Análisis del Phishing y la Ley de delitos informáticos en Colombia

Jaiver Julián Medina Martínez[1], Camilo Hernán Cárdenas Osorio[2], Mauricio Mejía Lobo[3]

RESUMEN
Las tecnologías de la información siguen y seguirán evolucionando, esta situación conlleva drásticos cambios en la sociedad, y en el uso que se les den. Dentro de los usos, como toda herramienta puede tener sus bondades pero también sus efectos o usos negativos los cuales son explotados por una minorías, pero con unos impactos drásticos y altos, como respuesta a ello los gobiernos desde sus poderes legislativo, ejecutivo y judicial, interponen leyes y grupos para el seguimiento y judicialización de quienes las usan con fines delictivos, y de allí nacen varias inquietudes, por ejemplo la seguridad, el conocimiento, por lo anterior se emprende una revisión bibliográfica centrada en el phishing con el fin de determinar el estado frente a este reconocido y en aumento delito.

Palabras Clave: Phishing, Delitos Informáticos, Suplantación, Robo de identidad, Ciberseguridad.

INTRODUCCIÓN

El concepto de phishing se puede definir como un método usado para sustraer información y obtener beneficios económicos a partir de ello.
Según el gremio representativo del sector financiero colombiano Asobancaria (2019), dice que el Phishing: Es una modalidad de fraude, que consiste en el envío masivo de mensajes electrónicos en los que aparece una dirección web falsa / clonada de una entidad bancaria, con el fin de capturar información sensible de los usuarios como sus claves de acceso, etc.

La palabra "phishing" proviene originalmente de la analogía de que los primeros criminales de Internet usaban señuelos de correo electrónico para "phish", pesca de contraseñas y datos financieros de un mar de internautas. El uso del "ph" en la terminología se pierde con el tiempo, pero lo más probable es que esté vinculado a convenciones populares de nombres de hackers como "phreaks" que se remonta a los hackers tempranos que estaban involucrados en "phreaking"-el hacking de los sistemas de telefonía. (Ollmann, 2007).

Phishing es un delito informático que proviene desde hace más de 20 años, claro que en esa época no tenía tal nombre, ya que para el año 1990 ya existían personas maliciosas y delincuentes que enviaban correos electrónicos solicitando información personal, según el artículo de Matute indica que el termino se conoce 6 años más tarde del primer ataque dirigido a la empresa estadunidense America On Line.

La primera mención del término phishing fue en enero de 1996. Se dio en el grupo de noticias de hackers alt.2600, aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker 2600 Magazine. El término phishing fue asignado para quienes pretendían apoderarse de cuentas de miembros de AOL.

[1] jaiver.medinama@amigo.edu.co
[2] camilo.cardenasos@amigo.edu.co
[3] mauricio.mejialo@amigo.edu.co

La historia señala que los primeros casos de phishing se detectaron a mediados del año 1990 por la empresa estadounidense America On Line. El estafador enviaba un correo electrónico solicitando diversa información de facturación, entre las que se encontraban los números de las tarjetas de crédito empleadas para pagar por el servicio. (Ayala, 2011).

MÉTODO

Revisión teórica mediante una búsqueda exhaustiva del material en la cual se lograron identificar 15 documentos de los cuales se hizo la abstracción sobre los resultados más significativos del cual se presenta el resultado.

Tipos de Phishing

Spear Phishing. Está dirigido a personas específicas o a grupos reducidos. De esta manera las campañas son mucho más personalizadas y dirigidas, aumentando el número de víctimas.
Según Kaspersky (2019), plantea en su página web oficial el funcionamiento del Spear Phishing de la siguiente manera:
Llega un correo electrónico, aparentemente de una fuente confiable, que dirige al destinatario incauto a un sitio web falso con gran cantidad de malware. Estos correos utilizan técnicas inteligentes para captar la atención de las posibles víctimas.

