Amenazas a la información personal financiera

José Javier Diaz Quesada[1], Miguel Hernández Bejarano[1],*

[1] Fundación Universitaria Los Libertadores; jdiazq@libertadores.edu.co
[2] Fundación Universitaria Los Libertadores; mhernandezb@libertadores.edu.co
* Correspondence: jdiazq@libertadores.edu.co

Received: 30/09/2020; Accepted: 2/11/2020; Published: 31/12/2020

Abstract: En el presente artículo se abordan los diferentes tipos de amenazas y delitos que se llevan a cabo en internet para robar información personal financiera, se explica en que consiste el Ciberdelito, se realiza una explicación detallada de lo que es el Phishing, Whaling, Vishing y Smishing; técnicas que han tenido mucho éxito al momento de substraer datos personales y credenciales bancarias. Adicionalmente se muestran datos estadísticos en lo que respecta a las aplicaciones más usadas al momento de atacar en la red y el perfil de los Ciberdelincuentes. Finalmente se presenta una serie de consejos y buenas prácticas para que el lector aprenda como prevenir y saber qué hacer en caso de ser víctima de estos ataques.

Keywords: Ciberdelito, Página Web, Información Personal, Phishing

1. Introducción

Los cibercriminales con el paso del tiempo mejoran sus métodos para robar cuentas y comprometer identidades de los clientes o empleados de los diferentes bancos que existen, pero, aunque la tecnología ha ido evolucionando también ha ido cogiendo fuerza un método muy común. "El Phishing" el cual consiste en enviar emails o crear páginas web con información falsa dirigida a los usuarios en internet. Todo esto con el fin de captar información personal.

Debido al creciente aumento de la tecnología, los bancos facilitan al cliente procesos bancarios con nuevos canales emergentes como lo son canales Móviles y Banca en Línea; estos a su vez abren nuevas puertas a los cibercriminales. Por estas razones actualmente crece el interés en los diversos ataques cibernéticos ya que estos abarcan ataques a la confidencialidad de los datos personales, a la entidad bancaria y a la confianza que el titular de la cuenta deposita en la seguridad del sistema para la realización de todo tipo de transacciones comerciales y personales [1].

La finalidad del presente artículo es advertir y dar información de buenas prácticas para ayudar a los usuarios a identificar claramente las amenazas a las que están expuestas las credenciales bancarias y la información Personal. De esta manera Minimizar las brechas existentes entre la información Bancaria y los cibercriminales.

La ciberdelincuencia se define con carácter estricto como cualquier tipo de actividad ilícita en la que se maneje Internet, una red privada, pública o un medio informático doméstico [2]

Así como en la sociedad se pueden encontrar delincuentes, del mismo modo en el mundo informático encontramos a los Ciberdelincuentes, que en términos globales son personas que realizan prestezas delictivas en internet como sustraer información, acceder a redes privadas, timos, y todo lo que tiene que ver con las infracciones y la ilegalidad.

De acuerdo a la Firma, las acciones de los Ciberdelincuentes se pueden clasificar en 3:

- Asaltos a sistemas informáticos y piratería.
- Fraude o falsificación.
- Publicación de contenidos prohibidos.

Por otro lado, la división española Computer Forensic (Empresa dedicada a la recuperación de datos, borrado seguro y peritaje informático). Ha identificado tres características principales que enmarcan estos tipos de delitos [3].

Tienden a ser delitos que son muy difíciles de demostrar ya que la mayoría de veces resulta complicada encontrar las pruebas.

Son acciones que pueden realizarse de una manera rápida y sencilla. Algunas veces estos tipos de delitos se pueden cometer en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

Los delitos informáticos en general tienden a evolucionar, siendo cada vez más efectivos; esto hace que sea difícil su identificación y persecución.

Es de vital importancia entender los tipos de amenazas a las que está expuesta la información en la red para así tomar medidas y buenas prácticas frente a este tema. Por esta razón se muestra a continuación los tipos de malware y los métodos más comunes para robar información de los usuarios informáticos.

