Ingeniería Social

Nombre estudiantes aquí

Escuela 4-xxx “Nombre escuela aquí”

Tecnologías de la información y la comunicación

Prof. Julio Y. Silva

28 de agosto de 2022

Índice aquí

Ingeniería social y cómo protegerse

En cualquier cadena de seguridad, los humanos somos casi siempre el eslabón más débil, porque somos susceptibles de todo tipo de tácticas de manipulación. Las técnicas de ingeniería social se aprovechan de esta vulnerabilidad humana para engañar a las víctimas y conseguir que divulguen información privada. Aprenda a detectar un ataque de ingeniería social y cómo un software de seguridad potente puede ayudarle a evitar que sea víctima de tácticas de ingeniería social.

¿Qué es la ingeniería social?

La ingeniería social es la práctica de utilizar técnicas psicológicas para manipular el comportamiento. La ingeniería social se produce aprovechando el error humano y animando a las víctimas a actuar en contra de sus intereses. En el ámbito de la seguridad de la información, la definición de ingeniería social se refiere a conseguir que las personas divulguen datos privados en línea, como datos de acceso o información financiera.

En otros contextos, la ingeniería social significa algo ligeramente diferente. En las ciencias sociales, por ejemplo, la ingeniería social es simplemente el esfuerzo por influir psicológicamente en los comportamientos sociales a una escala mayor, de grupo. Eso puede incluir animar a la gente a comportarse correctamente en el transporte público, dejar de fumar o incluso apoyar un cambio político.

Aquí nos centraremos en la ingeniería social en el contexto de la seguridad de la información, donde los hackers despliegan técnicas en línea para obtener acceso a información confidencial. En este ámbito digital, la ingeniería social puede definirse como un ciberdelito.

¿Cómo funciona la ingeniería social?

La ingeniería social funciona aprovechando los prejuicios cognitivos de las personas. Un atacante de ingeniería social se hace pasar por alguien simpático, digno de confianza o con autoridad y engaña a la víctima para que confíe en él. Una vez que la víctima confía en el atacante, es manipulada para que revele información privada.

Por desgracia, hay muchos sesgos cognitivos que los atacantes pueden explotar en su beneficio, robando los datos privados de las víctimas delante de sus narices. Las técnicas de ingeniería social explotan esta tendencia a la confianza de muchas maneras diferentes.

Tipos de ataques de ingeniería social

Una de las mejores maneras de protegerse de un ataque de ingeniería social es conocer los métodos más comunes utilizados en la ingeniería social. Hoy en día, la ingeniería social se produce con frecuencia en línea, incluso a través de estafas en las redes sociales, donde los atacantes se hacen pasar por un contacto de confianza o una figura de autoridad para manipular a las personas para que expongan información confidencial.

Aquí otros tipos de ataques comunes en la ingeniería social:

Phishing

El phishing es un tipo de ataque de ingeniería social en el que las comunicaciones se disfrazan para que parezcan proceder de una fuente de confianza. Estos mensajes –a menudo correos electrónicos– están diseñados para engañar a las víctimas y conseguir que den información personal o financiera. Después de todo, ¿por qué habríamos de dudar de la autenticidad de un mensaje que llega de un amigo, un familiar o una tienda que visitamos a menudo? Las estafas de phishing se aprovechan de esta confianza.

Spear phishing

El spear phishing es un tipo de ataque de ingeniería social que se dirige a grandes empresas o a personas concretas. Los ataques de spear phishing están muy dirigidos a pequeños grupos o personas con poder, como ejecutivos de empresas y celebridades. Los ataques de ingeniería social que utilizan este método suelen estar bien estudiados y disfrazados de forma insidiosa, lo que dificulta su detección.

Vishing

El vishing, también conocido como «phishing por voz», es un tipo sofisticado de ataque de phishing. En estos ataques, se suele falsificar un número de teléfono para que parezca legítimo: los atacantes pueden presentarse como personal informático, compañeros de trabajo o banqueros. Algunos atacantes también pueden utilizar cambiadores de voz para ocultar aún más su identidad.

Smishing

El smishing es un tipo de ataque de phishing que llega en forma de mensaje de texto o SMS. Habitualmente, estos ataques piden a la víctima que realice alguna acción inmediata a través de enlaces maliciosos en los que hay que hacer clic o números de teléfono a los que hay que llamar. A menudo, solicitan a las víctimas que revelen información personal que los atacantes pueden usar en beneficio propio. Los ataques de smishing suelen transmitir una sensación de urgencia para que las víctimas actúen rápidamente y caigan en la trampa.

