Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional Mendoza

Administración de Sistemas de Información

Informe de exposición: Ingeniería Social

Equipo docente:

Profesor Titular: Ing. Julio Cuenca

JTP: Mg. Ing. Mario Centeno

Grupo: N°6

Comisión: 4K10 - 2024

Integrantes:

Secotaro Ianardi, Leonardo Tomas

Duran, Andrea Tatiana

Lucero Fiorelli, Facundo Nicolas

Ogás, Sebastián Andrés

Peruzzi, Agustín Luis

Valdivia Dadda, Juan Manuel

Ministerio de Capital Humano
Universidad Tecnológica Nacional
Facultad Regional Mendoza

Definición y caracterización de la Ingeniería Social

La seguridad de la información se encuentra estrechamente ligada a la vanidad humana. En el ambiente informático, es muy conocido el dicho “una computadora apagada es una computadora segura”. Ahora bien, si la computadora está apagada, ¿quién es el objetivo? El usuario. No hay un solo sistema en el mundo que no dependa de un ser humano, lo que conlleva una vulnerabilidad independiente de la plataforma tecnológica.

La Ingeniería Social puede definirse como una ***acción o conducta social destinada a conseguir información de las personas cercanas a un sistema***. Es el arte de conseguir de un tercero aquellos datos de interés para el atacante por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos.

En palabras de Kevin Mitnick, uno de los personajes más famosos del mundo por delitos utilizando la Ingeniería Social como principal arma:

> *"usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es un llamado a un empleado desprevenido e ingresar sin más. Tienen todo en sus manos".*

La efectividad del ataque se radica en las cualidades propias del ser humano como, por ejemplo: credulidad, inocencia, curiosidad, ambición, desconocimiento, confianza, modos de relacionarse con otros, gusto por el morbo, etc.

Si bien parece poco creíble que con sólo preguntar por la información que a uno le interesa se obtenga lo que se desea; esta técnica puede resultar de una efectividad absoluta, si la persona con fines maliciosos se gana la confianza de la víctima a la que intenta engañar.

Este “arte de engañar” puede ser utilizado por cualquiera, desde un vendedor que se interesa en averiguar las necesidades de sus compradores para ofrecerles un servicio, hasta creadores de malware y atacantes que buscan que un usuario revele su contraseña de acceso a un determinado sistema. Más allá de las coincidencias, o no, en el límite de lo éticamente correcto, todo intento de obtener información confidencial para un uso inapropiado, resulta una actividad altamente cuestionable.

Otra importante característica de la Ingeniería Social es su excelente relación costo-beneficio obtenida con su aplicación, la convierte en una técnica de lo más eficiente: con sólo una llamada telefónica, un correo electrónico o un mensaje de texto vía SMS el atacante puede obtener acceso a información valiosa del usuario, la empresa o incluso acceder a una red de sistemas.

Los atacantes que usan la Ingeniería Social por lo general tienen dos objetivos:

- Sabotaje: alterar o corromper datos
- Robo: obtener objetos de valor como información, acceso a sistemas o dinero

Métodos

Los distintos métodos de Ingeniería Social suelen tener en común los siguientes pasos:

- Preparación: recopilar información básica de la víctima
- Infiltración: comunicarse y generar confianza en la víctima
- Explotación: de las debilidades de la víctima
- Desentendimiento

A su vez, el atacante suele mostrar los siguientes comportamientos para ser más efectivo:

- Intensificación de las emociones
- Urgencia
- Confianza

Tipos de ataque

Existen diferentes tipos de técnicas de ingeniería social:

- Phishing: envían correos electrónicos falsos para obtener información de la víctima. Por ejemplo, pueden solicitar datos personales, de tarjetas de crédito, de la obra social, de actualización laboral, contraseñas de sistemas, etc.