Por un lado Kaspersky muestra una lista de los Malware más comunes para substraer o dañar información los cuales son: Virus clásicos, Gusanos de red, troyanos, Spyware, Adware, Riskware y Rootkits [4].

Estos tipos de Malware por si solos no representan un riesgo tan alto para el usuario, el riesgo comienza cuando se ingresa a internet y se ejecutan estos programas sin darse cuenta; de aquí parte la importancia de conocer el segundo componente que hace posible que el usuario ejecute estos programas sin notarlo. La ingeniería social [5].

1.1 **Ingenieria Social**

Es una técnica aplicada por los atacantes para mentir a los usuarios informáticos, y así forzarlos indirectamente a realizar una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social [6].

Por otra parte, RSA (Empresa dedicada a criptografía y software de seguridad). Define que existen 4 tipos de amenaza a la información financiera: Phishing, Whaling, Vishing y Smishing. Ahora observe en que consiste cada una [7].

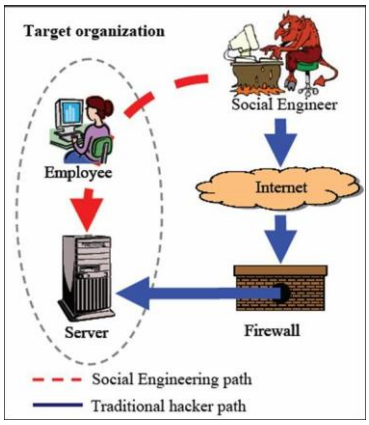
Phishing. (*La que más éxito tiene a la hora de robar información bancaria*) Consiste en una serie de programas espías que se generalizan a través de correo. Los emails de phishing están diseñados para verse igual a la correspondencia legal enviada por organizaciones bancarias, o algunas marcas conocidas [8] [9]. Dichos emails contienen un enlace que re direcciona al usuario a una página falsa en la cual se solicita el ingreso de datos confidenciales, como por ejemplo el número de la tarjeta de crédito [10].

Whaling. La técnica es la misma utilizada en el Phishing con la variante que este consiste en enviar correos de orden jurídico o muy creíble a usuarios acaudalados e influyentes como gerentes de alguna empresa.

Lo que caracteriza este tipo de delitos es el uso inmenso de la ingeniería social combinado con el uso de software malicioso [11] [12].

Vishing. También llamado VoIP phishing. Los criminales configuran una llamada de marcado automatizada en una región o código de área en particular [13]**.** Esta técnica usa códigos de área forjados y nombres de la institución financiera, organización o negocio [14]**.**

Smishing. Utiliza textos SMS a un teléfono móvil para iniciar la estafa. Si una víctima se registra en uno de los sitios web falsos con un teléfono inteligente, también podría terminar descargando código malicioso que podría dar a los criminales acceso a cualquier cosa en el teléfono [15]**.**



Grafica 1. Ingeniería social vs Hacking tradicional. [16]

En la gráfica 1 se observa un contraste entre los dos métodos que suelen usar los Ciberdelincuentes, se observa que haciendo ingeniería social (parte fácil) se utiliza al usuario para ganar acceso a la información objetivo y haciendo hacking tradicional (parte compleja) se requiere tener de un profundo conocimiento técnico para ganar acceso a través de los distintos dispositivos que protegen la información.

