InterSedes, *Revista electrónica de las sedes regionales de la Universidad de Costa Rica*,
ISSN 2215-2458, Volumen XXIV, Número 49, Enero-Junio, 2023.
10.15517/isucr.v24i49 | intersedes.ucr.ac.cr | intersedes@ucr.ac.cr

InterSedes

ESP Editorial Sede del Pacífico

Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo

Attacks based on social engineering in Colombia, good practices and recommendations to avoid risk

Paola Maritza Rincón Nuñez
Universidad Nacional Abierta y a Distancia.
Duitama, Colombia.
paola.rincon10@gmail.com

Resumen: En el artículo se describe el análisis realizado sobre los ataques de ingeniería social en Colombia; así como un compilado de buenas prácticas y recomendaciones para evitar el riesgo que pueden ser aplicables tanto a usuarios comunes como a empresas. Inicialmente se realiza una breve descripción de la terminología relacionada con la Ingeniería social, normativa, legislación y conceptos, esto con el propósito de familiarizar al lector; posteriormente se logra identificar cuáles son las técnicas de ingeniería social más utilizadas y que afectan a la población colombiana. Otro aspecto importante es mencionar las estrategias o campañas creadas por parte de las entidades del estado o privadas, para contribuir a mitigar la ocurrencia de incidentes relacionados o producidos por este tipo de ataques. A partir de esto, la ciudadanía, los entes gubernamentales y las empresas, deberán abordar el tema como una problemática socioeconómica, que puede afectar desde su entorno familiar hasta el laboral o, en el caso de las empresas, su imagen y reputación.

Palabras clave: Cibercrimen, Correo electrónico, Delito informático, Seguridad de los datos, Información

Abstract: The article describes the analysis carried out on social engineering attacks in Colombia; as well as a compilation of good practices and recommendations to avoid risk that may be applicable to both common users and companies. Initially a brief description of the terminology related to social engineering, regulations, legislation and concepts is made, this with the purpose to familiarize the reader; Subsequently, it is possible to identify which are the most used social engineering techniques that affect the Colombian population. Another important aspect is to mention the strategies or campaigns created by state or private entities to help mitigate the occurrence of incidents related to or caused by this type of attack. Based on this, citizens, government entities and companies must address the issue as a socioeconomic problem, which can affect everything from their family environment to their work environment, or in the case of companies, their image and reputation.

Keywords: Cybercrime, Email, Computer crime, Data security, Information

Recibido: 07-03-22 | Aceptado: 28-06-22

Cómo citar (APA): Rincón Nuñez, P. M. (2023). Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo. InterSedes, 24(49), 120-150.

Publicado por la Editorial Sede del Pacífico, Universidad de Costa Rica

Introducción

Con el transcurso del tiempo, empresas, trabajadores y consumidores no logran dimensionar el valor que representan los activos de información y se exponen a una perdida innecesaria de datos o de dinero. Los ciber delincuentes son conscientes de esta situación y mediante diversas técnicas buscan engañar a los usuarios para obtener un beneficio, generalmente económico.

Por esta razón, se analiza el impacto de los ataques de ingeniería social en Colombia desde el año 2016, para lograr identificar cuáles delitos informáticos relacionados son los que más se producen en el país. Otro aspecto por verificar es la evolución que han tenido dichos ataques, puesto que, a medida que mejora la tecnología y las medidas de protección, también las técnicas utilizadas por los atacantes se fortalecen. Para responder a la necesidad de protección ante la ingeniería social que exige la sociedad, es necesario hacer la revisión de las estrategias diseñadas para este fin por parte de las entidades del estado o entidades privadas. Esto permite conocer qué aspectos contribuyen a mitigar de alguna manera este riesgo.

La información de personas o empresas que se encuentra pública en sitios de internet es la que más adelante les permite a los atacantes construir su estrategia de ataque, de alguna manera ganar la confianza de las víctimas y finalmente acceder a los datos confidenciales o simplemente engañar para obtener beneficio económico. De la investigación realizada se obtiene un conjunto de buenas prácticas y recomendaciones mediante las cuales es posible contribuir para la concienciación en seguridad de la información o para la elaboración de una guía que les permita a las personas tomar medidas de protección frente a este tipo de ataques.

Se puede tener innumerables tipos de contraseñas, protección física o lógica, pero cuando el activo de la información se encuentra bajo custodia o manejo de un ser humano, es posible que sea vulnerado si el atacante hace uso de los ataques basados en la ingeniería social y la tecnología.

Aunque la ingeniería social y los ataques relacionados no son algo novedoso, puesto que desde hace varios años se ha venido hablando del tema y se ha producido información al respecto, al observar un panorama de los ciber delitos en el mundo se observa

cómo ataques de ingeniería social se ubican en los primeros lugares, y a medida que avanza la tecnología e internet, estos ataques también evolucionan y emplean técnicas cada vez más sofisticadas. En el trabajo de grado titulado Estudio de metodologías de Ingeniería Social, se define como un "conjunto de técnicas o estrategias sociales que se utilizan de manera predeterminada por un usuario para obtener algún tipo de ventaja respecto a otros" (Berenguer, 2018, p. 2).

Esto implica que aún no existe ningún sistema que esté en capacidad de prevenir estos ataques. Para el año 2016, en Colombia el crecimiento de los ataques de ingeniería social fue considerable, esto se reporta en el informe *Amenazas del cibercrimen en Colombia 2016-2017* de la Policía Nacional, donde se evidencia que hubo un incremento del 114% de ataques de malware con respecto al año 2015. El hurto por medios informáticos y semejantes representó el 68% de los casos reportados, seguido del acceso abusivo a un sistema informático con 13% y violación de datos personales con 12% (Policía Nacional de Colombia, 2017).

El informe *Balance cibercrimen en Colombia 2017* (Policía Nacional de Colombia) hace un resumen del año 2017 en cuanto a ciberdelitos en Colombia, lo cual arroja resultados poco esperanzadores ya que se incrementan los delitos y aparecen nuevas técnicas para engañar a los ciudadanos: el 60% de las estafas se realizaron por compra o venta en línea (*Vishing*); estafas por llamadas telefónicas, 16%; engaños a través de mensajes de texto (*Smishing*), 13%; estafas asociadas a cartas nigerianas, 8% y, para cerrar, ofertas fraudulentas, con un 2% (2017).

La problemática que golpea a la población es evidente, ya que los delincuentes pasan al mundo digital para cometer las actividades ilícitas, y es allí donde logran captar bastantes víctimas. En el caso de un *Phishing*, en cuestión de minutos el atacante puede enviar el señuelo a miles de personas, y solamente tiene que esperar que empiecen a morder el anzuelo. Una implicación adicional de la ingeniería social es que también se utilizan estas técnicas para realizar la distribución de virus, gusanos, *spyware*, *ransomware* y otros programas maliciosos usados para obtener información confidencial (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, 2016), así se manifiesta en la "Guía para la implementación de seguridad de la información en una MIPYME".

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

La ingeniería social supone una práctica en términos de la seguridad informática, entendida como un conjunto de técnicas empleadas para obtener información confidencial. Mediante la manipulación de la víctima, generalmente lo que el atacante busca es obtener un beneficio económico, o bien, datos personales, credenciales de acceso o números de cuentas. Una de las estafas más conocidas es el famoso timo 419 o carta nigeriana, que, según la tesis *Fraudes en Internet*, de Dinca (2016), es uno de los más antiguos, y tomó ese nombre porque viola el artículo 419 del código penal de Nigeria. Este fraude consiste en prometer a la víctima parte de una enorme fortuna y para hacer efectiva la transferencia del dinero, se solicitan datos personales y número de cuenta bancaria. Un aspecto importante es que la persona que supuestamente será beneficiada debe cubrir unos gastos que se generan por la transferencia internacional y otros trámites requeridos para completar el traspaso de los fondos.