Whaling

El whaling es uno de los ataques de phishing más ambiciosos que existen, con consecuencias catastróficas. Este tipo de ataque de ingeniería social suele estar dirigido a un objetivo de alto valor. A veces se habla de «fraude de los directores generales», lo que da una idea de la marca típica. Los ataques de whaling son más difíciles de identificar que otros ataques de phishing, porque adoptan con éxito un tono de voz apropiado para los negocios y utilizan el conocimiento interno de la industria en su beneficio.

Baiting

Los ataques de ingeniería social no siempre tienen su origen en Internet: también pueden empezar fuera de las redes. El baiting se refiere al caso en el que un atacante deja un dispositivo infectado con malware (por ejemplo, una unidad USB) en algún lugar fácil de encontrar. Estos dispositivos suelen estar etiquetados de forma especial para crear curiosidad. Si alguien especialmente curioso (o avaricioso) lo recoge y lo conecta a su equipo, este podría infectarse involuntariamente con malware.

Scareware

El scareware es un tipo de malware que utiliza la ingeniería social para asustar a las personas y conseguir que descarguen un falso software de seguridad o visiten un sitio infectado con malware. El scareware suele aparecer en forma de ventanas emergentes, que dicen ayudar a eliminar un virus informático que supuestamente existe en su dispositivo. Una vez que se hace clic en la ventana emergente, se le redirige a un sitio malicioso o se instala aún más malware sin que lo sepa.

Si sospecha que tiene scareware, u otro tipo de ventana emergente molesta, analice de forma periódica su PC con una herramienta de eliminación de virus de confianza. Analizar periódicamente su dispositivo en busca de amenazas es una buena higiene digital. Puede evitar futuros ataques de ingeniería social, e incluso puede ayudar a mantener sus datos privados a salvo.

Pretexting

El pretexting consiste en crear un escenario falso, o «pretexto», que los estafadores utilizan para engañar a sus víctimas. Los ataques de pretexting pueden producirse en línea o no, y son uno de los trucos más eficaces para un ingeniero social: los atacantes investigan mucho para hacerse pasar por auténticos.

No es fácil descubrir las artimañas de un pretexto, así que tenga cuidado al compartir información confidencial con extraños. Y si alguien le llama con un problema urgente, póngase en contacto con la organización para descartar un ataque de ingeniería social.

Honey trap

Una honey trap es un tipo de esquema de ingeniería social en el que un atacante atrae a una víctima a una situación sexual vulnerable. El atacante aprovecha la situación como una oportunidad para la sextorsión u otro tipo de chantaje. Los ingenieros sociales suelen tender trampas enviando correos electrónicos de spam en los que afirman haber estado «observando a través de su cámara web» o algo igualmente siniestro.

Si recibe un correo electrónico como este, compruebe que su cámara web es segura. Mantenga la calma y no responda: estos correos no son más que spam.

Spam en el correo electrónico

El spam en el correo electrónico es uno de los tipos de ingeniería social más antiguos en Internet y es responsable de prácticamente toda la basura que llega a su bandeja de entrada. En el mejor de los casos, el spam en el correo electrónico es molesto. En el peor de los casos, se trata de una estafa para obtener sus datos personales. Muchos servidores de correo electrónico revisan los mensajes automáticamente en busca de spam malicioso, pero el proceso no es perfecto y a veces llegan mensajes peligrosos.

Los métodos descritos anteriormente son los tipos más habituales de ataques de ingeniería social que se utilizan para tener acceso a los datos personales de las víctimas. Los atacantes siempre encuentran nuevas maneras de engañar a las personas y a las máquinas, especialmente con formas más creativas de utilizar métodos de ingeniería social tan antiguos como el spam en el correo electrónico y el pretexting.

Cómo evitar la ingeniería social

La mejor manera de evitar los ataques de ingeniería social es saber cómo detectarlos al verlos. Una vez que cae en las redes de un ingeniero social, puede ser difícil librarse de ellas. Afortunadamente, no necesita ser un experto en tecnología para seguir buenas prácticas de ingeniería social. Lo único que necesita es su intuición y sentido común.

Cambie la configuración de spam en el correo electrónico

Una de las formas más fáciles de protegerse de los ataques de ingeniería social es ajustar la configuración de su correo electrónico. Puede reforzar sus filtros de spam y evitar que se cuelen en su bandeja de entrada correos electrónicos de spam de ingeniería social. El procedimiento para configurar los filtros de spam puede variar en función del cliente de correo electrónico que utilice, así que consulte nuestra guía para bloquear los mensajes de spam.