Es importante que el usuario sepa que en Colombia existe una ley que protege al ciudadano frente a este tipo de delitos:

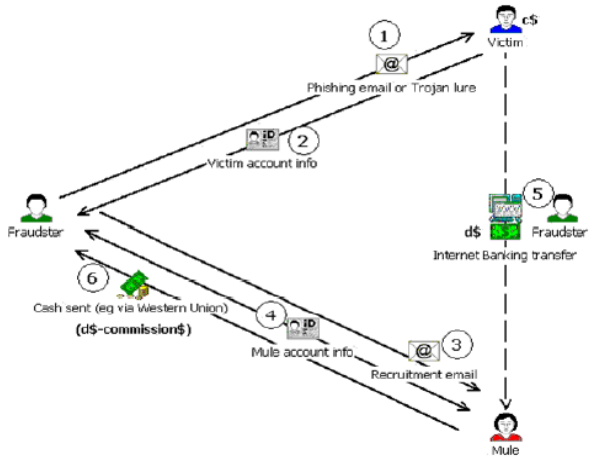
La protección de la información y de los datos es abarcada por la Ley 1273 de 2009 contemplada en el código penal [17]**.**

En esta Ley se encuentran contemplados una serie de capítulos que informan acerca de las Penas o Multas que se impondrán a las personas que cometan delitos informáticos.

2. Anatomía y estadística de los fraudes financieros

2.1 Anatomía

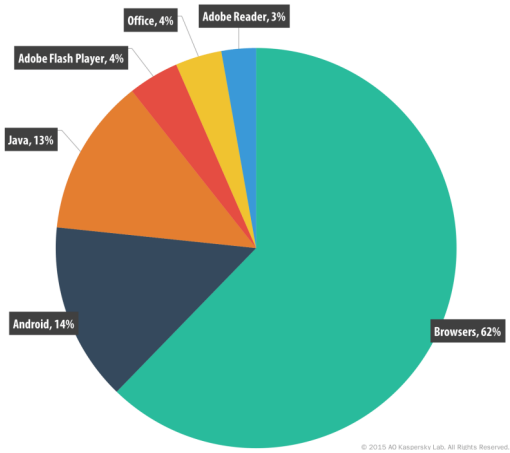
A continuación, se muestra en la gráfica 2 la estructura y el funcionamiento del delito financiero, en el cual el delincuente toma los datos de 2 víctimas; una para robar el dinero y otra (mula) para depositar el dinero robado y posteriormente transferirlo a la cuenta del delincuente [18].



Grafica2. Anatomía de un fraude bancario en internet [19].

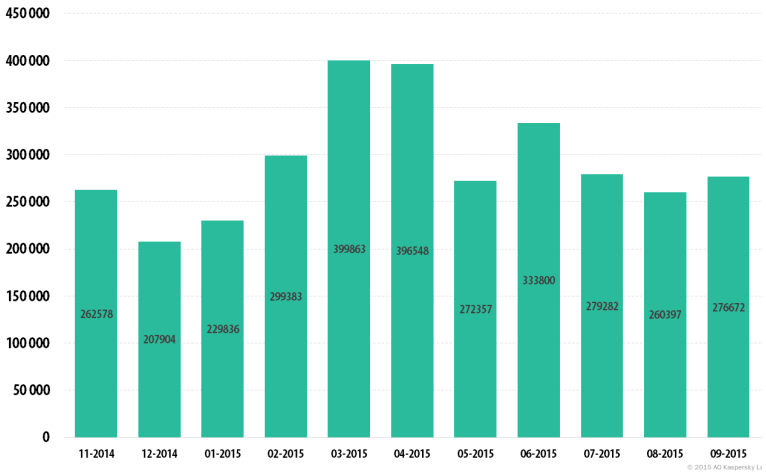
2.2 Estadística de ataques a cuentas bancarias

Las estadísticas que corresponden a continuación se basan en las detecciones manifiestas por el modulo antivirus de Kaspersky Lab. La firma pidió permiso a los usuarios de sus productos para proporcionar estos datos. Las estadísticas anuales para el 2015 se basan en los datos recibidos entre noviembre de 2014 y octubre de 2015 [4].



Grafica 3. Distribución de los exploits utilizados en los ataques cibernéticos, según el tipo de aplicación atacado de 2015 [4].