Con la masificación de las tecnologías y el acceso a internet los delincuentes encontraron un campo de acción más amplio para llevar a cabo las estafas y engaños, en el Boletín de Información, número 324 de Sánchez (2012), *Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos*, menciona que a través del *mail spoofing* se logran obtener números de tarjetas de crédito. Esta técnica consta de la suplantación por medio de correo electrónico de una entidad legítima, en este caso de un banco.

En el artículo de Oxman (2016), se realiza una aproximación a nivel legal de las consecuencias que acarrea para los delincuentes la práctica de estos dos tipos de fraudes informáticos. No obstante, existe normativa en los países que condenan estos delitos, pero aun así se siguen cometiendo, ya que muchas veces las víctimas prefieren no denunciar.

En Colombia, la situación en cuanto a los ataques de ingeniería social va en aumento, de acuerdo con el informe publicado por la Cámara Colombiana de Informática y Telecomunicaciones (2019), *Tendencias cibercrimen Colombia 2019-2020*, los incidentes que más se reportan en el país son: *Phishing*, 42%; suplantación de identidad, 28%; envío de malware, 14%; y los fraudes, 16%.

Según este informe, la tendencia para el año 2020 en Colombia es que este tipo de ataques de ingeniería social aumenten, haciendo uso de BEC (*Business Email Compromise*) basado en *Deepfake*

(técnica de inteligencia artificial que permite la edición de videos y audios falsos de personas que hacen pasar por reales), *Botnets* para difusión de correos extorsivos, uso de perfiles falsos para difundir *malware* y tráfico de datos robados en *Darknet*.

Referente teórico

Los ataques de ingeniería social se han encargado de comprobar que el eslabón más débil de la cadena de la seguridad informática es el ser humano, ya que continúan presentándose incidentes de ciberseguridad en donde el atacante obtiene credenciales de acceso o información sensible gracias a la manipulación de un usuario. Kevin Mitnik, en su libro *El arte del engaño*(2001), explica cómo logró obtener contraseñas o información sensible solamente fingiendo ser otra persona, esto a través de "un tipo de ataque contra el elemento humano durante el cual el atacante induce a la víctima a divulgar información o realizar acciones que no deberían" (Nohlberg, 2018).

Uno de los activos con mayor valor para las organizaciones es la información que manejan. Dicha información es todo el conjunto de datos que proporciona sentido a una organización, datos que definen procesos, datos que intervienen en procedimientos y, en caso de no tomar las medidas suficientes para protegerlos, serán datos que caerán en manos equivocadas. Por otra parte, haciendo más extenso el concepto de seguridad en lo referente a las telecomunicaciones y la informática, es posible encontrar dos diferentes enfoques: seguridad de la información y seguridad informática. En primera medida, la seguridad de la información se constituye como un conjunto de medidas y procedimientos, de tipo humano y técnico cuyo objetivo es proteger la integridad, confidencialidad y disponibilidad de la información. Esto también es conocido como la tríada de la CIA, la cual se refiere a un modelo de seguridad de la información formado por tres componentes principales: Disponibilidad, Integridad y Confidencialidad.

De acuerdo con la definición anterior, el concepto es amplio porque reúne medidas de seguridad que impactan sobre la información sin importar su tipo; es decir, es independiente del medio de almacenamiento o la manera en la que es transmitida. Por otra parte, la seguridad informática es una rama de la seguridad de la

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

información cuyo objetivo es proteger toda aquella información que se gestiona a través de una infraestructura tecnológica, sistemas de información y telecomunicaciones. Esta protección va orientada a lo que se quiere proteger y al momento en el que se realiza la protección. En función de lo que la organización quiere proteger:

- Seguridad física: protección física y del entorno (incendios, robos, inundaciones, etc.).
- Seguridad lógica: mecanismos de protección que se aplican sobre la parte lógica del sistema informático.
- En función del momento en el que la organización efectúa la protección:
- Seguridad activa: tipo de seguridad que se encargada de prevenir, detectar y evitar incidentes que afectan a los sistemas informáticos.
- Seguridad pasiva: técnicas y procedimientos que se llevan a cabo para hacer que las consecuencias del incidente sean mínimas.

La mayoría de los profesionales de la seguridad informática están familiarizados con la ingeniería social y sus peligros. Pero hay que tener en cuenta que la ingeniería social puede tener diferentes definiciones dependiendo del contexto. Para el desarrollo del presente documento la definición más aproximada y concisa es la propuesta por Alexander: "la ingeniería social es un vector de ataque que depende en gran medida de la interacción humana y a menudo implica engañar a las personas para que rompan los procedimientos normales de seguridad" (2016).

Básicamente, para que un ataque logre tener el éxito y el impacto esperado, se debe engañar al usuario del sistema o persona. Para este fin los atacantes han encontrado diferentes técnicas y métodos, los cuales a través del tiempo se han vuelto más sofisticados y con un nivel mayor de complejidad. Esto asegura en cierta medida que para la víctima sea complicado evadir un ataque de esta naturaleza y por este motivo los ciber criminales encuentran en la ingeniería social un mecanismo efectivo para penetrar en las organizaciones, haciendo uso de *Phishing*, *Smishing*, *Vishing* e *Impersonation*. Con el fin de explicar de mejor forma estos términos a continuación se

mencionan las definiciones de cada uno:

Phishing. En el documento "Qué es el Phishing y cómo protegerse", se explica que el *Phishing* constituye una de las modalidades de estafa preferida por los atacantes, con el fin de conseguir datos del usuario como su número de tarjeta de crédito, o cualquier información que posteriormente pueda ser utilizada de forma fraudulenta (AcensTechnologies, 2014). Por otra parte, el artículo científico "Seguridad por capas frenar ataques de Smishing" define el término *Smishing* como una combinación de la palabra "Phishing" y "SMS". Es un nuevo tipo de técnica o variante del *Phishing* que tiene como propósito robar la información de un usuario, mediante el uso del servicio de mensajería de texto (SMS) de un teléfono móvil (Martínez, 2018).

Adicionalmente, el *Vishing*, que es una combinación de las palabras 'voz' y 'Phishing', es un fraude telefónico en el que los estafadores intentan engañar a la víctima para que divulgue información personal, financiera o de seguridad, o que transfiera dinero (Europol, 2019). Esta definición se presenta en el documento titulado "Fraude del CEO".

Finalmente, la *Impersonation* consiste en ataques de suplantación de identidad que pueden ser particularmente perjudiciales para la reputación en línea de la víctima. A medida que los motores de búsqueda agregan cada vez más los datos en línea de las personas, utilizados para una variedad de propósitos, incluida la evaluación de su idoneidad para el empleo, los ataques de suplantación, particularmente aquellos que no se detectan, pueden tener serios efectos adversos para las víctimas, incluso en el mundo fuera de línea (Goga y otros, 2016). Así describen este ataque en el artículo "Exposing Impersonation Attacks in Online Social Networks".

Actualmente para cualquier persona es común el uso de celular y equipos de cómputo, por este motivo es importante conocer y estar alerta sobre los distintos tipos de amenazas cibernéticas. Claudia Castillo, de BBVA, menciona que: "El 'phishing', 'vishing' y 'smishing' son algunos los fraudes electrónicos que utilizan los ciber delicuentes para robar datos privados, pero mediante información y prevención se pueden evitar" (Castillo, 2018). Al tener las personas acceso con mayor facilidad a las tecnologías y dispositivos móviles, se facilita la actividad de los ciberdelincuentes ya

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

que lanzan muchos ataques de este tipo a diario y la cantidad de víctimas potenciales es alto. Por esta razón los actores maliciosos continúan perfeccionando estas técnicas para conseguir una tasa de efectividad mayor.

