México, Ciudad de México

Básicos de seguridad para un usuario común

Juan Daniel López Gómez
Gerencia de Infraestructura

RESUMEN

Mientras se navega por internet o se hacen operaciones en la web, un usuario se encuentra expuesto a un sinfín de amenazas que no sólo pueden poner en riesgo la integridad de su computadora o teléfono inteligente, sino además puede ser víctima del robo o secuestro de su información sensible tal como números y claves de tarjetas de crédito, direcciones de casa y/o trabajo, contactos importante etc.

La finalidad de este documento es exponer las técnicas y formas que tienen los ladrones de información para aprovecharse de usuarios poco cuidadosos, así como explicar qué hacer para reconocer posibles casos de fraude electrónico.

PALABRAS CLAVE:

Ciberseguridad, seguridad, fraude, electrónico, hackers, ladrones.

INTRODUCCIÓN

Actualmente las actividades de una persona involucran a las tecnologías de la información, básicamente está en interacción con una computadora, un teléfono, correo electrónico, redes sociales y operaciones bancarias.

En todas y cada una de dichas actividades el usuario debe ser cuidadoso ante las amenazas presentes en la red. Navegar sin un poco de conciencia o sentido común puede significar en perder más que una computadora puede terminar en robo; un mal momento para la persona en cuestión.

DESARROLLO

¿Qué es un hacker?

Posiblemente, al escuchar dicha palabra llegan recuerdos de películas de las cuales un hacker era visto como una persona misteriosa encerrada en su lugar secreto rodeado de computadoras y que siempre se la pasaba tecleando códigos no entendibles para una persona promedio, el objetivo de los códigos

era variado, pero no es más que ficción. En la vida real un hacker se define como:

"Concretamente es una persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo." (Muñoz de Frutos, 2015)

Con base en lo dicho, un hacker es una persona que desafía la seguridad y la integridad de un sistema, además de que hay una variante que se aprovecha de las vulnerabilidades sociales y personales de un individuo para sacar partida y beneficiarse a sí mismo.

Sin embargo, dentro del mundo misterioso de los hackers se encuentra una clasificación muy importante ya que de ella se pueden conocer sus intenciones, así como la forma en la que trabajan.

1.1 Tipos de hackers

Como una clasificación a grandes rasgos, se encuentran dos tipos de hackers; los de sombrero negro y los de sombrero blanco. Los primeros son aquellos cuyas acciones se centran en romper un sistema y obtener información valiosa para ser vendida al mejor postor o que toman "secuestrada" para que el o los dueños de la información paguen el rescate o liberación de sus datos (crackers y ransomware); por otra parte, también se aprovechan del perfil social de una persona, así como van analizando su comportamiento y actividades para hacer actos de extorsión y amenazas (ingeniería social). Se identifican por el símbolo del sombrero negro, como puede verse en la ilustración 1.

Por el otro lado se encuentran los hackers de sombrero blanco que son aquellos cuyas actividades se centran en encontrar las debilidades o "puertas traseras" de un sistema que pueden ser aprovechadas con mal intención por los hackers del grupo opuesto. Al encontrar áreas vulnerables es entonces que informan al dueño o creador del sistema de las debilidades encontradas, y así puedan corregir dichos fallos de seguridad, por ejemplo, algunas empresas reconocidas como Google, Amazon o Microsoft retan a una serie de personas a encontrar vulnerabilidades o fallas en sus sistemas; la recompensa suele ser bastante jugosa.

"Muchos otros buscadores de fallos han utilizado su habilidad para sacar

partido de la oportunidad. Esto se debe a que las empresas de software no son las únicas que pagan para enterarse de estos errores. Los ciber ladrones también ofrecen dinero por conocer vulnerabilidades que pueden explotar con virus y otros programas maliciosos." (Ward, 2014)

Ilustración 1. Ícono con el que se puede reconocer a los hackers de sombrero negro.

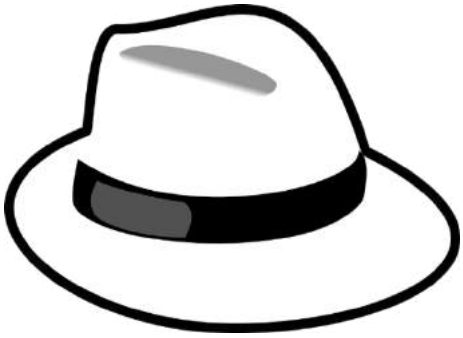

Ilustración 2. Ícono que hace alusión al grupo de hackers de sombrero blanco.

Una vez conocidos los dos tipos de hackers, es momento de conocer algunas de las prácticas a las que suelen recurrir para obtener información de manera ilegal o para encontrar vulnerabilidades en los sistemas. Se identifican por el contrario de los primeros con el color blanco; véase la ilustración 2.

2. Técnicas de hacking

Cuando no se está acostumbrado al lenguaje técnico, las palabras que conforman esta sección no son familiares para la mayoría de las personas. A continuación, se enlistan las técnicas a las cuales se les echa mano para robar información o detectar fallas de un sistema.

