Francisco Ruiz Sala

La ingeniería social y el phishing

Resumen: A partir de las experiencias de los primeros *hackers*, se explican los conceptos de *phishing* y de ingeniería social y se dan recomendaciones para evitar caer en fraudes informáticos.

Phishing, un reto para la ciudadanía digital

La creciente importancia de nuestra vida en línea ha aparejado también el surgimiento de diversas amenazas a la seguridad de nuestra información personal y, por lo tanto, a nuestro bienestar personal y financiero.

La palabra *phishing* proviene del inglés y significa "pescando", (sustituir la f por ph es un uso de los *hackers*). El concepto se refiere a diversos métodos de fraude electrónico a los cuales se les llama "ingeniería social".

La ingeniería social es un conjunto de técnicas que usan los delincuentes informáticos. Sus objetivos suelen ser usuarios incautos, a quienes se les roba información confidencial, ya sea por medio de enlaces maliciosos, archivos que infecten sus equipos e incluso, logrando que la proporcionen por su propia voz.

Podemos definir la ingeniería social como engaño y fraude combinados con elementos tecnológicos, elementos que facilitan a los delincuentes la tarea de obtener la información que buscan, ya que una gran parte de los usuarios de estas tecnologías no conocen bien su funcionamiento, y esto da al delincuente una ventana de oportunidad para su ataque. La mayor parte de los ataques tienen el objetivo de robar, ya sea la identidad o el dinero de los usuarios

Los *hackers* y el origen del *phishing*

Pocos conocen el origen de la ingeniería social; sin embargo, este se remonta a 1972, cuando Dennis Dan "Denny" Teresi explicó a su amigo John Thomas Draper que un silbato obsequiado en cajas de cereales (Figura 1) podría ser usado para engañar a los equipos telefónicos y hacer llamadas gratis, con ayuda de un dispositivo para generar tonos llamado *blue box*. Draper (conocido más tarde como "El capitán Crunch") y Teresi se convertirían en dos de los *hackers* más famosos de la historia, y se dedicaron a introducirse de manera ilegal al sistema telefónico, que podría considerarse como uno de los más avanzados tecnológicamente en aquel entonces.

No solo usaron la técnica de la "caja azul", también utilizaban diversas formas de engaño, a las que llamaron "ingeniería social". Teresi, quien conocía bien la jerga profesional de los telefonistas, se dedicaba a llamar por teléfono engañando a los técnicos de las compañías telefónicas haciéndoles creer que era uno de sus pares, para obtener información confidencial, simplemente por medio de la palabra. Cabe señalar que Draper fue arrestado en 1972 bajo cargos de fraude telefónico, aunque más tarde fue contratado por Steve Jobs.

Figura 1. John Draper explica el uso del silbato de 2600 Hercios. Foto por Sebaso (2015)

Durante los años 80 sería Kevin Mitnik (Figura 2), otro *hacker* famoso, quien siguió los pasos de sus predecesores telefónicos y comenzó a utilizar la ingeniería social como técnica principal para poder entrar a las compañías de computadoras engañando a los empleados.

Figura 2. Kevin Mitnik en Campus Party México 2010. Fuente: https://www.flickr.com/photos/campuspartymexico/4889638678/

En sus inicios, el espíritu *hacker* hacía referencia a quienes conocían los sistemas y consideraban como un reto el entrar a estos y modificarlos. Desde entonces la connotación del término ha cambiado y actualmente se le suele relacionar con delincuentes que roban, espían, y propagan virus; son considerados como piratas electrónicos. La línea entre vulnerar el sistema, y hacer daño o robar puede ser muy delgada.

Existen *hackers* que contribuyen a la seguridad de los sistemas, pues son contratados para poner a prueba un sistema y encontrar sus vulnerabilidades. Se les suele apodar "*hackers* de cachucha blanca". Sin embargo, es muy fácil pasar de *hacker* a delincuente informático, y quienes lo hacen son llamados "*hackers* de cachucha negra". Por esa causa, para las leyes el ser *hacker* es lo mismo que ser un delincuente informático, ya que vulnerar los sistemas informáticos es un delito.

Con este contexto histórico y la explicación de la ingeniería social, podemos describir lo que es *phishing*, que en realidad es una técnica heredada de la ingeniería social y la cual, principalmente por medio de mensajes de correo electrónico nos engaña para robarnos, espiarnos e incluso permite utilizar nuestras computadoras para acciones maliciosas. Con el *phishing* los delincuentes informáticos son capaces de cometer delitos e incluso despojarnos de nuestro dinero.