La ingeniería social, según Thomas Douglas, investigador de la Universidad de Minnesota, es un término que ha sido utilizado entre *crackers* y samurái para técnicas de *cracking* que dependen de debilidades en el factor humano, más que del software; cuyo objetivo es engañar a las personas para que revelen contraseñas u otra información que comprometa la seguridad de un sistema objetivo (2003). Las estafas clásicas incluyen llamar a una marca que tiene la información requerida y hacerse pasar por un técnico de servicio de campo o un compañero de trabajo con un problema de acceso urgente. Para enmarcar la ingeniería social dentro de la seguridad de la información se debe hacer una aproximación más detallada del término, para así comprender la importancia de no ser víctima de un ataque que utilice metodologías asociadas, lo cual es un aspecto clave para determinar los conceptos de forma más acertada y ajustada. En el artículo "Ingeniería Social: El Ataque Silencioso", se explica que el fin del atacante que hace uso de la ingeniería social es explotar al eslabón más débil de la organización, el usuario. Dependiendo de su osadía, habilidades y conocimientos, el atacante puede utilizar herramientas tecnológicas, incluso encuentros cara a cara para obtener la información que necesita (López & Salvador, 2015).

Es relevante reconocer que no solamente el usuario final de los sistemas de información está expuesto a sufrir un ataque de Ingeniería Social; el personal de seguridad informática también está expuesto y es igual de vulnerable, situación que pudo ser comprobada por el "Experimento Robin Sage". En este experimento se creó un perfil falso en las redes sociales Twitter, LinkedIn y Facebook: Robin Sage, 25 años, analista de seguridad en la Armada de los EE.UU, graduada en el MIT, con 10 años de experiencia en seguridad. Transcurridos 28 días logró conseguir: 300 contactos, acceso a datos militares confidenciales y dos ofertas de trabajo (una de ellas de Google). La identidad, por supuesto, era falsa, la foto fue extraída de un sitio web de pornografía, esto en la red ayudó a generar la confianza (Valverde, 2012).

Para que un ataque de ingeniería social impacte de la manera esperada en la víctima, es necesario que se recopile cierta información previamente (a través de internet o presencialmente), lo cual ayuda a confundir o distraer al usuario, ya que se da una falsa sensación de seguridad cuando se proporcionan datos que supuestamente solo podrían saber entidades o personas que tienen alguna relación directa. Por este motivo es que generalmente se suplantan organizaciones o empresas de renombre.

El Instituto Nacional de Ciberseguridad de España, en el artículo "OSINT - La información es poder" (La Inteligencia de fuentes abiertas – OSINT) es el proceso de recopilar datos disponibles de fuentes abiertas públicas para su uso en labores de inteligencia. En el contexto de las agencias de inteligencia, el término "abierto" se refiere a fuentes que están disponibles para el público en general en contraposición a fuentes cerradas/clasificadas o clandestinas (Martínez, 2016). Por otra parte, el artículo "Ingeniería social: ¿Se puede hackear a una persona?" establece que, independientemente de cómo se obtenga la información mediante OSINT, es necesario tener una idea clara sobre lo que se busca (Policía Municipal, 2019). A primera vista, puede parecer algo sencillo, pero no lo es. Inicialmente se piensa en obtener toda la información sobre el objetivo, pero cada tipo de información tiene diferente valor y el valor puede cambiar con el tipo de ataque que se esté buscando ejecutar.

Existen técnicas que han evolucionado, de tal forma que se presentan como ataques más precisos y que casi siempre logran su cometido. Los ciber criminales buscan que el impacto sea alto y se dirigen a organizaciones que manejan información más relevante y valiosa que un usuario convencional. Una característica de la ingeniería social es que evoluciona de acuerdo con las exigencias del entorno y las técnicas asociadas también adquieren dimensiones diferentes, con lo cual se logra un nivel de efectividad que permite vulnerar incluso a personal con conocimientos técnicos o competencias en seguridad informática. Algunas de las modalidades más usadas actualmente son:

Spear phishing. Es usado por atacantes más sofisticados que delimitan su objetivo y aumentan la precisión de los mensajes, haciendo atractivo el mensaje y con una aparente legitimidad. De acuerdo con CERT-UK, en "An introduction to social enginee-

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

ring", "Si bien un ataque dirigido de este tipo disminuye el número de víctimas potenciales, también es probable que resulte en un mayor beneficio para el atacante" (2015). Los correos electrónicos que se envían de esta manera, en su mayoría, parecen legítimos y son extremadamente difíciles de identificar como maliciosos.

También se encuentra la técnica de *Baiting*, que es muy similar a un troyano. Utiliza un medio físico y hace uso de la curiosidad o avaricia de la víctima. Se asemeja a un ataque de *phishing*. Sin embargo, "lo que lo hace diferente de otros tipos de ataques de ingeniería social es el ofrecimiento de un artículo u objeto que los piratas informáticos usan para atraer a sus víctimas" (Fernández, 2018). Los *baiters* (así son llamados estos atacantes) en ocasiones utilizan música o descargas gratuitas de películas, u ofrecen credenciales a una determinada página o sitio web.

Por otra parte, se encuentra el *Watering hole attack*. "Este ataque busca comprometer a un grupo específico de usuarios finales al infectar sitios web que los miembros del grupo visitan" (Wright, 2019). El objetivo es infectar la máquina de un usuario y obtener acceso a la red en el lugar de trabajo del objetivo.

Finalmente, *Quid pro quo* es un ataque que promete la obtención de beneficios a cambio de información; el beneficio que normalmente se ofrece es un servicio. En el caso del *baiting* se ofrece un bien a cambio. Se puede considerar una solicitud de información suya o de su organización a cambio de algún tipo de compensación, que puede ser servicio técnico o servicios profesionales.

Una de las primeras descripciones sistemáticas del proceso de explotación de la ingeniería social como un vector de ataque fue dado por Kevin Mitnick (2001). El proceso que propone tiene cuatro fases:

1. Investigación: Se refiere al proceso de recopilar tanta información como sea posible sobre el objetivo. Esta información se utiliza en fases posteriores y es de importancia crítica para realizar los ataques dirigidos.
2. Desarrollo de *Rapport and Trust*: En esta fase se hace uso de varias técnicas para lograr que la víctima confíe en el atacante. La información recopilada en la fase anterior, a menudo se usa para ese propósito.
3. Explotación de la confianza: En la fase de "explotación" de

un ataque de ingeniería social, el atacante logra una ganancia medible en información o privilegios.

4. Utilice la información: En la fase final del ciclo hace referencia a "cobrar" las ganancias obtenidas en la fase anterior. Como lo insinúa el término "Ciclo de ataque", esta fase puede pasar nuevamente a otra fase de investigación, completando así la naturaleza cíclica del proceso. Esta transición es la ingeniería social.

Metodología

A partir de una investigación realizada sobre los ataques basados en ingeniería social en Colombia, se busca proponer un compilado de buenas prácticas y recomendaciones para evitar el riesgo o ser víctimas de este tipo de ataques. Inicialmente se realizó la definición del problema, así como la referenciación ante las autoridades competentes. Posteriormente se estableció el alcance del proyecto, el cual pretende identificar los ataques más recurrentes en Colombia que usan técnicas de ingeniería social y proponer medidas para contrarrestar esta amenaza. Es importante tomar un periodo en el cual sea posible analizar el comportamiento de los delitos informáticos, de tal forma que se evalúa lo denunciado en el país desde el año 2016 al 2019.