De acuerdo a la gráfica 3 definiendo para el lector, un exploit es un programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma tal que un atacante podría usarla en su beneficio. [20] Así se observa que la vulnerabilidad más aprovechada por los Ciberdelincuentes ha sido la de los browsers con un 62% [21].



Grafica 4. El número de usuarios atacados por malware financiero, noviembre 2014 a octubre 2015 [4].

2.3 Buenas prácticas para evitar ser víctima de ciberdelito.

- Cambiar regularmente las contraseñas
- Usar Mayúsculas, Minúsculas, Caracteres Especiales, Números y una longitud de contraseña mayor a 8 caracteres [22].
- En el ambiente laboral no dejar las contraseñas corporativas sobre el escritorio o en lugares de fácil acceso ya que alguien podría tomarlas.
- Evitar crear contraseñas de fácil uso como: 12345 o nombres personales ya que con ciertos tipos de software como "John the Ripper" es fácil descifrarlos usando diccionario de listas y fuerza bruta [23].
- Desconfiar de software gratis o de prueba en la Red ya que estos pueden tener ejecutables que espíen los equipos remotamente.
- Desconfiar de correos provenientes de empresas o aplicaciones dudosas realizando búsquedas en internet [24].
- No brindar información personal a fuentes desconocidas [25].

2.4 En caso de sospechar ser víctima de un ciberdelito.

- Desconectarse rápidamente de la Red [26].
- Sin importar que el Usuario se haya conectado a Internet por medio de un teléfono, por cable o Wi-Fi, se recomienda que este deshabilite su conexión lo más pronto posible. Así, resulta posible evitar que la información llegue al cibercriminal [27].
- Si el usuario se encuentra en el trabajo, es recomendable contactar el Departamento de informática y comunicar el hecho [28].
- Además de que los datos personales puedan estar en peligro, es probable se hayan robado información de vital importancia para la entidad [29].
- De un modo u otro, el departamento IT debe ser el primero en conocer la existencia del problema y deberá estar en condiciones de poder ayudarlo con alguno de los pasos concernientes al proceso de recuperación [30].
- Analizar la computadora Afectada con un programa antivirus actualizado [30].
- Realizar Back Ups de la información importante de modo que, en caso de perder esta información, sea posible restaurarla y continuar con el trabajo interrumpido [31].
- Buscar indicios de robo de identidad [32].

3. Conclusión

Es cierto que la tecnología crece en el tiempo exponencialmente; las personas se documentan, los cibercriminales agudizan sus métodos y expanden sus estrategias para cometer Ciberdelito. En las próximas décadas comenzaremos a experimentar más de la red, materializada con la tendencia del internet de las cosas; esto propone un riesgo ya que para una persona que pertenece al campo de la cibercriminalidad se expanden sus objetivos de ataque y se facilitan los puntos débiles en la seguridad de nuestros dispositivos, por esta razón será necesario invertir tiempo y dinero en investigar más el campo de la seguridad informática, para que cuando esta tendencia se radique por completo en la sociedad, no tome por sorpresa a los cibernautas los ataques hechos en este campo. [33].

References

[1] A. R. a. L. Parthiban2, «The effect of cybercrime on a Bank's finances,» *EP (excellent publishers),* p. 4, 2014.

[2] Bullguard, «http://www.bullguard.com,» 15 09 2016. [En línea]. Available: http://www.bullguard.com/es/bullguard-security-center/internet-security/security-tips/cybercrime.aspx.

[3] Recovery Labs, «http://www.delitosinformaticos.info,» 02 10 2016. [En línea]. Available: http://www.delitosinformaticos.info/delitos_informaticos/definicion.html.

[4] Kaspersky, «www.securelist.com,» 12 10 2015. [En línea]. Available: https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/.

[5] M. K. a. J. S. Rafael Fedler, «An Antivirus API for Android Malware Recognition,» *IEEE,* p. 2, 2013.

[6] symantec, «https://www.symantec.com,» 03 10 2016. [En línea]. Available: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad.

