DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ingeniería social

CURSOS EN LÍNEA

Ingeniería social

Algunos de los riesgos más importantes para la seguridad informática implican la vulnerabilidad del factor humano, este es el caso de ataques realizados por medio de ingeniería social.

Los ataques de ingeniería social se basan en la manipulación psicológica para que las personas realicen una acción o revelen información sensible que pudiera ser utilizada contra los sistemas de seguridad. Básicamente, se trata de un conjunto de técnicas que intentan engañar o abusar de las emociones, confianza, inocencia e ignorancia de las personas.

Existe una gran cantidad de técnicas de ingeniería social que convendría revisar a detalle. Sin embargo, en este documento nos concentraremos en aquellas realizadas con mayor frecuencia por medio de los sistemas informáticos con la finalidad que usted se encuentre preparado y pueda identificarlos.

Engaños y fraudes en la red

Internet es un sitio inseguro, así que podemos encontrar una gran diversidad de engaños y fraudes que intentan abusar de las personas. A continuación, revisaremos los métodos principales de ingeniería social a los que nos enfrentaremos en la red.

La mejor forma de evitar ser víctima de un ataque de ingeniería social es la educación y consciencia sobre el conjunto de técnicas comúnmente usadas para que se revele información o se realice una acción que no haríamos en una situación normal.

Figura 1. La ingeniería social está considerada como una de las principales estrategias para realizar ataques en sistemas informáticos.

Phishing

Actualmente, el phishing es el ataque principal que reciben tanto las organizaciones como las personas. El phishing es un intento de adquirir información sensible utilizando, primordialmente, el correo electrónico, aunque existen variantes de este ataque donde se utilizan mensajes vía redes sociales. En el phishing, un atacante emplea un conjunto de técnicas de ingeniería social tales como el engaño y la persuasión para que el usuario realice acciones específicas en su navegador.

Existen diferentes modalidades y términos especializados cuando se habla de phishing:

Cuando se realiza por medio de mensajes de texto del tipo SMS se le denomina smishing.

Cuando se realiza por medio de mensajes de mensajes de voz o llamadas se conoce como vishing.

Estos son términos especializados, pero es necesario comprender que el ataque intenta explotar el factor humano.

En estos ataques, un agente malicioso puede hacerse pasar por una empresa, organización o una persona confiable (por ejemplo, bancos, redes sociales, proveedores de servicios, un contacto conocido) y enviar un mensaje en donde se le pide a la víctima realizar una acción que comprometa su seguridad como puede ser la descarga de un archivo, que se acceda a un enlace que lleva a un sitio web malicioso o que se coloque información sensible en un formulario.

Figura 2. El correo electrónico es el principal medio para el phishing.

Para alcanzar el éxito, los atacantes hacen uso de mensajes elaborados en donde se plantea una situación extraordinaria. Por ejemplo, el robo de una cuenta de una red social, la mención de un cargo no identificado en la cuenta bancaria, un paquete que no se puede entregar, un mensaje de soporte técnico solicitando información para reparar un servicio, etc. Como puede adivinar, el objetivo es provocar en la víctima un sentimiento de angustia o urgencia que lo incite a la acción. Para incrementar sus posibilidades, los atacantes pueden llegar a utilizar logotipos oficiales, así como cualquier otro tipo de información relativa al usuario para hacer el mensaje lo más realista posible.

Sin embargo, si un usuario llega a hacer clic en los enlaces o descargar y ejecutar los archivos adjuntos, el atacante no solo podría llegar a obtener más información del sistema de la víctima, sino que podría llevar a que el atacante tomará control sobre él. Además, si el usuario ingresa sus credenciales (usuario y contraseña) en un portal falso creado por el atacante que simule ser uno verdadero, estará concediendo información sensible que pudiera poner en peligro su información e incluso su integridad. Por tal motivo, resulta importante mantenerse alerta ante los correos electrónicos de fuentes no confiables y comprobar por otros medios si la información que presentan es verdadera.

Figura 3. El phishing es una de las principales amenazas en el mundo digital.

Pharming

En el pharming se utiliza una técnica de redirección que provoca que los usuarios, al intentar ingresar a un sitio legítimo, sean enviados a un sitio falso especialmente preparado por el atacante.

Para esto, se puede llegar a usar una combinación de técnicas avanzadas en las que las solicitudes que realiza en un navegador web para un sitio auténtico sean trasladadas a un sitio apócrifo. Por ejemplo, el atacante pudiera modificar las entradas del servidor DNS o la caché del sistema del usuario, existen muchas técnicas para conseguir este resultado.