Para la recolección de datos se acudió al CAI Virtual de la Policía Nacional de Colombia, específicamente la herramienta de Ciberincidentes (https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real), la cual muestra en tiempo real o en un periodo definido por el usuario la cantidad de delitos informáticos denunciados y realiza una clasificación de los mismos. A continuación, en la Figura 1 es posible apreciar la interfaz de la herramienta, donde se muestra a la izquierda el tipo de delito que se denuncia, en la parte derecha se muestra la modalidad bajo la cual se cometió el delito, en la parte inferior derecha se muestra el sector que resultó afectado y finalmente en la parte inferior se muestra la fecha, hora y ciudad donde se registraron los hechos.

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

Figura 1

Herramienta ciberincidentes – Policía Nacional

Nota: La figura muestra la herramienta ciberincidentes. Fuente: CAI Virtual Policía Nacional de Colombia (2022).

Finalmente, se realizó un análisis que permitió identificar los delitos informáticos que hacen uso de técnicas de ingeniería social y a partir de esto se obtuvo el compilado de buenas prácticas y recomendaciones para contribuir a mitigar este tipo de ataques y generar en las personas y organizaciones una cultura de seguridad de la información.

Enfoque

El enfoque de la investigación es cuantitativo, debido a que se realizó una valoración de los casos denunciados en Colombia. El alcance del estudio es descriptivo ya que se identificaron algunos indicadores y características propias de cada tipo de ataque, que posteriormente permitieron definir un conjunto de recomendaciones y buenas prácticas para mitigar esta amenaza.

Población de estudio

Se realizó levantamiento y análisis de información sobre los casos denunciados en Colombia del año 2016 al 2019, haciendo uso de la herramienta de ciber incidentes del CAI Virtual de la Policía Nacional de Colombia.

Técnicas de recolección

Inicialmente se realizó una revisión documental sobre la ingeniería social y los ataques basados en esta, con el fin de conocer a nivel conceptual y teórico este fenómeno que afecta a la ciudadanía y a las empresas, lo que permitió obtener un mayor grado de conocimiento del tema de estudio y realizar una propuesta estructurada que contiene un compilado de buenas prácticas y recomendaciones para combatir este tipo de delitos informáticos desde la perspectiva de la prevención.

Procesamiento de análisis

En el informe *Tendencias del ciber crimen en Colombia*, se estima que cerca de un 90% de los ciberataques a empresas en Colombia se deben a ingeniería social. La clave del asunto está en que el ciber delincuente necesariamente debe engañar a la víctima, para lograr este propósito gana su confianza o simula ser una persona o entidad que genera confianza, para lograr obtener acceso a la in-

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

formación, gracias a esto se han originado los BEC, *Bussines email compromise* (Cámara Colombiana de Informática y Telecomunicaciones, 2019), lo cual no es más que el compromiso a través de los correos electrónicos corporativos. Cada vez es más frecuente encontrar que dentro de las organizaciones y grandes empresas, se habla de correos sospechosos o que su contenido no correspondía al contexto de la organización.

La ingeniería social y la explotación de vulnerabilidades siguen siendo los principales vectores que puede aprovechar un atacante para comprometer los servicios de una empresa. Los engaños basados en ingeniería social han evolucionado a lo largo de los años, volviéndose cada vez más efectivos. Para lograr determinar cuáles son los ataques de ingeniería social más utilizados en Colombia, se hace uso de la herramienta del CAI VIRTUAL de la Policía Nacional que permite, a través de un filtro temporal, identificar la cantidad de delitos informáticos que se denuncian y bajo qué modalidad fueron ejecutados los ataques. Para efectos de poder realizar el análisis con más detalle se realiza la búsqueda por años: 2016, 2017, 2018 y 2019.

Para el año 2016, se logra evidenciar que, en Colombia, delitos relacionados con la ingeniería social, como estafa, suplantación, *phishing*, *vishing* y *smishing*, ocupan los primeros lugares dentro de las denuncias realizadas. El sector ciudadano ha sido el más afectado por este tipo de ataques.

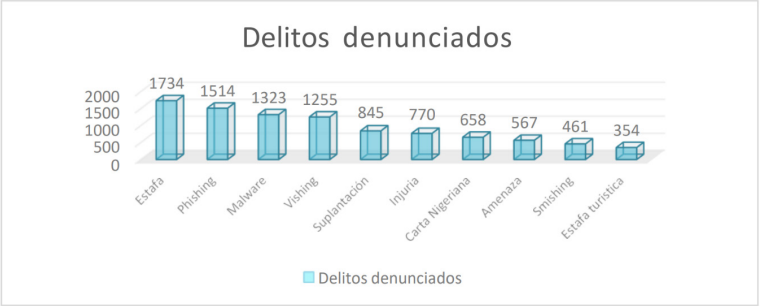
Para el año 2017, los delitos asociados a la ingeniería social, como estafa, suplantación, *phishing* y *vishing*, ocupan los cuatro primeros lugares dentro de las denuncias realizadas. El sector ciudadano continúa siendo el más afectado por este tipo de ataques.

En el año 2018, los delitos asociados a la ingeniería social continúan dentro de los diez primeros lugares dentro de las denuncias realizadas, con modalidades como suplantación, estafa, *phishing*, *vishing* y *smishing*. El sector ciudadano continúa siendo el más afectado por este tipo de ataques.

En el 2019, la situación es idéntica, con modalidades como: estafa, *phishing*, *vishing*, suplantación, carta nigeriana, *smishing* y estafa turística, como se logra evidenciar en la Figura 2.

Figura 2

Delitos denunciados en el año 2019

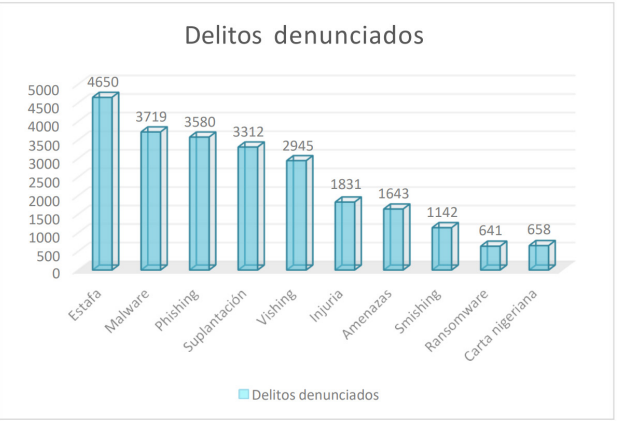


Fuente: CAI Virtual, Policía Nacional de Colombia (2022).

Para realizar una síntesis de lo encontrado gracias a la herramienta del CAI Virtual de la Policía Nacional de Colombia, se procede a compilar los datos para lograr obtener cuáles delitos asociados a la ingeniería social son los más comunes en Colombia entre 2016 a 2019, los cuales se muestran en la siguiente figura:

Figura 3

Delitos denunciados entre los años 2016 y 2019



Fuente: CAI Virtual, Policía Nacional de Colombia (2022).

