Crowe

Ataques de ingeniería social:

Efectos en las compañías y personas naturales

Audit / Tax / Advisory

www.crowe.com.co

Antes de ahondar en los conceptos técnicos acerca del nacimiento de los ataques de ingeniería social, cómo nos están afectando y la forma en la que gracias al avance en conectividad al internet y el uso de dispositivos han tenido un efecto de crecimiento de manera proporcional frente a estos ataques, es importante conocer las cifras en los últimos años que han marcado un antes y después frente a los ciberataques de los que todos están expuestos.

Según el cisoverso, una comunidad privada de profesionales de ciberseguridad, se calcula que en la actualidad hay al menos 45 mil millones de usuarios en las diferentes redes sociales, y de estas, por lo menos una de cada cinco cuentas sería ciber atacada en las próximas 24 horas, así mismo, estudios confirman que al menos el 80% de los códigos maliciosos están desarrollados con el fin de obtener información bancaria.

Por otra parte, a inicio de la pandemia de covid-19, en el 2020 los ataques informáticos se vieron incrementados un 400%, según informó la FBI, los números más elevados y preocupantes, teniendo en cuenta que los medios digitales a partir de esa fecha serían las herramientas más utilizadas, tanto por personas del común y compañías en el mundo.

Así mismo, en un estudio publicado por Fortinet y Crowdstrike, para el 2021 se presentaron alrededor de 41 billones de ciberataques en el mundo, de los cuales 7 billones corresponden a Colombia, posicionándolo como el cuarto país más ciber atacado a nivel mundial.

Los datos presentados anteriormente son solo uno de los tantos reflejos que la pandemia dejó en el mundo de la mano con el rápido avance tecnológico, pues la accesibilidad al internet, la importancia de los datos personales y la necesidad de estar conectados y tener un dispositivo inteligente como un celular, tablet o computadoras, también ha crecido de la mano con los riesgos cibernéticos y de otras índoles que, nos deja ver cómo cada día es más alta la exposición que hay frente a la inseguridad tecnológica.

Pues según informe de cifras realizado en un estudio por We Are Social y Hootsuite, señalan que para enero del 2022 el número de usuarios de internet en el mundo alcanzó los 4,950 millones de personas, lo que representa al 62,5% de la población mundial (7.910 millones de personas).

Enero 2022 · Usuarios de internet en el mundo

Población total	Usuario único de teléfono móvil	Usuarios de internet	Usuarios activos en redes sociales
7.91 Billones	**5.31** Billones	**4.95** Billones	**4.62** Billones
Urbanización	Vs Población	Vs Población	Vs Población
57.0%	**67.1%**	**62.5%**	**58.4%**

Tomada de: We are social

Ataques de Ingeniería Social

Según una de las compañías internacionales dedica a la seguridad de la informática, Kaspersky lab, la ingeniería social se define como “La práctica ilegitima de obtener información confidencial través de la manipulación de usuarios legítimos”, pues resulta ser una técnica de diferentes formas en la que los cibercriminales se acercan a interactuar con los usuarios con el fin de obtener información confidencial sin ser percibido por la persona u empresa que está siendo atacada.

Es importante tener en cuenta que, los ataques de ingeniería social no solo afectan los ámbitos corporativos o laborales, sino también a los usuarios habituales en el mundo digital, quienes día a día aumentan su conectividad, pues realmente su enfoque es obtener información de cualquier persona que pueda resultarle útil para su objetivo.

“Cuando las personas deben enfrentar situaciones aterradoras, la primera reacción es actuar y, luego, pensar. La ingeniería social se basa en esta vulnerabilidad para que los ataques sean exitosos”.

Así mismo, existen varios tipos de ciber crímenes, y también existen varios tipos de clasificaciones de ataques de ingeniería social, teniendo en cuenta que de manera general los atacantes hacen uso de algunos patrones específicos para establecer una relación de confianza con la víctima, ya sea mediante promesas dudosas, ofrecimientos irrisorios, ventas agresivas, amenazas, necesidad por urgencia, suplantación de familiares, contactos conocidos o entidades de confianza.

Esto, se ve reforzado por lo indicado por el Dr. Robert Cialdini, en su libro publicado en 1984 “Influence: the psychology of persuation”, donde establece seis principios de la influencia y la persuasión:

1. **Reciprocidad:** Las personas tratan a los demás según como perciben que son tratados.

2. **Coherencia y compromiso:** Los humanos tendemos a ser coherentes con nuestras conductas previas, Es decir, somos propensos a realizar acciones que ya hayamos hecho antes y nos haya hecho sentir bien.

3. **Aprobación social:** Mecanismo psicológico por el que tendemos a dejarnos llevar por el comportamiento social mayoritario y opinión pública (Presión social).

4. **Autoridad:** Las figuras con más autoridad o que son lideres gozan de mayor credibilidad.