- Vishing: obtienen información a través de una llamada telefónica. El ciberdelincuente se hace pasar por un familiar, personal de una empresa o de soporte técnico.
- Smishing: mediante mensajes de texto, que muchas veces incluyen un enlace a un sitio web.
- Spear phishing: envían un correo electrónico falso a alguien que tiene, por ejemplo, un determinado cargo o maneja información sensible en una empresa. Los delincuentes conocen a la persona e intentan robarle datos.
- Quid pro quo: ofrecen a la víctima algo deseable (como un concurso) a cambio de su información personal.
- Farming: realizan varias comunicaciones con las víctimas hasta conseguir la mayor cantidad de información posible.
- Robo de cuentas de correos electrónicos: roban cuentas reales para cometer ilícitos entre los contactos de la víctima, enviar software malicioso o para obtener información personal.
- Cebo: abusando la curiosidad de la víctima para que se exponga, ya sea abriendo un enlace, un archivo adjunto o un pendrive abandonado en un espacio público.
- Acceso físico: el atacante se presenta en persona haciéndose pasar por alguien más.

- Scareware: malware que busca asustar a la víctima para que descargue otro malware o revele información confidencial.

La amenaza de la IA

Con el avance IA, las técnicas utilizadas por los ciberdelincuentes para manipular a las personas y hacer que revelen información confidencial se han vuelto más sofisticadas y efectivas:

- Phishing personalizado: la IA analiza datos de redes sociales para crear correos electrónicos de phishing muy convincentes, dirigidos a individuos específicos.
- Deepfakes y suplantación de identidad: los deepfakes son vídeos, imágenes o archivos de voz manipulados con software de inteligencia artificial (IA) para parecer reales y auténticos. Los ciberdelincuentes pueden usarlos para extorsionar, cometer fraude o manipular a las víctimas para que realicen acciones perjudiciales.
- Chatbots maliciosos: que interactúan con las víctimas de manera muy convincente para obtener datos sensibles y cometer fraude.
- Evolución de Patrones: los algoritmos de aprendizaje automático pueden estudiar y aprender de los sistemas de detección de fraudes, adaptando sus técnicas para evadir la detección.

Casos de estudio

Comunicación laboral fraudulenta

Un compañero de nuestro equipo de trabajo recibió en una ocasión en su dirección de correo laboral un mensaje cuyo remitente era “Comunicación Interna”, instando a activar la autenticación de dos factores en su cuenta mediante un enlace. Cabe destacar que este nombre del remitente es usado por una cuenta de correo oficial de la organización.

El correo presentaba el mismo formato que los correos legítimos, desde las imágenes, fuentes y tamaño de letra hasta la redacción y ortografía. El enlace tenía texto que fingía ser la URL legítima del cliente de correo web de la organización.

Sin embargo, al mantener el cursor sobre el remitente, mostraba que su dirección no era legítima. Haciendo lo mismo, podía verse que el enlace también era falso.

Apenas se supo de esto, se instó a todos los empleados que hubieran sido engañados a cambiar su contraseña, pues fue un ataque masivo.

Ataque de Vishing

Un miembro de la familia de un compañero recibió una llamada telefónica de un supuesto representante del banco en el que tiene una cuenta. El tono de la llamada era muy profesional y la persona que hablaba parecía tener conocimiento de ciertos detalles básicos de la cuenta, como el nombre completo del familiar y la dirección postal. El supuesto agente le informó que

había habido una actividad sospechosa en su cuenta y que necesitaba verificar su identidad para prevenir un posible fraude. Durante la llamada y con la excusa del supuesto fraude, el supuesto agente solicitó la confirmación de información sensible, como el número completo de la tarjeta de débito y el código de seguridad que se encuentra en la parte posterior de la misma. El familiar, confiando en que estaba hablando con un representante legítimo del banco, proporcionó esta información. Horas más tarde, el familiar recibió notificaciones de transacciones no autorizadas realizadas desde su cuenta bancaria.