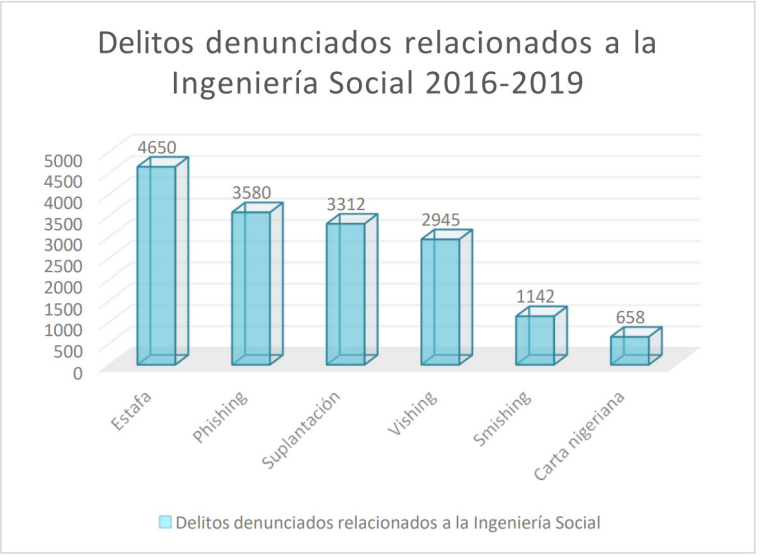
De acuerdo con el análisis de los datos anteriores, es posible deducir que, en el país, una de las técnicas más utilizadas y que mayor impacto ha tenido es la estafa, con el 17 %; en tercer lugar, el *phishing*, con el 13 %; en cuarto lugar, la suplantación, con el 12%;

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

quinto lugar, *Vishing*, con el 10%; octavo lugar para el *Smishing*, con el 4%; y finalmente la carta nigeriana en décimo lugar, con el 2%. Con el fin de resaltar y evidenciar de mejor manera lo anterior, es elaborada la gráfica que se muestra en la figura 4 que consolida los delitos más denunciados y que están relacionados a la ingeniería social, lo cual permite que sea posible dimensionar e identificar el comportamiento de este tipo de delitos en Colombia.

Figura 4

Delitos denunciados relacionados a la ingeniería social entre 2016 y 2019



Fuente: CAI Virtual, Policía Nacional de Colombia (2022).

Con esto se obtiene que, en el periodo seleccionado, el 58% de los delitos informáticos denunciados en Colombia está relacionado a técnicas de la ingeniería social. Un aspecto que llama la atención es la aparición en 2019 de la carta nigeriana: una de las técnicas más antiguas ha vuelto a aparecer en escena. Tomando en cuenta los vectores de ataque es posible determinar que el 73% de los ataques ha sido mediante correos fraudulentos personalizados, lo que comúnmente se conoce como *phishing*. Aunque se tiene una

categoría especial para esta técnica, las campañas de *malware* y *ransomware* se entregan haciendo uso del *phishing*.

Al realizar un análisis sobre el comportamiento del cibercrimen en Colombia tomando como base el número de denuncias instauradas ante el ecosistema de la Fiscalía General de la Nación, las policías judiciales del CTI y la Policía Nacional (DIJIN-SIJIN), a través del aplicativo a denunciar, para finales del mes de noviembre del 2021 registraron 46.527 denuncias por distintos delitos, lo que es equivalente a un incremento del 21% respecto al año 2020. Si se tienen en cuenta comparativamente los años 2019 y 2021, es decir, sin contabilizar el año 2020 en el cual se vivió la pandemia, el incremento alcanzó un 107% acumulado entre el incremento suscitado durante el 2020 y el aumento continuo durante el 2021.

Sin duda el ciberdelito se ha convertido en la tipología criminal de mayor crecimiento en Colombia durante los últimos tres años, impulsado por aceleradores como la pandemia y el consecuente incremento del comercio electrónico cuyo crecimiento alcanzó el 59.4% en las transacciones durante el periodo de cuarentena obligatoria y del 35% durante el 2021, con ventas estimadas en 37 billones de pesos al finalizar el año según cifras de la Cámara de Comercio electrónico de Colombia CCCE (TicTac, 2021).

Durante el año 2021, con un 45% de variación porcentual respecto a los casos registrados durante el 2020, la Violación de Datos Personales, con 13.458 casos, es el delito de mayor crecimiento en el país. Lo anterior en relación con las campañas de *Phishing*, mediante las cuales los cibercriminales envían enlaces que dirigen al usuario hacia sitios web con formularios que generalmente son utilizados para obtener información personal.

El acceso abusivo a sistemas informáticos presentó un total de 9.926 denuncias, y un incremento del 18% respecto a las cifras reportadas durante el 2020. Posteriormente, se encuentra el hurto por medios informáticos, el cual tuvo un incremento del 3%. No obstante, se han registrado 17.608 denuncias entre enero y noviembre del año 2021, siendo el delito que sucede con mayor frecuencia en el país.

Las actividades previas de ingeniería social que realizan los ciberdelincuentes están vinculadas a la modalidad de *SIM SWAPPING* que sigue teniendo crecimiento durante el 2021 y que ha constituido la principal técnica que utilizan los cibercriminales

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

para suplantar a la víctima y posteriormente apoderarse de la SIM CARD, para acceder de manera fraudulenta a los servicios de banca electrónica de la víctima suplantada.

Con 7.654 casos, la suplantación de sitios web tuvo un incremento similar del 3% respecto al año 2020, siendo el *Phishing* y el *Smishing* las principales modalidades utilizadas por los cibercriminales, algunas veces combinados con técnicas de llamadas en escenarios de ingeniería social y manipulación.

Durante el año 2021 se presentó un incremento de casos de *Smishing* por el uso creciente de mensajes de texto vía SMS que incorporan dentro del cuerpo del mensaje una URL acortada de la entidad suplantada.

Estrategias propuestas por parte de las entidades del estado colombiano para la mitigación de los ataques de ingeniería social

En cuanto a la generación de estrategias que contribuyan a mitigar el riesgo asociado a los ataques de ingeniería social, el estado colombiano y entidades del sector privado han diseñado estrategias para que los ciudadanos aprendan a identificar ataques de este tipo y, si en determinado momento han sido víctimas, ha creado los canales por los cuales puede realizar la respectiva denuncia y poner en conocimiento de las autoridades la ocurrencia del hecho.

colCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Este grupo tiene como finalidad y principal responsabilidad la coordinación de la Ciberseguridad y la Ciberdefensa Nacional, que estará en el marco del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. El propósito principal es la coordinación de acciones necesarias para proteger la infraestructura crítica del Estado colombiano frente a cualquier emergencia relacionada con la ciberseguridad que atente o comprometa la seguridad y defensa nacional (colCERT, 2017).

CSIRT-PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional. Este grupo fue creado con el propósito de atender las necesidades en cuanto a la prevención, atención e investigación de eventos e incidentes de seguridad informática, esto con el fin de proteger la infraestructura tecnológica, activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones. Uno de los objetivos del CSIRT es proveer asistencia técnica, asesoría y apoyo a

la comunidad y a las organizaciones públicas o privadas, en cuanto a la protección ante amenazas o incidentes informáticos. De la misma manera, busca consolidar procesos y procedimientos de atención de incidentes de seguridad de la información mediante el uso de estándares y buenas prácticas. También activar mecanismos de colaboración para la coordinación y gestión de incidentes entre entidades (CSIRT-PONAL, 2018).

CSIRT Financiero – Equipo de apoyo para la respuesta a incidentes de Ciberseguridad para el sector financiero colombiano. Este equipo ha sido desarrollado por la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, con el fin de proporcionar apoyo y respuesta ante incidentes que afectan al sector financiero y a la vez fomentar la colaboración entre sus miembros e intercambio de información para afrontar de mejor manera las amenazas cibernéticas. El equipo es altamente calificado y contribuye en procesos de gestión de riesgos y seguridad de datos con el fin de crear espacios digitales seguros (CSIRT Financiero, 2019).

Sistema Nacional de Denuncia Virtual ¡ADenunciar!. Este sistema, que se ha implementado en conjunto entre la Policía Nacional y la Fiscalía General de la Nación, permite que los ciudadanos puedan dar trámite a las diferentes solicitudes que están habilitadas en este sistema, pero para esto se requiere del registro del ciudadano. Les permite a los ciudadanos realizar 6 tipos de denuncias virtuales, las cuales serán atendidas por funcionarios de la policía judicial, siendo estos los encargados de validar si la información califica como denuncia penal y posteriormente realizarán el trámite correspondiente que haya lugar (Fiscalía General de la Nación, 2022).