Whale Phishing / Whaling. Esta clase de phishing tiene como objetivo funcionarios gerenciales de las empresas. Al igual que en el spear phishing, se hace un estudio previo de la posible víctima personalizando el mensaje para que sea más efectivo.
Según la empresa estadounidense desarrolladora de antivirus Trend Micro (2018), plantea en su página web oficial lo siguiente (Phishing ballena):
El phishing de ballena es un término usado para describir un ataque de phishing dirigido específicamente a personas adineradas, poderosas o prominentes. Debido a su estado, si un usuario de este tipo se convierte en víctima de un ataque de phishing, puede ser considerado un "gran phish" o, alternativamente, una "ballena".

Social Fish. Es un modelo dentro de la terminología phishing que hace énfasis en herramientas web para la clonación de alguna red social, ya sea Facebook, Twitter, LinkedIn, etc. Ya que esta cuenta con algunas “plantillas” y a la vez bajo segundo nivel de desarrollo abstrae y copia la información personal de los usuarios en una base de datos.

Shellfish. Provee una interfaz de usuario para acceder a los servicios del sistema operativo del equipo infectado con el malware.

El pharming, una combinación de los términos "phishing" y "farming". El pharming aprovecha los principios con los que funciona la navegación por Internet, es decir, la necesidad de convertir una secuencia de letras para formar una dirección de Internet, como www.google.com, en una dirección IP por parte de un servidor DNS para establecer la conexión. El exploit ataca este proceso de dos maneras. En primer lugar, un hacker puede instalar un virus o un troyano en la computadora de un usuario que cambia el archivo de hosts de la computadora para dirigir el tráfico fuera de su objetivo previsto, hacia un sitio web falso. En segundo lugar, el hacker puede infectar un servidor para que los usuarios visiten el sitio falso sin darse cuenta.

Cifras Internacionales

Según la fuente BITTIN SAS, para el año 2018 el cibercrimen dejó ganancias por encima de los 3 trillones de dólares, lo que representó para América Latina $6.179 millones. Para el año 2020, de acuerdo con las estimaciones y proyecciones y según el efecto de la cuarentena mundial se ha presentado un aumento considerable tasado en más del 30% de las ocurrencias con un especial énfasis en el phishing.

El mundo digital se ha integrado en toda la sociedad de una forma vertiginosa, en nuestro diario vivir son más las personas que se apoyan en Internet para utilizar sus servicios y realizar sus actividades, enviar un correo electrónico, participar en un foro de discusión, tener una sesión de chat, comunicación de voz sobre IP, descargar música o el libro favorito, hacer publicidad, etc. Son algunas de las cosas más comunes. Sin embargo, el mundo de los negocios empresariales es aún más complejo y la gama de servicios nos presenta mayores alternativas. (Clavijo, 2006)

Cifras en Colombia

Según la mencionada fuente para Colombia el negocio de los ciberdelitos dejó 31.498 denuncias. Los tipos de industrias más afectadas fueron el financiero con un 40%, el de telecomunicaciones con un 26%, Gubernamental con un 16%, productos con un 10% y el energético con una tasa del 9%.

A su vez según los tipos de delitos cibernéticos el Phishing se encuentra en el primer lugar en el país, seguido de la sextorsión, el Vishing, SIM Swapping, el formjacking y el secuestro de información. Según el centro cibernético policial durante el 2017 se evidencio un aumento significativo en conductas delictivas que vulneran la integridad de las personas. Siendo el "Artículo 269I. Hurto por medios informáticos y semejantes" la tipología criminal de mayor frecuencia, equivalente al 60%, seguido del "Artículo 269F. Violación de datos personales" con 16% y "Artículo 269A. Acceso abusivo a un sistema informático". (Centro Cibernético Policial, 2017)

Legislación Internacional

Naciones Unidas Asamblea General
A/74/130
Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos Informe del Secretario General.

