# PROTOCOLO PARA LA PREVENCIÓN DE ATAQUES DE PHISHING

**Bernal Garay Miguel Abraham [1], Lizárraga Hernández Jesús Alberto [1], Pinedo Lizárraga Jorge Roberto [1], Flores Navarro Agustín [1], Flores Espinoza Daniel Ernesto [1]**

*[1]Facultad de Informática Mazatlán, Universidad Autónoma de Sinaloa, México*

## Resumen

En la presente investigación se abordan distintos tipos de técnicas de robo de datos (pishing), su incidencia a través de los años y lugares, así como la peligrosidad y el daño que puede hacer esta técnica a todo tipo de usuarios conectados al internet, desde usuarios comunes hasta empresas. A partir de esto, se elaboró una lista de posibles soluciones, y como resultado se presenta un protocolo, con el objetivo de ofrecer al público en general una serie de pasos para prevenir ataques de este tipo.

Palabras clave: Phishing, Robo, Identidad, Informática.

## 1 INTRODUCCIÓN

El Phishing es una técnica de ingeniería social utilizada por los delincuentes, conocidos como Phishers para obtener información confidencial como nombres de usuario, contraseñas e información de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

Se define como un tipo de malware o un término para que alguien envía un correo electrónico falsificado a las víctimas al azar para tratar de obtener información personal sobre ellos. Más específicamente en la informática, el phishing es una actividad criminal utilizando técnicas de ingeniería social para adquirir fraudulentamente información sensible como nombres de usuario y contraseñas, tratando de engañar a los usuarios de sitios web populares enviándolos por correo electrónico versiones falsas de la web para dar a sus credenciales.

El Phising se ha convertido en uno de los crímenes más organizados del siglo 21. El PH (phishing) se deriva de las sofisticadas técnicas que emplean, para distinguir sus actividades de la pesca más simplista. Con término más informático el Phishing es una actividad delictiva utilizando métodos de ingeniería social para recolectar información importante como nombres y contraseñas, a través de sitios web maliciosos engañando al usuario enviando correos electrónicos falsos [1].

La mayoría de los ataques de Phishing comienzan con un correo electrónico que afirman que se ha emitido por una empresa de confianza. Este correo electrónico anima al usuario a hacer clic en la dirección que se proporciona en su contenido. Esta dirección se dirige al usuario a una página web ilegal, que está diseñado similar a un sitio web válido, por ejemplo, el sitio de un banco o una institución financiera. Según el informe de Anti-Phishing Grupo de Trabajo (APWG), que es una organización sin fines de trabajo para proporcionar una educación anti-Phishing para mejorar la comprensión pública de la seguridad, más del 66% de los ataques de phishing se dirigen las instituciones financieras y los sistemas de pago en línea. Además, la mayoría de los ataques de Phishing realiza a través de servidores web hackeados. De acuerdo con este informe, en septiembre de 2012, los Estados Unidos de suplantación de identidad de Estados Unidos fue el anfitrión de más del 73% de los sitios web [2].

Lo que es una realidad en la actualidad es que el Phishing afecta a las personas a nivel mundial y se lleva a cabo a nivel internacional, por lo que es difícil rastrear y procesar a los criminales detrás de él. Una técnica común que los estafadores han utilizado se llama 'flujo rápido', donde un gran número de servidores proxy y direcciones URL se utiliza para mantener la verdadera ubicación del sitio de Phishing oculta. De esta manera, es más difícil a la lista negra el sitio y el servidor que se utiliza necesita más trabajo para encontrar. Los atacantes también han comenzado a producir redes, donde cada parte del ataque se lleva a cabo por una persona diferente. Por ejemplo, una persona que es bueno para producir un sitio forjado podría producir un conjunto de herramientas para otros estafadores que utilizan, sólo se tengan que seleccionar un sitio para copiar y dónde enviar la información. Estos usuarios del kit de herramientas serían entonces sólo necesitará seleccionar víctimas y enviar correos electrónicos.
Curiosamente, tantos como una tercera parte de estos kits de herramientas que realmente enviar los datos robados en otro lugar. De esta manera la persona que creó el conjunto de herramientas ha reclutado esencialmente Phishers sin experiencia para hacer todo el trabajo y tener la culpa, pero

ninguno de cosechar las recompensas. De esta manera, el verdadero estafador podría escapar sin ser detectado.

“El problema con el Phishing es que los atacantes buscan constantemente formas nuevas y creativas para engañar a los usuarios haciéndoles creer sus acciones implican un sitio web legítimo o correo electrónico. Los creadores de Phishing se han vuelto más hábiles en la creación de sitios web para parecer idénticos a los sitios verdaderos, incluso incluyendo logotipos y gráficos en los correos electrónicos de Phishing” [1].