2.1 Técnicas más conocidas de los hackers

- *Phishing*. Esta técnica se basa en suplantar o hacer pasar la identidad de una persona u organización reconocida a través de correo electrónico con la finalidad de que el destinatario comparta su información personal tal como contraseñas, datos de tarjetas de crédito, etc. Los autores de este tipo de ataques han perfeccionado sus técnicas ya que muchas veces, sus correos parecen de la persona y

organización real. Está práctica ha ido en incremento como se observó en el último trimestre del 2019. (Galván, 2020)

- *Vishing.* Es una variante de la técnica anterior, que no se basa en texto, sino que se basa en hacerse pasar por alguien más a través de la voz. Parafraseando a (BBVA, 2015) el vishing se define como la práctica en la cual, aprovechando la tecnología de voz sobre IP (VoIP) el atacante se hace pasar por un banco, una operadora de una empresa o proveedor con la finalidad de que el sujeto al que se ataca dé información sensible o privada sobre su vida personal o laboral.

- Ingeniería social. Esta es una actividad que se basa en investigar a una persona basándose en su estilo de vida o rutina que publica en sus redes sociales tales como Facebook, Twitter o Instagram.

  El atacante recopila la información para realizar acciones ilegales tales como secuestro o extorsión. Otro ejemplo es el que se explica en (Kaspersky, s.f.)*: "[…] un hacker puede frecuentar el comedor público de un gran edificio de oficinas, buscar usuarios que estén trabajando en sus tablets o computadoras portátiles y mirar los dispositivos por encima de su hombro. Con esta táctica pueden conseguir una gran cantidad de contraseñas y nombres de usuario, todo sin necesidad de ni enviar un solo correo electrónico de ni escribir una línea de código de virus. Otros ataques requieren una comunicación real entre el atacante y la víctima; en estos casos, el atacante presiona al usuario para que le otorgue acceso a la red con el pretexto de un problema grave que es necesario resolver de inmediato."*

- Inyección de código SQL. SQL por sus siglas en inglés Lenguaje Estructurado de Consulta, es uno de los lenguajes para bases de datos más usados en todas las empresas alrededor del mundo. Una inyección de código consiste en usar ciertos caracteres en campos de un sistema que reciben texto y que

al enviarlos interactúan con la base de datos y que al encontrar un error muestran mensajes cuyo contenido pueden dar indicio al atacante de que el sistema está mal programado, algunos de los caracteres especiales con los que se debe tener cuidado mientras se programa una interfaz son: el asterisco (*), el guion (-) y las comillas simples (‘). Esta técnica es usada por ambos tipos de hackers.

3. ¿Cómo evitar ser víctima o qué hacer en caso de sido víctima?

- En el caso del phishing y vishing, es recomendable verificar la autenticidad del contenido con la persona o entidad quien se supone está requiriendo la información. En el caso de las entidades bancarias, éstas hacen hincapié en que nunca se deben compartir los datos personales por correo ni por llamada telefónica ya que nunca harían eso.

- No introducir los datos personales o bancarios en páginas cuya autenticidad sea dudosa o que se hagan pasar por las originales, nuevamente se recomienda consultar a la organización/empresa si dicha página es auténtica o no.

- No usar redes públicas para realizar transferencias o para compartir información sensible, ya que estas redes carecen de protección de los paquetes que son enviados.

- Mantener un bajo perfil en cuanto a publicaciones en redes sociales se refiere, ya que los ataques basados en ingeniería social suelen ser más difíciles de detectar. Esto aplica también para el perfil laboral de las personas, se recomienda no publicar o hablar acerca de las funciones que se llevan a cabo en el trabajo.

- Para evitar la inyección de código SQL, es necesario tener buenas prácticas en la programación de los sistemas e interfaces. Un ejemplo está en utilizar funciones -dependiendo el lenguaje de programación- que conviertan los caracteres especiales en simple texto para que tanto el programa como el gestor de la base de datos interpreten los caracteres como

si fueran parte de una orden programada.

- El consejo básico fundamental es usar un antivirus confiable al mismo tiempo que se instalen las actualizaciones del sistema operativo con el que se trabaje para que se reduzca la probabilidad de un ataque.

CONCLUSIÓN

Resulta abrumadora la cantidad de formas en las que un atacante puede robar la información de una persona, sin embargo, basta con el sentido común, así como seguir las recomendaciones expuestas para vivir una experiencia positiva en internet y durante las actividades diarias.

Por otra parte, hay que estar siempre informados acerca de las nuevas amenazas que se presentan en el mundo informático ya que de no hacerlo y por más precauciones que se tomen existe la posibilidad de ser víctimas de un ataque nunca visto.

REFERENCIAS

BBVA. (26 de Noviembre de 2015). *¿Qué es el vishing?* Obtenido de BBVA: https://www.bbva.com/es/vishing-la-imaginacion-los-estafadores-no-limites/

Galván, M. (19 de Febrero de 2020). *Phishing financiero aumentó en último trimestre del 2019*. Obtenido de El economista: https://www.eleconomista.com.mx/finanzaspersonales/Phishing-financiero-aumento-en-ultimo-trimestre-del-2019-20200219-0090.html

Kaspersky. (s.f.). *Ingeniería social: definición*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Muñoz de Frutos, A. (31 de Octubre de 2015). *¿Qué es un hacker y qué tipos de hacker existen?* Obtenido de Computerhoy.com: https://computerhoy.com/noticias/software/que-es-hacker-que-tipos-hacker-existen-36027

Ward, M. (3 de Febrero de 2014). *Cómo hacer dinero buscando fallos informáticos*. Obtenido de BBC News: https://www.bbc.com/mundo/noticias/2014/02/140203_tecnologia_encontrar_virus_il

RAFAEL HERNANDEZ MORALES
Gerente de Infraestructura

Tel. 55 50800048 Ext. 2329
infraestructura@praxisglobe.com
Rafael Hernandez