Los delitos que se pueden denunciar son los siguientes: Hurto a Comercio, hurto a personas, hurto a residencias, *delitos informáticos,* pornografía infantil y extorsión.

En el caso de estudio, los delitos informáticos que se pueden denunciar son aquellas conductas en que los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc.

CAI Virtual. En este portal, los ciudadanos pueden encontrar el medio que les permite reportar incidentes informáticos, también cuenta con un mural del cibercrimen en donde se exhiben

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

muestras de las diferentes modalidades que utilizan los ciberdelincuentes para tratar de afectar a las personas. Por otra parte, se encuentra la publicación de boletines en donde se muestran las nuevas amenazas y la manera en la que se ejecutan los ataques informáticos. Allí se pueden encontrar las recomendaciones, guías e informes que contribuyen a generar en los ciudadanos una cultura de auto cuidado en aspectos de los sistemas informáticos y el uso de TICS (Policía Nacional de Colombia, 2018).

Resultados

En este apartado se muestran los resultados obtenidos de la investigación realizada, de donde se extrae el compilado de buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de ingeniería social. De acuerdo con el análisis realizado, en el periodo de 2016 a 2019, en Colombia se mantiene la tendencia por parte de los ciberdelincuentes del uso de técnicas relacionadas a la Ingeniería Social, lo cual se reafirma en el comportamiento del cibercrimen para los años 2020 y 2021, de tal forma que se identifican 6 modalidades que representan un riesgo para los usuarios de internet en nuestro país. Por lo tanto, se proponen unas buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de este tipo.

Estafa

Aunque directamente la estafa no es una técnica de Ingeniería Social, sí utiliza muchos de sus elementos, ya que normalmente se engaña a la persona para proceder con la estafa. Los delincuentes utilizan planes muy creativos para lograr engañar a muchas personas cada año. La tendencia actual es incorporar a las nuevas tecnologías los viejos trucos con el fin de lograr que las personas les envíen dinero o proporcionen información personal. A continuación, se ofrecen algunos consejos prácticos que les ayudarán a mantenerse en cierta medida más seguras.

- Detectar a los impostores. Los estafadores normalmente se hacen pasar por alguien en quien la víctima confía, como lo puede ser un funcionario de una entidad del gobierno, algún miembro de la familia, una organización benéfica, una entidad financiera o una empresa con la que hace o ha

hecho negocios. Por ningún motivo se debe entregar información personal respondiendo ese tipo de solicitudes inesperadas, ya sea como un mensaje de texto, una llamada telefónica o un correo electrónico, y por ningún motivo debe enviarse dinero.

- Verificar la información a través de una búsqueda en línea. Al digitar el nombre de determinada empresa o producto en el buscador, se sugiere incluir palabras como "revisión", "queja" o "estafa", esto traerá resultados que pueden ayudar a aclarar la situación. También es recomendable realizar una búsqueda que describa la situación, como "Llamada de Banco". También se pueden buscar los números de teléfono de los cuales se han comunicado para ver si están relacionados con alguna estafa o si otras personas los han denunciado.
- No se debe confiar totalmente en el identificador de llamadas. Actualmente la tecnología permite que sea posible falsificar la información del identificador de llamadas, por lo que el nombre y el número que se visualiza en pantalla no siempre es real. Si por algún motivo alguien llama solicitando dinero o datos personales, colgar la llamada es lo más recomendable. Si se tienen dudas o se cree que la persona que ha llamado podría estar diciendo la verdad, es posible volver a llamar a un número que se sepa que es legítimo o comunicarse con la entidad que dice representar.
- No se debe pagar por adelantado. Un estafador podría pedir que se realice un pago adelantado por cosas como alivio de deudas, ofertas de crédito o préstamos, asistencia hipotecaria o una oferta de trabajo. Incluso, uno de los timos más usados es manifestar que ganó un premio, pero antes debe pagar algún impuesto o tarifa para que se haga efectiva la transacción. Si la persona decide realizar el pago, probablemente cobrarán el dinero y desaparecerán.
- Las tarjetas de crédito cuentan con protección antifraude, pero algunos métodos de pago no incorporan esta medida de protección. Cuando se realizan transferencias de dinero mediante servicios como Western Union o MoneyGram es más arriesgado, porque es casi imposible recuperar el di-

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

nero. Eso también sucede con las tarjetas recargables o de regalo. Las entidades del gobierno y las empresas honestas nunca exigirán que utilice estos métodos de pago.

- Antes de entregar dinero o información personal, se recomienda hablar con alguien de confianza y tomarse el tiempo para analizar lo que está sucediendo. Los estafadores normalmente presionan a las personas para que tomen decisiones rápidamente. Incluso pueden llegar hasta a amenazar. A partir de esto es aconsejable tomar las cosas con calma, analizar la situación, realizar una búsqueda en internet sobre el caso o situación, consultar a un experto o simplemente contarle a un familiar o amigo.

Phishing

Es fundamental tener claro que el antivirus es solo una pequeña parte en cuanto a la protección contra *phishing*. La intervención del usuario final influye de manera significativa al momento de evitar este tipo de ataques.

Se sugiere a los usuarios en general aplicar lo siguiente con mayor detalle para evitar ser víctimas de *Phishing*:

- Tener precaución al hacer clic en hipervínculos o enlaces que vienen dentro de correos electrónicos, SMS (mensajes de texto) o mensajes instantáneos, incluso si parecen haber sido enviados desde una fuente conocida o confiable. Para asegurarse adónde redirigirá, debe ubicarse el cursor sobre el enlace antes de hacer clic ; en la parte inferior izquierda de la ventana aparecerá la, esto para verificar que la URL lleve a un sitio web legítimo. Adicionalmente, jamás debe proporcionarse la contraseña, número PIN o cualquier otro dato confidencial. Si el mensaje genera alguna duda, lo mejor es consultar directamente con el remitente antes de hacer clic en algo que se considera sospechoso.
- Mantener el navegador actualizado. Esta práctica realmente es muy sencilla de incorporar a los hábitos digitales ya que únicamente se debe garantizar y permitir que los navegadores se actualicen cada vez que el fabricante publica una nueva versión. Las empresas desarrolladoras publican con regularidad actualizaciones o parches para corregir las

vulnerabilidades de seguridad que se han encontrado en su software. Actualizar siempre el navegador, el sistema operativo y demás aplicaciones cuando sea solicitado es fundamental para robustecer la seguridad de todo el sistema y, como medida adicional, habilitar las actualizaciones automáticas cuando sea posible.

- Verificar que la página web sea segura. Este aspecto siempre debe ser tenido en cuenta, sobre todo antes de realizar el ingreso de información confidencial (esto incluye nombres de usuario y contraseñas). La forma más sencilla de hacer esta verificación es confirmar que la URL de la página web comienza con HTTPS y que hay un icono de candado en la barra de direcciones. En algunos casos los sitios web también muestran sellos de confianza para indicar que el sitio es seguro. Si el navegador o el antivirus identifica un sitio web de *phishing*, este alertará de manera inmediata y procederá a bloquear el acceso al sitio. No se deben ignorar estas advertencias, a menos que se tenga seguridad de que se trata de un falso positivo.
- Una buena práctica es instalar una extensión *anti-phishing* en el navegador. Algunos navegadores traen incorporada una protección contra *phishing* bastante robusta, pero se puede llevar la seguridad a un nivel más alto realizando la instalación de una extensión de navegador *anti-phishing* dedicada. Recientemente, Microsoft lanzó Windows Defender Browser Protection, pero actualmente sólo es compatible con Google Chrome.
- Conocer el lenguaje que se utiliza en una suplantación de identidad. Los ataques de suplantación de identidad se caracterizan por parecer muy convincentes. Para identificar un correo electrónico o un mensaje instantáneo sospechoso lo mejor es familiarizarse con el lenguaje que se utiliza en ataques de *phishing*. Esto puede incluir errores gramaticales, tipográficos y frases que no encajan, puesto que suenan poco profesionales o fuera de contexto, palabras o situaciones que crean un sentido de urgencia. También puede ser sospechoso si se solicita verificar la cuenta, ya sea bancaria o de correo, teléfono, dirección, datos banca-

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

rios y cualquier otra información confidencial; o si incluye saludos en los que se dirigen a la persona usuaria como "Cliente", cuando se supone que la entidad tiene los datos y, por lo tanto, debería usar el nombre y apellido real.