También puede añadir las direcciones de correo electrónico de personas y organizaciones que sepa que son legítimas a sus listas de contactos digitales: cualquiera que en el futuro diga ser ellos pero que utilice una dirección diferente es probablemente un ingeniero social.

Investigue la fuente

Si recibe un mensaje de correo electrónico, un SMS o una llamada telefónica de una fuente no conocida, búsquela en un motor de búsqueda para ver qué aparece. Si forma parte de un ataque de ingeniería social conocido, el remitente puede haberse identificado como tal previamente. Incluso si el remitente parece legítimo, compruébelo de todos modos, porque la dirección de correo electrónico o el número de teléfono pueden resultar ser solo ligeramente diferentes de la fuente real, y pueden estar vinculados a un sitio web inseguro.

Este método no siempre funciona si el número de teléfono ha sido falsificado como parte del ataque de ingeniería social. Si una búsqueda en la web no muestra nada, otra forma de evitar un ataque es contactar directamente con la organización que dice haberse puesto en contacto con usted.

Si algo parece demasiado bueno para ser cierto, seguramente sea falso

Las habilidades básicas de pensamiento crítico son una de las mejores maneras de evitar que le ocurra un ataque de ingeniería social. Algunos ataques recientes de ingeniería social llevados a cabo en Twitter afectaron a famosos como Elon Musk y Bill Gates parecía que estaban enviando mensajes para dar miles de dólares en bitcoins si los seguidores les daban tan solo mil.

Parece bastante claro que unos famosos regalando miles de dólares en bitcoins suena demasiado bueno para ser verdad. En esta forma de ataque de ingeniería social, la intuición y el sentido común pueden ser la clave. Desconfíe de las ofertas que ofrecen grandes recompensas a cambio de una tarifa aparentemente pequeña. Y, si la solicitud parece venir de alguien que conoce, pregúntese «¿De verdad me pediría esta información de este modo?»

Utilice software de seguridad y confianza

Puede ahorrarse el tiempo y las molestias de tener que comprobar las fuentes y evitar ataques de ingeniería social gracias a software antivirus de confianza capaz de detectar mensajes o páginas web sospechosos. Este software de seguridad detecta y bloquea malware e identifica posibles ataques de phishing antes de que tengan la oportunidad de actuar sobre usted.

Ejemplos de ataques reales de ingeniería social

¿Alguna vez ha sido víctima de la ingeniería social? Quizá no se haya dado cuenta, porque los ataques de ingeniería social reales pueden ser de muchos tipos. En el contexto de seguridad de la información, los ataques de ingeniería social a menudo aparecen como un mensaje de correo electrónico, de texto o de voz de una fuente aparentemente inofensiva. Puede pensar que es capaz de detectar un mensaje de correo electrónico sospechoso por su cuenta, pero los atacantes se han vuelto más sofisticados.

Los siguientes ejemplos de la vida real muestran que incluso las organizaciones y las personas con defensas sofisticadas contra los ciberataques y recursos para evitar la ingeniería social pueden ser víctimas.

2020: Twitter

En 2020, Twitter se convirtió en el centro de ataques de ingeniería social cuando las cuentas de Barack Obama, Bill Gates, Elon Musk y otros fueron pirateadas para solicitar bitcoins a sus seguidores. Los creadores del ataque de ingeniería social ganaron casi $120 000 en Bitcoin, pero el mayor peligro fue el claro acceso de los hackers a las cuentas de los famosos, aunque, según supuestamente, no se comprometieron los datos personales.

2019: El timador de Tinder

Desde 2011, el infame "timador de Tinder" engañó a sus víctimas para que pagarán un lujoso estilo de vida a través de una serie de estafas románticas. Utilizó una combinación de manipulación, amor y mentiras para salirse con la suya, llegando a robar unos 10 millones de dólares en sus dos últimos años de artimañas de ingeniería social. En 2019 fue condenado, y en 2022 el timador cayó en una estafa, y perdió casi 7 000 dólares del dinero que tanto le había costado ganar (estafar).

2018: Alquileres de vacaciones

En 2018, las estafas de phishing en alquileres vacacionales, donde los hackers se hacían pasar por los caseros que ofrecían alquileres reales, fueron tan habituales que la Comisión Federal de Comercio de EE. UU. advirtió sobre ellas. En muchos casos, se piratearon los datos de contacto de los caseros reales, de modo que las víctimas tenían pocos motivos para pensar que no estaban hablando del alquiler con el propietario real.