Una vez redirigido al sitio falso, es posible que el usuario no note ninguna diferencia, pues los atacantes copian la estructura de los sitios legítimos para no levantar sospechas. Una vez dentro, el usuario ingresa sus credenciales (usuario y contraseña) como normalmente lo haría y el sitio podría responder con un mensaje de error, pero lo relevante en este caso, es que al ingresar sus datos en este sitio falso le ha dado la información directamente al atacante.

El principal objetivo del pharming es la recolección de credenciales de usuarios. Para prevenirlo es vital mantener actualizados los sistemas y el navegador web, además verificar que se usan conexiones seguras en línea y ser cauteloso con los enlaces sospechosos y sitios web que se visitan.

Figura 4. El pharming es una técnica de ingeniería social que busca hacerse con las credenciales de usuarios.

Scam

La traducción de scam a español es "estafa". Internet está llena de estafas en donde se asegura a los usuarios una presunta compensación económica u otro beneficio por algún tipo de acción. En el scam se pueden usar técnicas de phishing, pharming, entre muchas otras, para guiar al usuario a hacer clic en algún enlace, dirigirse a un sitio web malicioso, enviar datos, descargar archivos, etc. En este punto usted debe ya debe identificar los patrones de acción que los atacantes buscan de los usuarios.

Las estafas en internet son tan variadas que resultaría imposible abarcarlas todas, pues, además, muchas de ellas están diseñadas para contextos específicos. Sin embargo, por regla general: **si algo parece demasiado bueno para ser verdad, es muy probable que se trate de una estafa**.

En México algunas de las principales estafas en la red están relacionadas con descuentos y préstamos económicos, ofertas de empleos, automóviles y departamentos en oferta, e incluso, las estafas relacionadas con supuestas parejas sentimentales. Existen noticias muy desagradables sobre alguna de estas estafas que han llevado a consecuencias irreversibles en la vida de las personas. Desgraciadamente, para evitar este tipo de ataques se necesita sentido común, pero como se ha mencionado, las técnicas de ingeniería social se utilizan para colocarnos en una situación de urgencia, deseo, ansiedad, miedo… que nos resta capacidad de reacción.

Figura 5. Existen innumerables modalidades de estafas en la red.

HOAX (noticias falsas)

Los hoax son distribuidos entre los usuarios de correo electrónico y redes sociales. Se trata de las cadenas de mensajes que podemos encontrar por estos medios. Un hoax es un tipo de engaño que pretende hacer pasar información falsa como verdadera. Las noticias falsas son utilizadas frecuentemente en campañas que intentan influir en la opinión general. Las campañas de influencia intentan cambiar la opinión, acciones o comportamiento del público al que van dirigido por medio de una serie de acciones coordinadas. Si bien este tipo de campañas han existido por siglos, la tecnología de comunicación y la evolución de los dispositivos informáticos, así como el

surgimiento de redes sociales, han permitido que la información se pueda compartir y divulgar a un ritmo nunca antes visto.

Figura 6. Día a día surgen diferentes noticias falsas en la red.

Este tipo de mensajes también puede ser utilizado en combinación con otros ataques. Por ejemplo, esta información se puede usar para crear un miedo innecesario y provocar conductas irracionales. Imagine una falsa campaña donde se alerta a los usuarios de un virus informático destructivo que puede afectar sus equipos sino descargan cierto programa o que elimine ciertos archivos de su computadora. Puede adivinar que el malware es justamente lo que el usuario descargará en caso de seguir esta noticia falsa o que sería el mismo usuario el que afectaría su sistema por eliminar posibles archivos clave. Nuevamente, en este apartado resulta imposible imaginar todos los escenarios posibles. Por lo tanto, se recomienda prudencia y la verificación de información en fuentes oficiales y acreditadas.

Tácticas de ingeniería social

Como se ha señalado, los ingenieros sociales utilizarán una serie de técnicas que, en combinación con los recursos que ofrece internet y las redes sociales, pueden llegar a crear escenarios realmente convincentes. Por lo tanto, será apropiado prestar atención en las tácticas comunes a las que seguramente se enfrentará. De manera general, la ingeniería social se basa en un conjunto de tácticas como son:

- Autoridad. Es posible que el atacante se haga pasar por una autoridad o institución para abusar de su confianza y solicitar su información.
- Intimidación. En esta táctica el atacante utiliza amenazas y el miedo para crear escenarios donde se le hace creer a la víctima que algo malo pasará sino se revela información o se realiza una acción particular.
- Consenso y aprobación social. Esta táctica aprovecha la forma en la que llegamos a comportarnos, pues tendemos a mirar el comportamiento de las otras personas y seguir su ejemplo en una situación en la que no sabemos cómo responder.