- Es recomendable digitar las URL y utilizar marcadores para evitar hacer clic en enlaces, puesto que cuando esto se hace en enlaces que vienen en correos electrónicos puede existir un alto riesgo para los usuarios. En su lugar, basta con abrir el navegador y escribir de forma manual la URL de la entidad o empresa de la que se recibió el correo electrónico. Por otra parte, es aconsejable marcar los sitios web que se utilizan con frecuencia y abrirlos rápidamente desde el navegador cuando sea necesario; pero antes debe asegurarse que los sitios efectivamente son legítimos.
- El *phishing* no afecta únicamente a la banca en línea. Normalmente se tiende a asociar con este tipo de banca, pero es importante mencionar que los ataques del tipo *phishing* se utilizan también para suplantar o hacerse pasar por una organización o individuo, y los efectos pueden ser igual de devastadores que un fraude bancario, puesto que el atacante apunta a obtener beneficio económico. Por ejemplo, perder las credenciales de acceso del correo electrónico o de las cuentas en redes sociales puede traer consecuencias graves y con alcance en la vida personal y profesional. Cuando se produce el robo de las credenciales de inicio de sesión de un sitio o servicio, también puede afectar otras cuentas si se usan las mismas contraseñas para otros servicios en línea.
- Prestar atención a las ventanas emergentes. Afortunadamente, esto se ha venido controlando desde los navegadores, pero aún se utilizan en algunos sitios web. Se recomienda tener cuidado al ingresar datos o información, puesto que ha habido casos de ataques relacionados con el *phishing* en ventanas que se hacen pasar como una parte legítima del sitio web principal. Firefox, Google Chrome y Microsoft Edge cuentan con configuraciones integradas que contribuyen a bloquear las ventanas emergentes.
- No solamente es el correo electrónico. Hay que tener presente que existen otros vectores de ataque, la forma más

utilizada para el envío de ataques de phishing es el correo electrónico, pero eso no quiere decir que otros canales de comunicación sean más seguros. Existen ataques en las redes sociales, los cuales se han popularizado en los últimos años, y los investigadores en seguridad informática incluso han detectado aplicaciones de *phishing* maliciosas publicadas en Google Play. De tal forma que se resalta la importancia de poner atención al momento de transmitir datos en cualquier dispositivo que se conecte a Internet, sin importar la aplicación que se esté utilizando o el medio de comunicación.

Suplantación

La suplantación de identidad en línea no es lo mismo que tener la cuenta de redes sociales comprometida; hace referencia a que una persona malintencionada configure una cuenta completamente diferente, pero muy similar a un nombre y con una foto de perfil existente. Cuando esto sucede alguien está tratando de engañar a los contactos en las redes sociales para que hagan algo que beneficie al atacante (comúnmente, transferir dinero), o se quiere dañar la reputación de la víctima.

- Revisar la lista de amigos o contactos. Asegurar que se está en contacto a través de las redes sociales solo con personas que realmente se conocen o con las que se tiene una relación de amistad, o en las que al menos se puede confiar, puede contribuir a detectar perfiles sospechosos. Los estafadores a menudo envían solicitudes de amistad a las personas para obtener detalles sobre sus vidas, que luego pueden utilizar maliciosamente en su contra.
- En el caso de encontrar cuentas que estén suplantando una identidad se debe denunciar la cuenta. En el caso de ser una suplantación del propio perfil, se debe publicar inmediatamente en las redes sociales comprometidas varias advertencias con el fin de alertar a los contactos de que alguien está suplantando la identidad y que se proceda a bloquear esa cuenta de inmediato.
- No contactar al suplantador. Esto es una pérdida de tiempo, puesto que ponerse en contacto con el impostor y acusarlo

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

o pedirle que detenga su actividad genera que este trate de engañar a los contactos de manera más rápida. Al contactar al estafador puede suceder que trate de engañar o solicitar dinero para dejar de suplantar o que incremente las actividades fraudulentas en el perfil falso con el fin de obtener beneficio antes de que le bloqueen la cuenta.

Vishing

El *phishing* de voz, mejor conocido como *vishing*, se produce cuando un delincuente intenta obtener información a través de una llamada telefónica. De hecho, las estafas más elaboradas utilizan una combinación de fraude por correo electrónico y voz para parecer más legítimas y engañar de forma más sencilla a la víctima. A partir de lo anteriormente mencionado es fundamental identificar este tipo de llamadas y tener en cuenta algunas recomendaciones para evitar ser víctima de este ataque.

- Bloquear las llamadas automáticas. Este tipo de llamadas se realizan de manera automatizada, normalmente mediante un mensaje grabado. Los estafadores también utilizan marcadores automáticos para realizar una gran cantidad de llamadas en cuestión de pocos minutos, por lo que tienen más posibilidades de comunicarse con una persona real. Contra esto se pueden bloquear de forma manual los números maliciosos desde un teléfono inteligente. Para realizar este procedimiento se debe consultar el manual del teléfono o consultar al operador de telefonía para obtener instrucciones específicas.
- No responder a números desconocidos. Bloquear números de teléfono no detendrá los intentos de *vishing*, porque los estafadores usan software para codificar su número de teléfono real. Por ejemplo, los estafadores suelen imitar el código de área y los primeros tres dígitos de su número de teléfono para engañar a las víctimas y hacerles creer que es una llamada local. Si se bloquea un número, los estafadores simplemente llamarán desde otro. Si la víctima contesta el teléfono y luego cuelga inmediatamente, el estafador sabrá que la línea está activa. Sin embargo, si no levanta el teléfono, los estafadores eventualmente considerarán que el nú-

mero está inactivo. Es recomendable no responder llamadas desconocidas. Como resultado, la frecuencia con la que se reciben las llamadas automáticas comienza a disminuir.

- Si una persona recibe una llamada informándole de actividad inusual en una de sus cuentas, es recomendable sospechar de la información que se está recibiendo. La persona al otro lado de la línea puede incluso tener parte de la información personal, pero eso no significa que sea una autoridad real. Se recomienda no negar ni confirmar la información que proporciónense proporcione, y no aportar ninguna información propia. Lo mejor que se puede hacer en estos casos es colgar el teléfono y llamar directamente a la organización que afirman representar. confíese aconseja desconfiar de la información de contacto proporcionada por la persona que llamó. Si es un estafador, esta información simplemente conducirá a canales no oficiales.

Smishing

En caso de recibir un mensaje de texto de un número desconocido que promete librar de las deudas hipotecarias hay que empezar a desconfiar. A continuación, se enumeran algunas prácticas útiles para evitar estos ataques. En primera instancia, se deben buscar los mismos signos que se buscarían en un correo electrónico que fuera un intento de *phishing*, luego se debe:

- Verificar si hay errores ortográficos y gramaticales.
- Visitar el sitio web del remitente en lugar de proporcionar información en el mensaje.
- Verificar la información del remitente y dirección de teléfono para asegurarse de que coincida con la de la empresa a la que pretende representar.
- No proporcionar información financiera o de pagos sobre nada que no sea el sitio web de confianza.
- No hacer clic en enlaces de remitentes desconocidos o en aquellos que generen desconfianza.
- Tener cuidado con "responder rápido", "registrarse ahora" u otras ofertas agresivas y demasiado buenas para ser verdad.

