Evite ser víctima de estafas electrónicas: Reconozca un ataque de ingeniería social.

Karina Astudillo B.

Gerente de IT, Elixircorp S.A. Máster en Administración de Empresas, ESPOL. Catedrática de la Maestría de Seguridad Informática.

RESUMEN

El artículo trata de algunos puntos relacionados con los delitos y fraudes informáticos y como reconocerlos como usuarios. Se conceptualizan los temas acerca de la ingeniería social que está en pleno auge en nuestro medio y a nivel mundial, lo que supone grandes cifras en esta modalidad de estafa.

PALABRAS CLAVE

Ingeniería Social, keyloggers, pishing.

ABSTRACT

The article discusses some points related to computer crime and fraud and how to recognize them as users. They conceptualize the issues about the social engineering that is booming in our country and worldwide, which means large numbers in this type of scam.

KEYWORKS

Social Engineering, keyloggers, phishing.

1. INTRODUCCIÓN

En base a nuestra experiencia en seguridad informáticanos atrevemos a decir que "vale más un usuario final instruido en buenas prácticas de seguridad, que cualquier equipo o software de protección".[1]

Esto cobra vida especialmente hoy, cuando la Fiscalía reportó haber recibido más de 1300 denuncias relacionadas con estafas electrónicas en el primer trimestre del año con pérdidas que superan el millón de dólares en el Ecuador (El_Universo, 2011)

Por esta razón no podíamos dejar pasar desapercibido un problema que contribuye con la inseguridad presente en nuestro país y a nivel mundial: los engaños y fraudes electrónicos. ¿Pero en qué consisten estos engaños? ¿Y cómo podemos detectarlos para no caer víctima de ellos?

Para ello debemos primero tener claro que este tipo de estafas o fraudes se denominan en el argot de seguridad como ataques de ingeniería social.

2. EN qUÉ CONSISTE LA INGENIERÍA SOCIAL

Ingeniería Social "es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos."(WIKIPEDIA).

En resumen, la Ingeniería Social es un tipo de ataque mediante el cual se abusa de la ingenuidad de los usuarios finales y se logra engañarlos para que revelen información confidencial ya sea de índole personal como es el caso del número de tarjeta de crédito o la clave del cajero automático, o de la empresa donde trabaja como por ejemplo el nombre de usuario que utiliza para ingresar a la red y la clave de acceso respectiva.

3. TIPOS DE ATAqUES DE INGENIERÍA SOCIAL

Dependiendo si para la realización del ataque interviene o no una computadora, los ataques de Ingeniería Social se clasifican en:

- Basados en humanos (human-based).
- Basados en computadoras (computer-based).

3.1. Ataques basados en humanos

En este tipo de ataques el hacker malicioso o cracker contacta directamente a su víctima ya sea de forma personal o bien con un llamado telefónico. Debido a que hay una interacción entre la víctima y el agresor este tipo de ataques tienden a ser los más exitosos, porque extrañamente las personas tienden a confiar más en otras personas que en un correo electrónico o una página web.Los ataques basados en humanos pueden ser de diferentes tipos, siendo los más populares:

- Hacerse pasar por un empleado de la empresa en que trabaja la víctima: en este tipo de ataque el cracker pretende ser un compañero de trabajo autorizado a solicitar información confidencial. Para que este ataque tenga éxito el cracker se toma el trabajo de recabar información sobre los nombres de los empleados, cargos, jerarquía y usa nombres de conocidos de la víctima durante la conversación.

  Un típico caso es el fingir que es un empleado nuevo o un pasante, o que es el nuevo chico de sistemas y está actualizando las claves. Estos ataques tienen éxito en empresas grandes donde no todo el mundo se conoce y en que no hay políticas establecidas para la entrega de información confidencial.

- Hacerse pasar por una persona importante: en este caso el cracker pretende ser un Gerente de otro departamento o sucursal o bien un cliente importante, para intimidar a un empleado de menor jerarquía para que le de información. Un ejemplo típico es el caso del "Gerente" que pide una carpeta importante a una secretaria porque está por entrar a una reunión.

  Estos ataques tienen éxito porque explotan el miedo de perder el puesto de los empleados y por eso a pocos se les ocurriría cuestionar a alguien que parece ser una figura de autoridad.