El informe se ha preparado en cumplimiento de la resolución 73/187 de la Asamblea General, titulada "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos". En esa resolución, la Asamblea General solicitó al Secretario General que recabara las opiniones de los Estados Miembros sobre los problemas a que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y que presentara un informe basado en esas opiniones para examinarlo en su septuagésimo cuarto período de sesiones. Contiene información de los Estados Miembros presentadas en cumplimiento de la resolución.

Convención de Budapest El 23 de noviembre del año 2001 en Budapest Hungría, tuvo lugar un consejo de ministros de Europa, llamado convenio sobre la ciberdelincuencia, en donde se establecen cuáles son en su momento las conductas delictivas por los ciberdelincuentes y las leyes para afrontarlas. (Consejo de Europa, 2001).

Legislación en Colombia

Ley 1273 de 2009, De la protección de la información y de los datos". Dentro de los artículos 269A y siguientes, según la ley 1273 (2009) estos son:

> **Artículo 269G: Suplantación de sitios web para capturar datos personales.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Cabe aclarar que, aunque literalmente los términos: "Phishing" e "Ingeniería social", no están contemplados en los artículos del código penal del 2009. Sus acciones delictivas, son las que irrumpen frente a la ley y ocasionen sanciones según su estado de acción.

Ley 1298 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

CONCLUSIONES

La seguridad de la información es de gran importancia y debe ser un tema estratégico y crítico, por tal motivo debe ser prioridad estar actualizados de las nuevas formas de seguridad de la información organizacional y de la evolución de los malware para así poder tomar las medidas más adecuadas para contrarrestar estos ataques.

Se debe estar actualizado en delitos informático ya que nos ayudará a tener más cuidado con las páginas a las que se ingresa, ni brindar nuestra información personal para evitar que nos ataquen con el cibercrimen.

AGRADECIMIENTOS

Universidad Católica Luis Amigó

REFERENCIAS

AO Kaspersky Lab. (2019). Ingeniería social: definición. Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

AO Kaspersky Lab. (2019) ¿Qué es el spear phishing? Recuperado de https://latam.kaspersky.com/resource-center/definitions/spear-phishing

Asobancaria. (2019). Saber más ser más - Programa de educación financiera de los bancos en Colombia. Phishing. Recuperado de http://www.asobancaria.com/sabermassermas/phishing/

Bittin, Investigación digital, Informática forense, Recuperación y confidencialidad de la información. www.bittin.co

Centro Cibernético Policial. (Diciembre de 2017). *Cai Virtual Policía.* Recuperado el 30 de Julio de 2018, de Balance Cibercrimen en Colombia 2017: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Clavijo, C. A. (enero- Julio de 2006). Políticas de seguridad informática. *Entremados*, *2*(1), 86-92. Recuperado el 13 de Julio de 2018, de http://www.redalyc.org/articulo.oa?id=265420388008

Congreso de la República de Colombia (2009). Ley N° 1273 de enero del 2009. Bogotá D.C.: Congreso de la República de Colombia.

Congreso de la República de Colombia. (2018). Ley 1928 de 2018, Rama Legislativa (2019).

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. Budapest: Consejo de Europa.

Matute, J. C. (12 de 2013). EL DELITO INFORMÁTICO DE PHISHING. Quevedo, Ecuador. Recuperado el 16 de 07 de 2018, de http://dspace.uniandes.edu.ec/handle/123456789/2819

Oxman, N. (2013, noviembre, 13). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Scielo. Recuperado de https://scielo.conicyt.cl/scielo.php?pid=S0718-68512013000200007&script=sci_arttext&tlng=en

Ollmann, G. (2017). *The Phishing Guide.* Estados Unidos de América. Recuperado el 16 de 07 de 2018, de http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf

Pérez, Y. (2017). Un caso de phishing más en Colombia. Universidad Cooperativa de Colombia. Recuperado de https://www.ucc.edu.co/noticias/conocimiento/ingenieria-arquitectura-y-urbanistica/un-caso-de-phishing-mas-en-colombia