Debido a esto se tuvo que bloquear la tarjeta y denunciar el fraude a la policía

Otro ataque de Vishing

En este caso me pasó a mí personalmente (Valdivia), recibí una llamada de un número el cual decía que era parte del equipo de seguridad de mercado pago, el atacante mencionaba que una persona había realizado un pago a través de mi cuenta que no era yo y realizando los pasos que el me solicitaba se podía cancelar ese pago. Durante la llamada se me solicitó que acceda a las opciones de seguridad de mi cuenta para ver qué dispositivos tenía vinculados a la misma, a continuación se me solicitó que acepte la vinculación de un nuevo dispositivo (la computadora del estafador) para tomar el control de mi cuenta y así robar la plata. En este caso detecté enseguida que era falso, primero porque el personal de mercado pago nunca pediría realizar los pasos mencionados y segundo el número de teléfono no estaba asociado a ningún tipo de soporte de mercado pago.

Este tipo de actividades son muy peligrosas ya que las personas mayores caen muy fácilmente en este tipo de estafas.

Google y Facebook Spear Phishing Scam

Uno de los casos más grandes de los que se tenga conocimiento tuvo como víctimas a Google y Facebook.

Un equipo de personas lideradas por Evaldas Rimasauskas creó una empresa fantasma, configurando cuentas bancarias para esta, haciendo pasar la misma por otra empresa de hardware que genuinamente tenía negocios con las víctimas.

Luego de esto enviaron periódicamente emails con facturas cobrando por bienes y servicios ofrecidos por la empresa que en verdad trabajaba con las víctimas. En estos mails se daba la instrucción de depositar los pagos en las cuentas bancarias de la empresa fantasma. Desde 2013 hasta 2015, se enviaron estos mails que causaron en conjunto una pérdida de más de 100 Millones de dólares.

Robo de código fuente a Motorola

Para finalizar la lista de casos de estudios es útil volver al comienzo del informe y hablar nuevamente sobre Kevin Mitnick, quien en 1992 pensó que sería una buena idea modificar el firmware del Motorola MicroTAC para poder tener más privacidad y escapar de las autoridades.

Para hacerse del código fuente optó por simplemente llamar a Motorola y pedir hablar con el project manager del proyecto. Luego de ser transferido

varias veces y hablar con distintas personas consiguió el número de la encargada del proyecto, pero al marcarlo se encontró con un mensaje pre grabado indicando que estaría de vacaciones pero podían contactarse con una compañera que había quedado a cargo.

Mitnick no lo dudo, y simplemente diciendo que trabajaba en otro campus de Motorola y usando un nombre falso pidió que le enviasen el código fuente, a lo que le preguntaron: “¿Qué versión quieres”, y él respondió “La última y mejor”.

Minutos después Kevin le explicaba a su interlocutora como comprimir y enviar el archivo haciendo uso de FTM, pero viendo que la transferencia fallaba ella consultó a su líder de seguridad por el problema: “Esta IP está fuera de la organización, así que no tengo permiso de enviarlo”. Mitnick se estaba dando por vencido hasta que la secretaria prosiguió e indicó “Pero me dieron el usuario y contraseña personal del líder se seguridad para que pueda enviártelo”. De esta manera Mitnick se hizo del código fuente del Motorola MicroTAC, algo así como el iPhone del momento.

Este caso es un muy buen ejemplo de cómo, incluso teniendo las personas correctas (un especialista en seguridad), una configuración adecuada (bloqueo de IPs externas) y una organización con miles de empleados, es posible que una persona burle todos los controles tan solo con una mentira.

FACC (fabricante austriaco de aviones) Spear phishing

FACC perdió alrededor de 42 millones de euros cuando la empresa fue víctima de una sofisticada estafa de correo electrónico comercial (BEC). Se

suplantó la cuenta de correo electrónico del director general de la empresa y se utilizó para enviar un correo electrónico "urgente" solicitando una transferencia de fondos. Este correo electrónico engañó a un empleado encargado de pagar la cuenta, que accedió a la solicitud, ingresando el dinero en la cuenta del estafador.