5. **Simpatía:** Es simple estamos predispuestos a hacer cosas que nos pida alguien agradable y simpático.

6. **Escasez:** Cuando sabemos que algo está a punto de agotarse lo valoramos y lo deseamos mucho más.

Es así, como podemos ver que la ingería social requiere tener conocimientos en habilidades sociales y comunicativas superiores o muy bien desarrolladas.

¿Cómo se encasillan los ataques de ingeniería social?

Para algunos autores o especialistas se agrupan en dos términos:

1. **Los masivos:** El grupo que intenta afectar al mayor número de usuarios con un único contacto o acción.

2. **El investigador:** El segundo grupo que realiza y recolecta más información de la víctima para poder personalizar el ataque y lograr una mayor probabilidad de tener éxito en su objetivo.

Realmente existen muchos tipos de clasificaciones para agrupar unas características y patrones de ataques que todos deberían conocer, entre los que encontraríamos:

- ✔ **Spam:** Envíos masivos de correos electrónicos o mensajes de texto que contienen cualquier tema no específico, generalmente acompañado de un enlace o archivo infectado con el objetivo de que algún usuario caiga en la trampa de abrirlo.

- **Phishing:** A diferencia del SPAM, estos correos electrónicos parecen ser legítimos y simulan provenir de fuentes fiables diseñados específicamente para engañar a las víctimas y que brinden su información personal o confidencial.

- **Baiting:** Un ataque de ingeniería social no muy conocido que se aprovecha de la curiosidad de la persona, en la forma de dejar señuelos. Por ejemplo, dejar abandonado un dispositivo USB en algún lugar fácil de encontrar como en un edificio de oficinas, con el objetivo de que la persona que lo encuentre ingrese este elemento al equipo y lo pueda infectar con algún tipo de virus informático (Malware).

- **Vishing:** Es una de las variantes de ingeniería social más recientes y se basa en la suplantación de números de teléfono para que parezcan venir de algún conocido cercano, como compañeros de trabajo, familia o de alguna entidad bancaria o servicios de telefonía, esto, con el objetivo de lograr que las personas den su información o accedan a cualquier acción no deseada.

- **Smishing (SMS + Phishing):** Es una combinación entre spam y phishing, con la diferencia que se distribuye a través de mensajes de texto que parecen venir de fuentes fiables como entidades financieras, que contienen enlaces con Malware para infectar el dispositivo móvil, o para solicitar información personal.

- ✔ **Qui Pro Quo:** Este tipo de estafa es en la que se busca a las personas para informales de algún beneficio ganado, como premios costosos o grandes descuentos, a cambio de información personal o laboral.

- ✔ **Pretexting:** Es el tipo de engaño más común en las cibercriminales, pues a través de una historia trágica o intimidadora se acercan a las personas con un grado de urgencia alto con el objetivo no dejar reaccionar a la víctima y entregue toda la información o dinero que ellos necesitan.

- ✔ **Farming:** Es el tipo de ingeniería social más clásico en la cual el atacante se acerca a las personas con el objetivo de establecer alguna relación o simplemente observar, escuchar e investigar sus espacios sociales y conocer sus perfiles de redes sociales, intentando recopilar toda la información hasta conseguir su objetivo, ya sea para perfilar un ciberataque a una persona o a una organización.

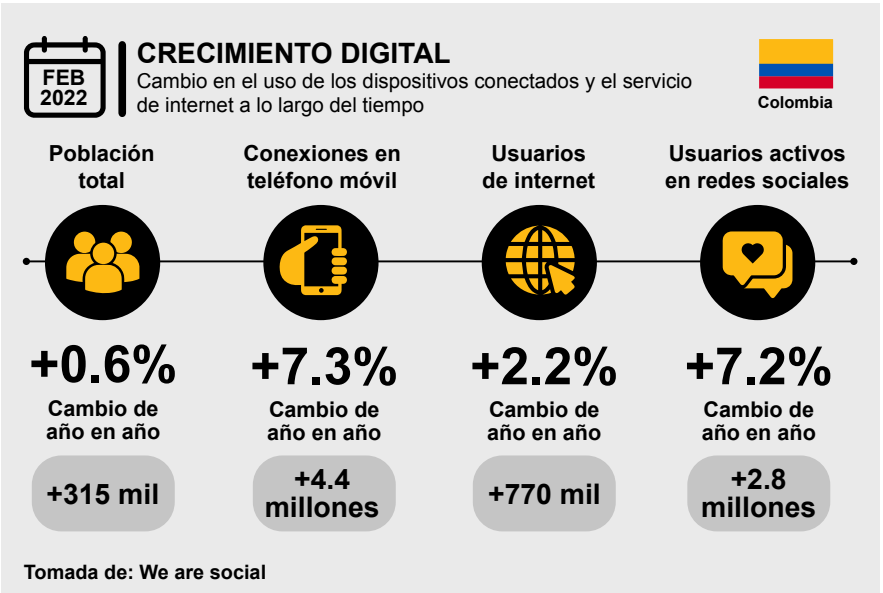
Por último, es importante resaltar el termino BEC (Bussiness Email Compromise) y un nuevo término: EAC (Email Account Comprimise), que son ataques focalizados en recolectar la información de las compañías y poder ejecutar ataques más efectivos que afecten a entidades privadas o gubernamentales.