2017: Ethereum Classic

El hackeo de 2017 de la criptomoneda Ethereum Classic, en el que los hackers se hicieron pasar por el propietario de Classic Ether Wallet, fue otra estafa de ingeniería social de alto nivel y de la vida real. Los hackers robaron miles de dólares en criptomoneda a usuarios desprevenidos. Hoy en día, las estafas de ingeniería social siguen siendo frecuentes en la comunidad Bitcoin, y la protección contra el criptojacking se ha convertido en una gran prioridad.

2016: Partido Demócrata

El hackeo del correo electrónico del Partido Demócrata de Estados Unidos en medio de las elecciones presidenciales de 2016 es uno de los ataques de ingeniería social más emblemáticos de los últimos tiempos. Los hackers rusos lanzaron un ataque de spear phishing contra los líderes de la campaña demócrata, que les permitió destapar información sensible de la campaña y datos de casi 500 000 votantes.

2015: Ubiquiti Networks

En 2015, el destacado fabricante de tecnología de redes Ubiquiti perdió 46 millones de dólares cuando el correo electrónico de un empleado de Ubiquiti Networks fuera hackeado. Las credenciales del empleado fueron utilizadas por los estafadores para solicitar transferencias bancarias falsificadas a través del departamento financiero de la empresa.

2014: Sony Pictures

Otro famoso ataque de ingeniería social fue el ciberataque de 2014 a Sony Pictures, cuando los hackers norcoreanos enviaron correos electrónicos de phishing disfrazados de correos de verificación de ID de Apple a los empleados de Sony Pictures. Los hackers utilizaron las credenciales de acceso para borrar las redes de Sony y robar registros financieros y otros datos privados de la empresa.

¿Por qué es tan peligrosa la ingeniería social?

La ingeniería social puede ocurrirle a cualquiera, ya sea en persona, por teléfono o en línea, y también es un método bastante fácil cuando se realizan estafas, fraudes u otros delitos. Los ingenieros sociales no necesitan tener grandes conocimientos técnicos; solo tienen que ser capaces de engañarle para que les entregue datos sensibles. El hecho de que todos estemos en riesgo hace que sea una estafa potencialmente devastadora.

Las redes sociales han ayudado a los ingenieros sociales a ser más habilidosos, creando perfiles falsos que parecen ser reales, o incluso suplantando a personas reales. Es importante estar alerta ante perfiles extraños o desconocidos en redes sociales.

Las tácticas de manipulación de la ingeniería social son insidiosas. A menudo, las víctimas de la ingeniería social no se dan cuenta de que están siendo manipuladas hasta que es demasiado tarde. Si bien los sesgos cognitivos pueden favorecer la adaptabilidad, también es verdad que pueden usarse en nuestra contra. Los ataques de ingeniería social buscan información privada de los usuarios, lo que puede conducir al robo de identidad, extorsiones y mucho más.

Figura 1

Los Ataques de Ingeniería Social a Menudo Provienen de Fuentes Aparentemente Fiables.



Nota. Además, no es solo su dinero lo que está en peligro: en ocasiones las calificaciones crediticias y las reputaciones en Internet se desmoronan y se acumulan las deudas en su nombre. Aunque estas situaciones pueden revertirse, pueden llevar tiempo e interminables comunicaciones con organismos para limpiar su nombre. Usar software antivirus ayuda, pero no consigue que su cerebro esté a prueba de ataques. La mejor manera de evitar los ataques de ingeniería social es saber cómo detectarlos al verlos.

¿Quién corre mayor peligro de sufrir ingeniería social?

Cualquiera puede ser víctima de un ataque de ingeniería social, porque todos tenemos sesgos cognitivos de los que no siempre somos conscientes. Las personas que carecen de conocimientos tecnológicos o están más aisladas socialmente, como los ancianos, pueden ser más vulnerables. Sin embargo, los conocimientos técnicos por sí solos no pueden proteger a las personas frente a la manipulación psicológica, ni siquiera en un entorno empresarial.

Protéjase frente a ataques de ingeniería social

En lo que se refiere a los ataques de ingeniería social, el mantenimiento preventivo es más importante que el mantenimiento correctivo, prevenir es mejor que curar. Y, en muchos casos, no hay más cura para la ingeniería social que no sea cambiar las contraseñas y asumir las pérdidas económicas con toda la dignidad posible.

Por muy poderoso que sea el cerebro humano, puede llevarnos por el mal camino.

Referencias

https://www.avast.com/es-es/c-social-engineering