- Llamada al Soporte Técnico: aquí en cambio se explota la predisposición de ayudar de los empleados de soporte o help-desk dado que parte de su trabajo consiste en ayudar a los usuarios que pierden sus claves o que no pueden ingresar a la red. En este ataque el cracker pretende ser un empleado asustado que olvidó su clave y teme que el jefe lo despida, porque olvidó enviar un mail importante el día

anterior. Para que tenga éxito el ataque, el hacker malicioso debe indagar previamente nombres de usuarios válidos y la jerarquía existente en la empresa víctima.

- Ingreso a una zona restringida través de un tercero amable (tailgating): en esta clase de ataque el cracker pretende ser un empleado de la empresa que olvidó su tarjeta de acceso y espera a que otro empleado amable le abra la puerta.

  Otra variación de ataque es en la que el "empleado" tiene las manos ocupadas y no puede sacar la tarjeta de acceso; nunca falta un buen samaritano que se apiada del "compañero" que carga la caja pesada y le abre la puerta con su tarjeta de acceso y hasta le ayuda a cargar la caja adentro de la empresa. Una vez dentro el cracker está libre para sustraer información o inclusive carpetas, laptops, etc.

- La llamada de actualización de datos: es increíble la cantidad de personas que aún caen en este tipo de engaños telefónicos. Aquí el cracker pretende ser un empleado del banco, tarjeta de crédito, compañía de seguros, etc., y se identifica dándole información a la víctima que es fácil de obtener públicamente, pero que suena convincente. Ejemplo: "El Sr. Arturo González? Mi nombre es Andrea Estévez y soy su agente de cuenta de Pacificard.

  Al momento nos encontramos actualizando datos de nuestros clientes para ponerlos al tanto de una nueva promoción. Por favor confírmeme, su segundo nombre es José verdad? Su segundo apellido es Paredes? Tenemos registrada como dirección de su casa….blahblah. Ahora por favor confírmeme su número de pin…"

- Vistazo sobre el hombro (shouldersurfing): aquí el cracker ha ganado previamente acceso físico a la empresa víctima por lo general haciéndose pasar por un cliente que va a solicitar información sobre los productos o servicios y entonces aprovecha de mirar cuando el empleado digita su clave ya sea directamente o utilizando cámaras espías escondidas en dispositivos tan inocentes como una pluma.

  Aunque pareciera una película de James Bond, les sorprendería saber lo fácil que se consiguen juguetitos como estos en Internet

y lo baratos que son (entre $30-$50 más el envío internacional).

Para protegernos de estos ataques la mejor arma es la educación de los usuarios finales, la elaboración de políticas de seguridad corporativas y el "principio de desconfianza". Siempre se debe verificar que la persona con quien se habla es efectivamente quien dice ser y que tiene la autorización requerida para solicitarnos información. Si desconfía de alguien, verifique primero los datos, su jefe no lo va a despedir por preocuparse por la seguridad de la empresa eso se lo aseguro.

3.2. Ataques basados en computadoras

En este tipo de ataques se utilizan medios electrónicos para perpetrar el ataque de ingeniería social. Los medios más utilizados son:

- Archivos adjuntos de correo electrónico: en este tipo de ataque el cracker envía un correo electrónico a la víctima fingiendo ser un amigo o una entidad con la que ésta tiene relación y adjunta un archivo que pretende ser información útil para la misma. El archivo adjunto puede contener un virus o gusano informático, o bien un troyano mediante el cual el cracker puede extraer información confidencial de la computadora de la víctima o inclusive tomar control remoto de la misma.

- Phishing y Sitios web falsos: el phishing es un engaño en el cual se hace uso de dos componentes, un correo electrónico que parece provenir de una entidad válida y que insta a la víctima a hacer click sobre un enlace que parece ser real y un sitio web falso que luce exactamente igual que el sitio real, al que se redirige la petición del usuario.

  Una vez en el sitio web falso el usuario ingenuo ingresa sus credenciales, el cracker las captura, la vícitima obtiene un mensaje de "datos confirmados" o "estamos en mantenimiento, pruebe en unos minutos" y el usuario es redireccionado a la página web de la institución real.