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 120-150 (Artículo).

- Escribir siempre direcciones web en un navegador en lugar de hacer clic en el enlace e instalar un antivirus compatible con dispositivos móviles en los dispositivos inteligentes.

Carta nigeriana

Este tipo de estafa es muy antiguo y en los tiempos modernos los estafadores utilizan la tecnología para tratar de engañar a más personas, por esta razón hacen uso de correo electrónico. Esto funciona de manera similar al *phishing* y combina elementos de la estafa y la suplantación, por lo tanto, las mismas recomendaciones expresadas anteriormente son efectivas con este tipo de ataque.

Conclusiones

Los ataques de ingeniería social han evolucionado de tal forma que cada vez es mucho más complicado para los usuarios identificar este tipo de amenazas. Desde los inicios de internet se han conocido casos de ataques de este tipo y, a pesar de esto, aún los delincuentes hacen uso de las mismas técnicas, pero incorporando nuevas tecnologías para engañar a las personas. El ciber crimen en Colombia ha tenido un crecimiento exponencial durante los últimos años de forma paralela al uso de las nuevas tecnologías y acceso a dispositivos móviles. Las pérdidas económicas generadas por los ciberataques asociados a la ingeniería social sitúan esta problemática como una de las principales actividades ilegales en el país.

Para los atacantes, la ingeniería social se ha convertido en su primera opción al momento de ejecutar un ataque, puesto que gracias a los diferentes métodos y técnicas se logra obtener mayor efectividad. Como se logra identificar, es una problemática real y es prioritario tomar medidas al respecto. La cantidad de delitos informáticos que son denunciados en Colombia son bastantes, como fue posible evidenciar, pero el escenario que más preocupa es el aumento desde el año 2016 y el hecho de que no todas las víctimas denuncian la ocurrencia de este tipo de eventos.

Al aprovechar las debilidades humanas naturales, las estafas del tipo *phishing* son comunes y eficaces, ya que su porcentaje de éxito radica en que el atacante envía miles de correos y, al lograr afectar un pequeño grupo de estos, puede obtener el beneficio económico.

Es importante contar con un software antivirus, toda vez que cumple un rol importante en la prevención de ataques de *phishing*, pero el usuario debe asegurarse de que su antivirus realmente combate el *phishing* y los riesgos de seguridad y privacidad que esto implica.

Toda organización cuenta con el factor humano. El ser humano por naturaleza es curioso, propenso a tomar decisiones de manera rápida y, con frecuencia, está guiado por las emociones. Por esta razón, es fundamental que se desarrolle un conjunto de herramientas de ingeniería social para contribuir a reforzar la seguridad contra los ataques de este tipo que normalmente aprovechan las vulnerabilidades humanas.

Referencias Bibliográficas

AcensTechnologies. (2014). Qué es el phishing y cómo protegerse [Archivo PDF]. https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

Alexander, M. (2016). *Methods for Understanding and Reducing Social Engineering Attacks*. Sans. https://www.sans.org/white-papers/36972/

Asobancaria. (2022). *CSIRT Financiero – Equipo de apoyo para la respuesta a incidentes de Ciberseguridad para el sector financiero colombiano.* https://csirtasobancaria.com

Berenguer Serrato, D. (2018). *Estudio de metodologías de Ingeniería Social.* [Trabajo Final de Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones] https://openaccess.uoc.edu/handle/10609/81273

Cámara Colombiana de Informática y Telecomunicaciones. (2019). *Tendencias cibercrimen Colombia 2019-2020*. https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Castillo, C. (2018). *'Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas?* BBVA. https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

CERT-UK. (2015). *An introduction to social engineering*. Public Intelligence. https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf

colCERT. (2017). Grupo de Respuesta a Emergencias Cibernéticas de Colombia. https://www.colcert.gov.co/?q=acerca-de#:~:-text=Nuestra%20Misi%C3%B3n,del%20Ministerio%20de%20Defensa%20Nacional.

CSIRT Financiero. (2019). Equipo de apoyo para la respuesta a incidentes de Ciberseguridad para el sector financiero colombiano. https://csirtasobancaria.com/quienes-somos

CSIRT-PONAL. (2018). Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional. https://cc-csirt.policia.gov.co/quienes-somos

Dinca, C. (2016). *Fraudes en Internet* [Trabajo Final de Grado, Universitat Jaume I]. http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequenc e=1

Douglas, T. (2003). *Hacker Culture*. University of Minnesota Press.

Europol. (2019). *Fraude del CEO* [Archivo PDF]. https://www.europol.europa.eu/sites/default/files/documents/colombia_1.pdf

Fernández, M. (2018). *Ingeniería Social: ¿qué es el Baiting* («cebar», o «poner carnada»)? Mailfence. https://blog.mailfence.com/es/que-es-baiting-ingenieria-social/

Fiscalía General de la Nación. (2022). *Sistema Nacional de Denuncia Virtual ¡ADenunciar!* https://adenunciar.policia.gov.co/Adenunciar/Login.aspx

Goga, O., Venkatadr, G., & Gummadi, K. (2016). *Exposing Impersonation Attacks in Online Social Networks* [Archivo PDF]. https://lig-membres.imag.fr/gogao/papers/impers_cosn14.pdf

López, C. y Salvador, R. (2015). *Ingeniería Social: El Ataque Silencioso* [Archivo PDF]. http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

Martínez, C. (2018). *Seguridad por capas frenar ataques de Smishing* [Archivo PDF]. https://dialnet.unirioja.es/descarga/articulo/6255067.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016). *Guía para la implementación de seguridad de la información en una MIPYME* [Archivo PDF]. https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Mitnik, K. (2001). *The Art of Deception*. Indianapolis: WILEY Publishing. ISBN 0- 471-23712-4

Nohlberg, M. (2018). *Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks* [Tesis doctoral. University of Skövde].

Oxman, N. (2016). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming" [Archivo PDF]. https://scielo.conicyt.cl/pdf/rdpucv/n41/a07.pdf

Policía Municipal Madrid. (2019). *Ingeniería social: ¿Se puede hackear a una persona?*[Archivo PDF]. https://cppm.es/wp-content/uploads/2019/03/ingenieria-social-se-puede-hackear-a-una-persona-abr2019.pdf

Policía Nacional de Colombia. (2017). *Informe Amenazas del Cibercrimen en Colombia 2016 - 2017*. https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017

Policía Nacional de Colombia. (2017). *Balance cibercrimen en Colombia 2017* [Archivo PDF]. https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

Policía Nacional de Colombia. (2018). *CAI Virtual*. https://caivirtual.policia.gov.co/contenido/cai-virtual

Policía Nacional de Colombia. (2022). *CAI Virtual*. https://caivirtual.policia.gov.co/

Policía Nacional de Colombia. (2022). *CSIRT-PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional*. https://cc-csirt.policia.gov.co

Sánchez, G. (2012). *Delitos en Internet: Clases de fraudes y estafas y las medidas para prevenirlos* [Archivo PDF]. https://dialnet.unirioja.es/descarga/articulo/4198948.pdf

TicTac. (2021). *Tendencias del cibercrimen 2021-2022* [Archivo PDF]. https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

Valverde, E. (2012). *Seguridad en Sistemas de Información. Un recorrido a vista de pájaro* [Archivo PDF]. https://ruidera.uclm.es/xmlui/bitstream/handle/10578/2302/Seguridad%20en%20Si-stemas%20de%20Informaci%C3%B3n%20ESI%202012-0.4.pdf?sequence=1&isAllowed=y

Wright, G. (2019). *Watering hole attack*. Tech Target. https://www.techtarget.com/searchsecurity/definition/watering-hole-attack