Pero... ¿por qué caemos en los engaños del *phishing*, principalmente en correos electrónicos?

Las razones son varias, una es el no prestar atención a la importancia de un correo falsificado, otra es la ambición de recibir un premio o regalo, y otra es responder de forma impulsiva al miedo. Es muy fácil caer en estos engaños debido a que los mensajes falsifican aspectos de instituciones reales e incluso de aquellas con las que tenemos contratos. Los delincuentes se aprovechan de nuestra falta de atención o nuestra codicia para llegar a su objetivo, que es principalmente el robo.

Protegerse del *phishing*

¿Cómo protegernos ante esta amenaza del *phishing* y de la ingeniería social?

El equipo de UNAM-CERT (en inglés Computer Emergency Response Team), como expertos en seguridad nos hacen las siguientes recomendaciones:

- Verifica el remitente, desconfía de correos que no muestren su procedencia, de aquellos remitentes que el dominio sea diferente al que usualmente recibes o si presenta errores en su escritura.
- No respondas al correo que parece sospechoso, ya que estarás validando ante los atacantes tu cuenta de correo en caso de ser *spam*.
- Sospecha de cualquier correo que tenga sentido de urgencia o de curiosidad y que te solicite una acción inmediata como abrir un enlace, descargar archivos o enviar datos personales.
- Pon atención en la dirección del sitio *web* al que te remiten, puede tener variaciones en su escritura o redirigirte a un sitio diferente al que indica.
- No abras archivos adjuntos de remitentes desconocidos.
- Configura tu cliente de correo electrónico para que puedas ver la dirección de correo electrónico del remitente y no solo el nombre de quien lo envía, así como evitar la carga automática de contenido remoto.
- Establece filtros de correo no deseado y fraudulento.

Los educadores y el *phishing*

¿Qué importancia tiene que los docentes conozcan este tema y lo expliquen a sus estudiantes? Actualmente, muchos de nuestros estudiantes tienen una intensa vida en línea y sus datos privados están muy expuestos.

Una forma usual de llegar a los usuarios es por medio del correo electrónico, pero cada vez es más frecuente utilizar las redes sociales, en las que suelen navegar habitualmente los jóvenes en edad formativa. Es por ello que los docentes deben orientarlos acerca de la información que publican y las interacciones a las que responden.

A continuación (Figura 3) mostramos un ejemplo de correo electrónico *phishing*, explicado para identificar los elementos importantes para no caer en una estafa electrónica.

Correo de PHISHING

Figura 3. Infografía de un correo de *phishing*.

Referencias

Martínez, C. (18 de enero de 2019). ¿Qué es el phishing? https://www.seguridad.unam.mx/que-es-el-phishing-2

González, M. (22 de noviembre de 2011). *Seguridad informática aplicada a un entorno doméstico*. Universitat Politecnica de Valencia. https://riunet.upv.es/handle/10251/7795

Hasle, H., Kristiansen, Y., Kintel, K., y Snekkenes, E. (2005). Measuring Resistance to Social Engineerng. In: Deng, R.H., Bao, F., Pang, H., Zhou, J. (eds.) *Information Security Practice and Experience*. https://doi.org/10.1007/978-3-540-31979-5_12

Lee, R. (Director), (2001). *The Secret History of Hacking*. Discovery Channel. https://www.youtube.com/watch?v=il7-u-kryDE&t=1336s

Rosenbaum, R. (1 de octubre de 1971). Secrets of the little blue box. En *Esquire*. https://www.esquire.com/news-politics/a38878/steve-jobs-steve-wozniak-blue-box-phone-phreaking/

Santillán, J. (2009). Ingeniería Social, Técnica de Ataque Eficaz en Contra de la Seguridad Informática. En *Revista de Seguridad DGTIC UNAM*. https://ru.tic.unam.mx/tic/handle/123456789/1711

Ficha de autor

L.I. Francisco Ruiz Sala: ***fruiz@astro.unam.mx***

Licenciado en informática y especialista en Cómputo de Alto Rendimiento por el Instituto de Matemáticas Aplicadas en Sistemas (IIMAS) de la UNAM. Profesor de Asignatura de la Facultad de Ciencias UNAM, en la materia de Computación y maestrante en Ingeniería y Ciencias de la Computación en la UNAM.