- Escasez. Aquí, el ingeniero social hace creer a la víctima que puede llegar a perder una oportunidad de adquirir un producto o servicio que se presenta de forma limitada. Esta táctica es muy utilizada en campañas de marketing.
- Urgencia. En esta modalidad, el atacante crea un escenario en el que se solicite la acción inmediata de la víctima, justamente, para que no pueda responder con mesura.
- Familiaridad y atracción. Con esta técnica el atacante aprovechará la relación o capacidad de atracción que tenga con la víctima. Los ingenieros sociales utilizan halagos y la persuasión para influir en las actividades de las víctimas.

El conocimiento de las tácticas de ingeniería social puede serle de utilidad para poder responder ante diferentes situaciones a las que se enfrentará en la red, pero también para analizar situaciones de su día a día en la interacción con las personas (principal escenario de acción de la ingeniería social).

Tendencias de nuevos ataques

En los últimos años hemos sido parte de una revolución en la tecnología. La irrupción de la inteligencia artificial ha marcado nuestra era y moldeará el futuro de los sistemas informáticos y, seguramente, cambiará la forma en la que interactuamos con ellos.

Desgraciadamente, con esta tecnología surgen nuevas oportunidades para las personas maliciosas que la utilizan para su beneficio. Así que, si el panorama de amenazas era desalentador, ahora debemos ser aún más cuidadosos.

Ataques con Inteligencia artificial

La inteligencia artificial hace referencia al desarrollo de sistemas informáticos con la capacidad de realizar de manera automática e independiente las tareas y toma de decisiones que anteriormente necesitaban la inteligencia e intervención humana. Es decir, en esta nueva era las computadoras pueden pensar y aprender como los humanos. A pesar de los beneficios que traen consigo estos alcances, debemos saber que esta tecnología está siendo usada para realizar ataques informáticos cada vez más elaborados.

La capacidad de la inteligencia artificial le permite generar texto, imágenes, audio, videos, y otros elementos que pueden ser utilizados con tácticas de ingeniería social para engañar a las personas. De hecho, ya lo hace. Observe la siguiente imagen:

Figura 7. Aitana López.[1]

Aitana López es una modelo digital creada por medio de inteligencia artificial que genera increíbles ganancias por su basta cantidad de seguidores en redes sociales que aumenta día con día.

No se necesita una gran capacidad técnica para la generación de modelos digitales, de hecho, cada día resulta más sencillo gracias a la inteligencia artificial. Pero no solo eso, la inteligencia artificial es capaz de generar videos a partir de imágenes, aplicar filtros extraordinarios, o bien, registrar e imitar la voz de una persona y responder mensajes en tiempo real con una precisión impresionante.

Así que es de esperar un perfeccionamiento en las técnicas de ingeniería social digital donde los ataques sean cada vez más difíciles de identificar. Pero, además, la inteligencia artificial es muy precisa en la generación de código, así que se está utilizando ya para la automatización y creación de malware indetectable para los mecanismos convencionales.

Figura 8. La inteligencia artificial forma parte de nuestras vidas y seguirá en evolución.

[1] [Aitana López]. Captura de pantalla. Recuperado de: https://businessinsider.mx/ai-influencer-aitana-clueless-agency-tech-spain-2023-11/?r=US&IR=T

Conclusiones:

El estudio de la ingeniería social y de los diversos tipos de engaños y fraudes en internet revela la complejidad y la constante evolución de las amenazas en el mundo digital. Es evidente que las personas maliciosas continúan adaptándose y desarrollando nuevas técnicas para engañar a los usuarios y comprometer su seguridad. Además, la presencia de la inteligencia artificial aumentará la complejidad y capacidades de los ataques. Por lo tanto, es necesario mantenerse informado y, sobre todo, ser conscientes de estos riesgos, pues solo así se podrán implementar medidas de seguridad proactivas para protegerse contra tales amenazas.

AUTOR

ELIER EMANUEL LÓPEZ BASILIO