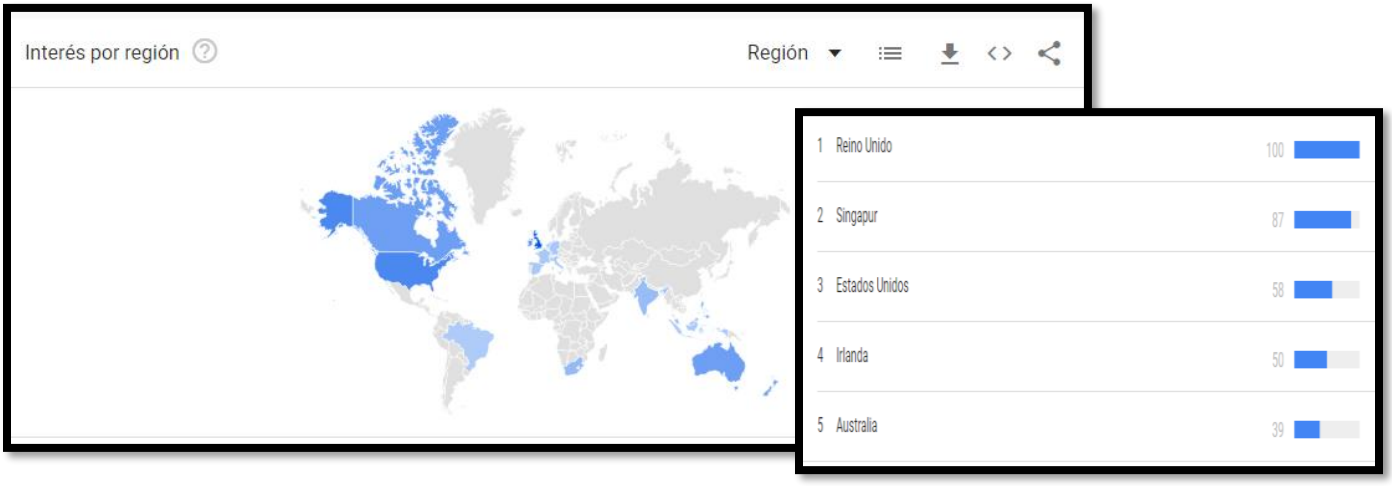
ANEXO

Recopilación de información a nivel mundial por medio de Google Trends para saber cómo se encuentra el alza de las amenazas de la seguridad informática, comparativas del uso del phishing, spoofing y reportes de estos ataques.



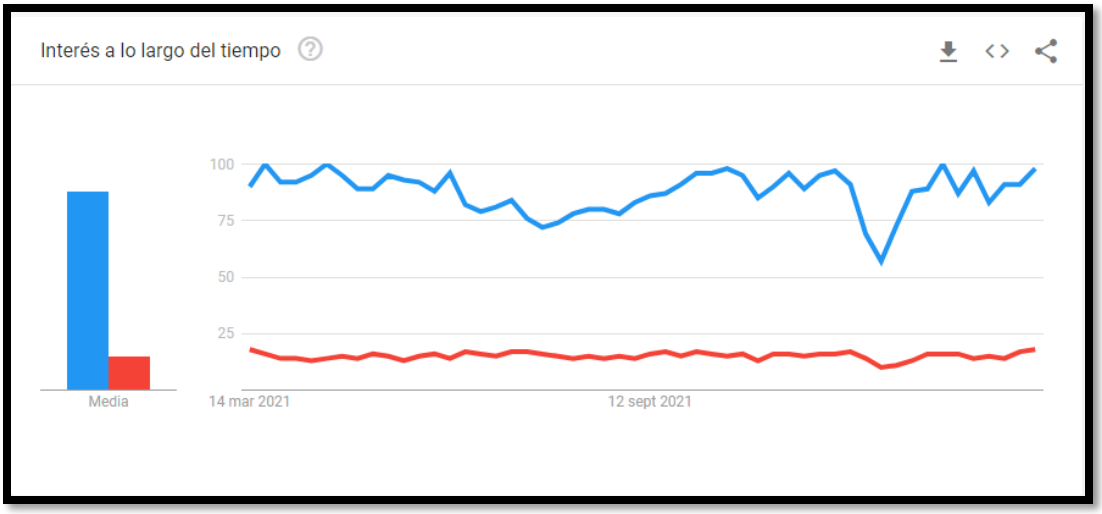
Fuente: Google Trends "últimos 12 meses"

Análisis: las amenazas a la seguridad informática en los últimos 12 meses se observa que en el mes de octubre del año 2021 tuvo un alza muy desagradable pero en la actualidad ya viene en decrecimiento debido a los diferentes software que cada vez son más eficientes para contrarrestar estos amenazas informáticas.



Fuente: Google Trends “últimos 12 meses”

Análisis: Mediante las estadísticas obtenidas con Google Trends observamos los datos que existen por países de reportes por phishing vemos que Reino Unido es el país con mayor influencia de reporte ataques fhishing.



Fuente: Google Trends “últimos 12 meses”

Análisis: Se realizó una comparación entre estos dos ataques de seguridad informática, y se observa que phishing es el ataque informático en los últimos meses más utilizado por los ciberdelincuentes.