Algunos tipos de Phishing se implantan en el navegador y suelen ser rastreadores web que también son conocidos como arañas y las referencias fantasmas. Los rastreadores tienen como objetivo, rastrear diferentes páginas web o correos no deseados y atacan a sólo en aquellos que carecen de ciertas características de seguridad, son más inofensivos que los fantasmas que son un spam persistente y no puede ser bloqueada fácilmente.

Existen otros tipos de Phishing como es el método PuP (programas con publicidad) que son software en diferentes tipos de programa como navegadores webs falsos, extensiones del navegador, barras de herramientas entre muchos otros [3].

El método Malware-Based Phishing es el más común que se basa en él envió de correos electrónicos en el cual se introduce una parte de malware como archivo descargable que manda al hipervínculo enviado por el mail o bien un archivo adjunto, este se aprovecha de la debilidad del dispositivo usado.

La falta de información sobre el Phishing en la sociedad es un problema bastante grave; cada día son más las víctimas, ya que al no estar informadas sobre los riesgos del Phishing y cómo prevenirlos las hace más vulnerables a este tipo de ataques.

Cada día las personas que practican el Phishing mejoran sus trampas, haciéndolas más creíbles incluso a usuarios que conocen de este problema. Pero también ha evolucionado la manera de cómo prevenirlos y distinguir cuales páginas son las confiables y cuales se trata de una trampa.

Hoy en día, los crímenes financieros se transforman de ataques directos sobre los ataques indirectos. En otras palabras, en lugar de robo de un banco, los delincuentes tratan de identificar a los clientes del banco con un truco específico. Los ataques a la seguridad informática se clasifican en tres tipos: los ataques físicos, ataques sintéticos, y los ataques semánticos [2]. La suplantación de identidad es un “mecanismo penal empleando tanto en la ingeniería social y el subterfugio de técnicas para robar los consumidores ' datos de identidad personal y credenciales de cuentas financieras”.

Actualmente existen una cantidad inmensa de malware, cada uno tiene sus propias características lo que lo separa de los demás haciéndolo único y peligroso, pero al final arrojando un resultado que los demás que es dañar al usuario. Como por ejemplo los virus que pueden eliminar ficheros, directorios y datos sin autorización del usuario, perdiendo información muy importante con pocas posibilidades o más bien escasas de recuperarla. Otro ejemplo es uno de los más comunes de encontrarse son los caballos de Troya o mejor conocidos como troyanos, este malware es uno de los más fáciles de caer ya que se hacen pasar por programas “seguros para el usuario” pero albergan un peligro dentro de ellos. Como su nombre lo dice caballo de trolla haciendo referencia al ataque de los aqueos como una estrategia para introducirse en la ciudad fortificada de Troya. Dicha amenaza al ser activada o abierta, permite el acceso no autorizado a datos en el computador o sistema informático infectado.