Conclusión: naturaleza de los ataques y mitigación

Si bien se podría entrar en particularidades según cada caso, es fundamental comprender que no hay tecnología capaz de proteger contra la Ingeniería Social, como tampoco hay usuarios ni expertos que estén a salvo de esta forma de ataque. La Ingeniería Social no pasa de moda, se perfecciona y sólo tiene la imaginación como límite.

La proliferación de la IA ha permitido perfeccionar los ataques, masificando los ataques personalizados que anteriormente estaban reservados a altos perfiles por su costo.

Los ataques de ingeniería social son muy difíciles de identificar. Los ciberdelincuentes usan diferentes técnicas psicológicas y sociales, distintos tipos de dispositivos y plataformas para engañar a las personas.

Así mismo, existe una única y efectiva forma de estar prevenido contra ella: la educación. No se trata aquí de una educación estrictamente técnica sino más bien una concientización social que permita al usuario estar prevenido y alerta para evitar ser un blanco fácil de este tipo de ataques.

Cualquier atacante con algo de experiencia puede engañar con facilidad a un usuario ingenuo. Si éste, en cambio, se encuentra debidamente capacitado e informado podrá descubrir la estafa y evitarla. Además, la educación de los usuarios suele ser una importante técnica de disuasión.

Algunos puntos importantes son:

- No entregar datos personales a personas extrañas por teléfono, correos electrónicos o redes sociales.
- Configurar la privacidad en las redes sociales para que no queden expuestos datos personales, reduciendo así el digital footprint.
- Informarse sobre este tipo de amenazas, ya que evolucionan constantemente.
- Usar una contraseña segura, única por aplicación y rotar las mismas periódicamente.
- Configurar la autenticación en dos pasos para estar alerta de accesos indebidos a tus cuentas.
- Prestar atención a cualquier persona que pida información personal, por cualquier medio.
- Seguir las cuentas oficiales de las entidades con las que interactuamos, como bancos, para conocer los riesgos actuales y los canales de comunicación seguros

- Limitar el acceso de los usuarios a los sistemas e información estrictamente necesarios, para mitigar el impacto de un posible ataque
- Verificar la identidad del remitente de mensajes de correo electrónico o quién se comunica por cualquier otro medio, pidiendo estos datos si es necesario.
- Estar atento a detalles como la gramática y la ortografía, las URLs, el diseño de sitios web, etc.
- No dejarse influenciar por la sensación de urgencia, que apresura la toma de decisiones.
- Si se está en un contexto organizacional, validar con algún par o superior la demanda de información y quien la realiza.

Bibliografía consultada

Franceschi-Bicchierai, L., & Franceschi-Bicchierai, L. (2024, 9 de Agosto). *How Kevin Mitnick stole the source code for the best cell phone of 1992*. VICE. https://www.vice.com/en/article/kevin-mitnick-hack-motorola-source-code/

Huddleston, T., Jr. (2019, 27 de Marzo). *How this scammer used phishing emails to steal over $100 million from Google and Facebook*. CNBC. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

Ibm. (2024, 22 de Julio). ¿Qué es la ingeniería social? *IBM Blog*. https://www.ibm.com/es-es/topics/social-engineering

Kostic, N. (2024, 21 de Marzo). *15 examples of social engineering attacks*. phoenixNAP Blog. https://phoenixnap.com/blog/social-engineering-examples

¿Qué es la ingeniería social? | *Definición*. (2017, 6 de Diciembre). https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering?srsltid=AfmBOoo_OdDqOaesl7pKpPjO_yuecEbDL1yvzQXzqWye7NeVeoZAJen9

¿Qué es la ingeniería social y cómo me protejo? (2024, 8 de octubre). Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte#:~:text=Se%20llama%20ingenier%C3%ADa%20social%20a,haci%C3%A9ndose%20pasar%20por%20otra%20persona.