Ciberataque en Colombia

Las personas naturales o “el usuario final” resultan ser el eslabón más débil en la Ciberseguridad y esto, tiene relación con la Ingeniería Social, pues las personas resultan ser más susceptibles a manipulación o engaños, lo que se ve reflejado en un estudio realizado por el Centro Cibernético de la Policía Judicial Colombiana (Dijin), donde confirman que para el año 2021 en Colombia se presentaron a nivel nacional **71.727 denuncias** por estafas, a través de llamadas telefónicas o por mensajes de texto, de los cuales el 25% corresponden a Bogotá con un total de 18.649 denuncias y esto a su vez, representa un aumento del 31% en comparación con el 2020 donde se recibieron 14.243 denuncias por estafa.

Lo que demuestra lo susceptible que las personas naturales pueden llegar a ser, abierto a una gran posibilidad de ser víctimas de un robo desde cualquier parte del mundo, pues ya no se habla de que se esté expuesto a los peligros habituales que cada país tiene en las calles, sino que, hay un riesgo aún mayor en el ciberespacio, donde en promedio, los colombianos pasan 3 horas y 46 minutos al día conectados a las redes sociales, dividiendo su tiempo en 8 redes distintas, pues según estudios que realizan anualmente We are Social en conjunto con diversas empresas de investigación e inteligencia de mercado, publicaron el

Digital 2022 Global Overview Report, donde se menciona que en el país en el año 2014 al 2022, la cantidad de usuarios ha crecido 109%.



La necesidad de tener que estar conectados en todo momento, de inscribir y compartir nuestros datos personales en diferentes portales o medios de información e incluso aumentar nuestras interacciones por las diferentes redes sociales, expuso aún más a los usuarios y fue aprovechado por los inescrupulosos o más conocidos como “hackers” para intentar obtener esta información.

Según un estudio de National Services Security Index realizado en octubre del 2022, Colombia ocupa el puesto 63 dentro de 160 países en el nivel de seguridad que tiene para los ciberataques. Pues a principios de año salió el decreto de seguridad digital 338 del 2022, por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital.

Adicional, frente a la situación del mundo ante los ciberataques, las compañías en el país han sido más consientes frente a sus estrategias para disminuir la probabilidad de ser ciberatacados, pues a pesar de los lineamientos y personal capacitado con los que pueda contar, las entidades deben tener un trabajo continuo para mejorar sus niveles de seguridad.

Es así, como la alta demanda de ingenieros ha aumentado por parte de las empresas que buscan mejorar sus estrategias de seguridad, siendo un punto importante y casi convirtiéndose en un trabajo esencial para las compañías que velan por su información personal en Colombia.

En conclusión, en el país y en el mundo no se está exento de poder sufrir de algún tipo de ciberataque, pues según las cifras mencionadas en este artículo se muestra la necesidad de estar alertas frente a cualquier situación sospechosa, pues resulta haber una alta necesidad de ser cuidadosos con la información personal que se registra a través de cualquier plataforma digital.

¡Contáctenos!

Sede Central Internacional

Crowe Global - New York City
515 Madison Avenue
8th Floor, Suites 9006--9008
New York, NY-10022
United States of America
MAIN +1.212.808.2000
Contactus@Crowe.org

Colombia

Bogotá D.C.

Carrera 16 # 93-92
Edificio Crowe
PBX +57.1. 605.9000
Contacto@Crowe.com.co

Barranquilla

Calle 77B # 57-103 Oficina 608
Edificio Green Towers
PBX +57.5.385.1888
Barranquilla@Crowe.com.co

Cali

Carrera 100 # 5-169 Oficina 706
Unicentro – Centro de Negocios
PBX +57.2.374.7226
Cali@Crowe.com.co

Manizales

Carrera 23 C # 62-06, Oficina 705
Edificio Forum Business Center
PBX +57.6.886.1853
Manizales@Crowe.com.co

Medellín

Avenida Las Palmas # 15 B 143 - Piso 5
Edificio 35 Palms Business Tower
PBX +57.4.479.6606
Medellin@Crowe.com.co

Smart decisions. Lasting value.

Jaime Mendieta
Gerente de transformación digital y TIC's
Jaime.mendieta@crowe.com.co

Contáctanos