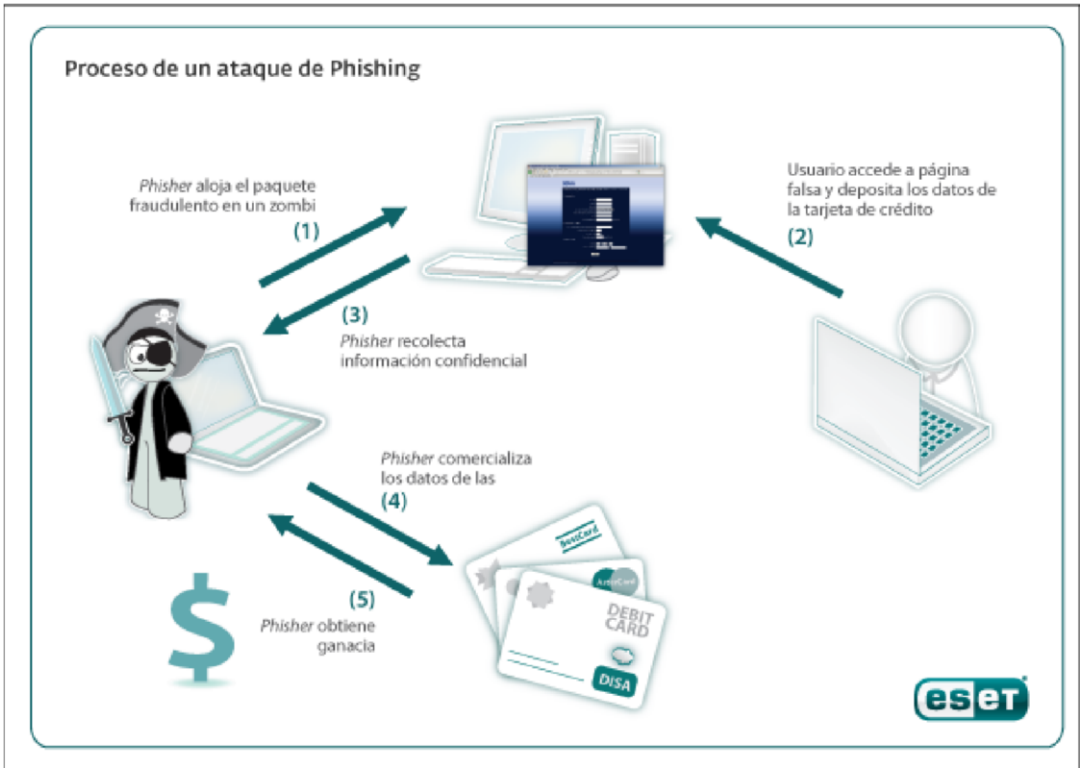


*Figura 1. Proceso de un Ataque de Phishing [4].*

Regularmente habrá usuarios que suelen ser un objetivo en específico y atacantes comunes, el objetivo de los Phisher suele ser muy común se basan en: dinero o información (que llevan a ganancias en dinero) además de las personas comunes están los peces gordos objetivos de alto valor como grandes corporaciones o gobiernos [3].

*Figura 2. Ejemplo de como mediante un correo de dudosa procedencia los Pishers pueden robar dinero a sus victimas [5].*

## 2 METODOLOGÍA

Las técnicas de investigación utilizadas durante el desarrollo de este trabajo han sido de tipo documental, debido a que se ha investigado y complementado por medio de la revisión bibliográfica de documentos como lo son: artículos y libros acerca del tema.

Para poder hacer esto primero se identificó como y a quienes afecta de manera mas frecuente, para después hacer recolección de diferentes recomendaciones y llegar a formar un protocolo, del cual primero nos enfocamos en el phishing que afecta a los usuarios que usan correo electrónico, en el cual se enfoca a que los usuarios identifiquen los correos que son clonados como si fuera una empresa real, identificando ciertos aspectos como el logo o nombres. Despues estar seguros que sea un remitente confiable y que no pida datos personales. Observar si el correo tiene links que te redirijan a paginas con conexion seguras y que que te señale que tu informacion es privada cuando se ingresa al sitio. De igual manera activar tu antivirus con protección web, que te ofrecen el bloqueo de anuncios, paginas maliciosas entre otras, usando herramientas del mismo antivirus que te ayuden a identificar paginas que principie la url con las siglas “ https://”. En diversos bancos se utiliza apps que envían notificaciones de identidad para asi estar al tanto de tus transacciones online. Después de verificar las

advertencias anteriores observar el texto ya que algunos correos tienen una traducción errónea, y podras prevenir este tipo de correo malicioso. Ya teniendo el concentrado el protocolo se realizaron pruebas de los pasos a seguir del respectivo protocolo para ver si se prevenia el Phishing y así poder descartar los pasos no óptimos, haciendo esto se pudo realizar un catálogo de las recomendaciones óptimas y que resultan idóneos para prevenir el Phishing.

## 3 RESULTADOS

Como resultado del presente trabajo (Figura X) se muestra a continuación el protocolo a seguir para prevenir el Phishing.

***1. APRENDE A IDENTIFICAR CLARAMENTE LOS CORREOS ELECTRÓNICOS SOSPECHOSOS DE SER PHISHING***

- Existen algunos aspectos que inequívocamente, identifican este tipo de ataques a través de correo electrónico:
- Utilizan nombres y adoptan la imagen de empresas reales
- Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa
- Incluyen webs que visualmente son iguales a las de empresas reales
- Como gancho utilizan regalos o la perdida de la propia cuenta existente

***2. VERIFICA LA FUENTE DE INFORMACIÓN DE TUS CORREOS ENTRANTES***

- Tu banco nunca te pedirá que le envíes tus claves o datos personales por correo. Nunca respondas a este tipo de preguntas y si tienes una mínima duda, llama directamente a tu banco para aclararlo.

***3. NUNCA ENTRES EN LA WEB DE TU BANCO PULSANDO EN LINKS INCLUIDOS EN CORREOS ELECTRÓNICOS***

- No hagas clic en los hipervínculos o enlaces que te adjunten en el correo, ya que de forma oculta te podrían dirigir a una web fraudulenta.
- Teclea directamente la dirección web en tu navegador o utiliza marcadores/favoritos si quieres ir más rápido.