- Ventanas emergentes o de pop-up: en este tipo de ataque el usuario ingresa a una página web de acceso gratuito como por ejemplo un foro, blog, o sitios en donde "regalan" software. Una vez en el sitio web aparece una

ventana emergente que insta al usuario a hacer click indicándole que ganó algo u ofreciéndole descargar canciones, emoticones, libros, jugar un juego, etc., gratis! Aquí hay varias opciones, o bien la "descarga gratuita" contiene virus, gusanos o troyanos o el jueguito que requiere que demos click varias veces para matar al marcianito tiene código oculto que aprovecha nuestros clicks para que autoricemos a un control como por ejemplo el flash a acceder a nuestro disco duro. En el caso puntual de este último ejemplo, tendrá éxito en versiones viejas de navegadores y del control de flash si el usuario no ha descargado las nuevas versiones que corrijen esta vulnerabilidad.

- Capturadores de teclas, keyloggers: los keyloggers son dispositivos de hardware o bien software que permite al cracker capturar todo lo que la víctima teclea en su computador. En este sentido hay keyloggers de software que se instalan inadvertidamente en la máquina de la víctima a través de un programa troyano (que pretende ser un aplicativo útil) y que envían de forma periódica y automática el texto capturado a través de Internet al cracker. Sin embargo, la mayoría de antivirus buenos logran detectar con éxito a estos programas espías; es por eso que los más peligrosos son los keyloggers de hardware, puesto que no pueden ser detectados por los antivirus o sistemas de detección de intrusos. Un keylogger de hardware se instala entre el teclado y el puerto respectivo del computador y los hay PS/2 y USB. Por lo general son del mismo color que el cable del teclado y el usuario no instruido tiende a confundirlo como parte del mismo, internamente tienen una memoria protegida con clave en la que se pueden guardar días y hasta meses de capturas.

  Tanto para instalarlo como para recuperar la información capturada el cracker debe tener acceso físico al equipo víctima. Para evitar caer en este tipo de ataque hay que tener la buena costumbre de revisar la parte trasera del computador cuando llegamos a la oficina y cada vez que regresemos del baño, cafetería, lunch, etc. Sé que suena molesto y paranoico, pero creánme el uso de keyloggers es real.

4. RECOMENDACIONES FINALES

En definitiva para evitar caer presa de ataques de ingeniería social debemos tomar las siguientes precauciones:

- Nunca abra un mail sospechoso y menos aún descargue o abra un archivo adjunto que le resulte extraño. Si proviene "de un amigo" al que puede llamar por teléfono o contactar por chat pregúntele si es cierto que él fue quien le envió el correo y si está seguro de la procedencia del archivo adjunto. Tenga la buena costumbre de mantener actualizada la licencia de su antivirus y descargue con frecuencia las actualizaciones de firmas del mismo, inspeccione los archivos sospechosos con el antivirus antes de abrirlos.

- Los Bancos y otras entidades no envían enlaces por mail ni le piden a sus usuarios comprobar sus claves. Si desconfía de un mail de este tipo coloque el puntero de su mouse sobre el enlace sin darle click y mire en la parte inferior de su cliente de correo la verdadera dirección del enlace, confirme que esta corresponde efectivamente a la de la entidad; preferiblemente no haga click si necesita conectarse a este enlace, tómese el trabajo extra de abrir el navegador y escribir usted mismo la dirección web oficial de la entidad en cuestión, sólo toma unos segundos más y puede ahorrarle un disgusto y mucho dinero.

- Jamás de información confidencial por teléfono o por correo electrónico. El personal de soporte de sistemas no necesita conocer su clave para darle autorización de ingreso a aplicaciones, ellos tienen usuarios administradores especiales que sirven para conceder esos permisos, desconfíe siempre de quien le pide su clave por teléfono o por mail.

- Es preferible pasar por desconfiado o desatento, antes que abrirle la puerta a un extraño. Si un "compañero" está cargando una caja pesada y le pide que pase su tarjeta para darle acceso a la empresa o a un área restringida, pídale mejor que le diga en qué bolsillo tiene su tarjeta y ofrézcase a sacarla para registrar su acceso, o bien pida ayuda a un guardia de seguridad para que ayude a su "compañero" con "la caja

pesada" y que este pueda pasar su propia tarjeta de acceso.

Está de más decir que use su sentido común, si algo le resulta inusual es porque probablemente lo es.

REFERENCIAS

- El_Universo. (23 de Marzo de 2011). Fraudes Informáticos. El Universo, pág. 14.

- WIKIPEDIA. (s.f.). es.wikipedia.org. Recuperado el 14 de Octubre de 2011, de http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

1