[7] RSA, «www.rsa.com,» 7 09 2016. [En línea].

[8] Microsoft, «www.microsoft.com,» 2013. [En línea]. Available: https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx.

[9] B. M. Hernández, C. E. Paez y F. A. Simanca H., «A Look at Usability, Accessibility and Cybersecurity Standards in Software Development,» *Communications in Computer and Information Science,* vol. 1485, nº 1, pp. 484-496, 2021.

[10] K. S. Samuel Marchal, «Know Your Phish: Novel Techniques for Detecting,» *IEEE,* p. 8, 2016.

[11] Panda Security, «http://www.pandasecurity.com/,» 27 06 2016. [En línea]. Available: http://www.pandasecurity.com/spain/mediacenter/seguridad/whaling-amenaza-contra-empresas/.

[12] S. E. Guevara, «La seguridad informática, una disciplina que no debemos desconocer,» *Revista Avenir,* vol. 1, nº 1, pp. 4-7, 2017.

[13] F. Maggi, «Are the Con Artists Back?,» *IEEE,* p. 4, 2010.

[14] Bancolombia, «http://www.grupobancolombia.com/,» 01 11 2016. [En línea]. Available: http://www.grupobancolombia.com/wps/portal/personas/aprender-es-facil/seguridad/telefono-celular/vishing/.

[15] A. H. M. K. O. Salem, «Awareness Program and AI based Tool to Reduce,» *IEEE,* p. 4, 2011.

[16] M. &. R. R. Hermansson, Artist, *Fighting Social Engineering.* [Art]. University of Stockholm.

[17] *La protección de la información y de los datos,* 2009.

[18] J. A. Rola Al Halaseh, «Analyzing CyberCrimes Strategies: The Case of Phishing Attack,» *IEEE,* p. 7, 2016.

[19] J. P. Stephen McCombie, «Winning the Phishing War,» *IEEE,* p. 8, 2011.

[20] SoftDoit, «https://www.softwaredoit.es,» 2016. [En línea]. Available: https://www.softwaredoit.es/definicion/definicion-exploit.html.

[21] ESET, «http://www.welivesecurity.com/,» 2016. [En línea]. Available: http://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/.

[22] Y. K. A. M. A. Habib Allah Yajam, «Sentence-based Passwords,» *IEEE,* p. 3, 2016.

[23] OpenWall, «http://www.openwall.com/john/,» 2016. [En línea].

[24] Panda Security, «http://www.pandasecurity.com,» 21 02 2016. [En línea]. Available: http://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/.

[25] Y. X. ,. C. Abdullah Algarni, «Measuring Source Credibility of Social Engineering Attackers on Facebook,» *IEEE,* p. 10, 2016.

[26] COMODO , «https://www.comodo.com,» 2016. [En línea]. Available: https://www.comodo.com/resources/home/what-are-phishing-scams.php.

[27] Avira, «https://www.avira.com,» 2016. [En línea]. Available: https://www.avira.com/es/support-what-is-phishing.

[28] V. P. A. A. M. H. Ibrahim Ghafir, «Social Engineering Attack Strategies and Defence,» *IEEE,* pp. 3-4, 2016.

[29] MCafee, «https://home.mcafee.com,» 2016. [En línea]. Available: https://home.mcafee.com/virusinfo/glossary?ctst=1.

[30] Norton, «http://co.norton.com,» 25 10 2016. [En línea]. Available: http://co.norton.com/victim/article.

[31] R. E. Crossler, «Protection Motivation Theory:,» *IEEE,* pp. 3-5, 2010.

[32] N. J. Dong Yan, «Protecting Enterprise Information from Employee's Misappropriation in China,» *IEEE,* pp. 2-3, 2016.

[33] MinTIC, «http://www.mintic.gov.co/,» 01 11 2016. [En línea]. Available: http://www.mintic.gov.co/portal/604/w3-article-6165.html.