***4. REFUERZA LA SEGURIDAD DE TU ORDENADOR***

- El sentido común y la prudencia es tan indispensable como mantener tu equipo protegido con un buen antivirus que bloquee este tipo de ataques. Además, siempre debes tener actualizado tu sistema operativo y navegadores web.

***5. INTRODUCE TUS DATOS CONFIDENCIALES ÚNICAMENTE EN WEBS SEGURAS***

- Las webs seguras han de empezar por 'https://' y debe aparecer en tu navegador el icono de un pequeño candado cerrado.

***6. REVISA PERIÓDICAMENTE TUS CUENTAS***

- Nunca está de más revisar tus cuentas bancarias de forma periódica, para estar al tanto de cualquier irregularidad en tus transacciones online.

***7. EL PHISHING SABE IDIOMAS***

- El phishing no conoce fronteras y pueden llegarte ataques en cualquier idioma. Por norma general están mal escritos o traducidos, así que este puede ser otro indicador de que algo no va bien.
- Si nunca entras a la web en inglés de tu banco, ¿Por qué ahora debe llegarte un comunicado suyo en este idioma?

***8. ANTE LA MÍNIMA DUDA SE PRUDENTE Y NO TE ARRIESGUES***

- La mejor forma de acertar siempre es rechazar de forma sistemática cualquier correo electrónico o comunicado que incida en que facilites datos confidenciales.
- Elimina este tipo de correos y llama a tu entidad bancaria para aclarar cualquier duda.

***9. INFÓRMATE PERIÓDICAMENTE SOBRE LA EVOLUCIÓN DEL MALWARE***

Figura X: Protocolo de prevención….

## 4 CONCLUSIONES

En esta investigación faltó aclarar ciertos ataques de Phishing ya que existen muchos ataques y cada uno se trata de diferentes maneras, al igual que su comportamiento con el ordenador es diferente y característico de cada uno, en conclusión lo que corresponde a prevención de Phishing mediante el Anti-Phishing se nota una muy eficaz prevención con el bloqueo de bloqueo de paginas Web no seguras, con los anuncios de spam que también los bloqueo de manera instantánea.

Como se puede observar la investigación esta enfocada en algunos tipos de Phishing, falto analizar mas tipos de Phishing, en un futuro se planea examinar mas tipos de Phishing así como investigar mas herramientas que sean eficaces para la prevención.

Con el protocolo creado y planeado se espera reducir considerablemente los ataques de Phishing.


[1] S. K. Ike Vayansky, "Phishing - retos y soluciones," *Fraude y Seguridad informatica,* p. 6, 2018.

[2] A. Y. V. Mahmood Moghimi, "Nuevo método de detección de phishing basado en reglas," *Sistemas Expertos con Aplicaciones,* p. 12, 2016.

[3] M. F. Christopher Hadnagy, Phishing dark waters, Estados Unidos: Wiley, 2015.

[4] J. Mieres, "Welivesecurity," Welivesecurity, 25 Agosto 2010. [Online]. Available: https://www.welivesecurity.com/la-es/2010/08/25/como-opera-phisher/. [Accessed 25 Noviembre 2019].

[5] T. Castillo, "Genbeta," Genbeta, 1 Octubre 2019. [Online]. Available: https://www.genbeta.com/seguridad/como-evitar-ser-victima-phishing-correos-otrosingeniosos-ataques-que-buscan-robarte. [Accessed 25 Noviembre 2019].

[6] E. S. A. V. Brynne Harrison, "Cómo la atención y elaboración protección contra el phishing," *Esmeralda Insight,* p. 17, 2015.

[7] L. james, Suplantacion de identidad expuesto, Estados Unidos: Syngress Publishing, Inc, 2004.

[8] F. A. S. C. Mohamed Alsharnouby, "¿Por qué phishing sigue funcionando: las estrategias de usuario para la lucha contra los ataques de," *Human-Computer Estudios,* p. 14, 2015.

[9] R. M. Reyes, Delitos informáticos estudio concreto sobre Fraudes y Phishing., Jaén, España, 2013.

[10] AndalucíaCERT, "Informe de divulgación phishing," Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A, 2017.

[11] Á. G. Vieites, Seguridad Infomatica Bàsico, Madrid: STARBOOK EDITORIAL, 2010.

[12] NOTIMEX, “México, entre los países con más ciberataques en AL,” *Excelsior,* p. 2, 05 Mayo 2019.