Plataforma de
Aprendizaje Virtual

Conceptos Fundamentales sobre Ciberseguridad

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 2

La ingeniería social

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 2

La ingeniería social

Este manual se realizó con la colaboración de la Dirección Nacional de Ciberseguridad, perteneciente a la Subsecretaría de Tecnologías de la Información de la Nación.

Ingeniería social

Dentro del campo de la ciberseguridad, existe un término llamado “ingeniería social”. Este concepto hace referencia a diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información privada y confidencial de los usuarios, sin necesidad de intervenir técnicamente un dispositivo o sistema digital. Muchas veces, el ciberatacante no cuenta necesariamente con conocimientos avanzados en informática, pero logra su objetivo a partir de técnicas persuasivas y engañosas.

De esta forma, consigue que las personas le revelen datos confidenciales o contraseñas, o que le abran el acceso a sus dispositivos, cuentas bancarias o información privada.

Generalmente, los ciberdelincuentes que realizan este tipo de ataques engañan a sus víctimas haciéndose pasar por otra persona. Por ejemplo, simulan ser familiares, técnicos de alguna empresa, integrantes de servicios públicos, compañeros de trabajo o alguien de confianza.

Algunos de los canales más utilizados para realizar los ataques de ingeniería social son:

- Llamadas telefónicas.
- Visitas personales al domicilio de las personas.
- Aplicaciones de mensajería instantánea.
- Correos electrónicos.
- Redes sociales.

Como mencionamos, los ataques de la ingeniería social se basan en la manipulación psicológica y el engaño, generando una falsa sensación de confianza en la víctima para poder acceder a la información buscada. La construcción de esa “confianza” puede llevar horas, días e incluso meses; se trata de un proceso en el cual el ciberatacante va estableciendo una relación de familiaridad con la víctima. Por esa razón, es fundamental conocer estos tipos de ciberataques y adquirir el conocimiento necesario para evitar “pisar el palito”.

Algunos de los métodos más comunes para cometer los ataques de la ingeniería social son:

- Hacerse pasar por una persona para obtener algún tipo de información.. Este pedido puede ser tanto desde modales amistosos y empáticos, o a través de un tono intimidante y amenazante.
- Ofrecer a la víctima premios o promociones únicas y limitadas a cambio de sus datos.
- Hacerse pasar por el técnico de la empresa o por la persona responsable de sistemas.
- Invitar a completar formularios para ganar un premio o un producto.
- Ofrecer actualizaciones de navegadores o aplicaciones a través de páginas falsas.

En ciberseguridad, suele considerarse a las personas como el “eslabón más débil” de la cadena de seguridad. ¿Qué significa esto? Que gran parte de los ciberataques logran su objetivo no tanto por las fallas de los softwares antivirus o de las herramientas de seguridad informática, sino debido a “fallas humanas”. La falta de formación y conocimientos en seguridad informática es la principal causa de que las personas sean el punto más vulnerable de la cadena.

Técnicas de la ingeniería social

Existen distintas técnicas de ingeniería social, algunas más utilizadas que otras. Veamos algunas de las más difundidas:

1. Phishing

El phishing es una modalidad de fraude que se utiliza para hacer una suplantación de identidad.. A través de esta técnica, los ciberdelincuentes envían correos electrónicos o mensajes de Whatsapp falsos para obtener información de la víctima. Es decir, utilizan los emails o mensajes con datos falsos, como “anzuelo” para “pescar” contraseñas y datos personales de la víctima. Por ejemplo, pueden solicitar los números y otros datos de tarjetas de crédito, de la obra social, de actualización laboral, contraseñas de sistemas, etc.

¿Cómo suele implementarse este tipo de ataque? El usuario recibe un correo electrónico que aparenta ser la comunicación de un banco, de servicios de pago, de una compra en línea o de proveedores de servicios públicos (luz o gas, turnos de vacunación, aerolíneas, etc). Generalmente, los mensajes suelen solicitar que se completen formularios, que se ingrese en un enlace (que puede redirigir hacia otra página falsa o directamente obtener información con solo clickear) o descargar algún archivo adjunto. De esta forma, los ciberatacantes buscan obtener datos de contraseñas, números de tarjetas de crédito, DNI, nombres de usuario, códigos PIN, etc. Estos datos pueden servirle al ciberdelincuente para hacerse pasar por la víctima, realizar compras o reservas en su nombre, extraer dinero, acceder ilegítimamente a sus cuentas o utilizar su identidad para diversos fines.

Los correos electrónicos y las páginas webs falsas suelen simular la escritura y el estilo gráfico (logos, imágenes) de la empresa o servicio por la que se hacen pasar. Por lo

tanto, no hay que confiarse por el hecho de que esté escrito formalmente o tenga una presentación prolija o similar a la original.

2. Vishing

El término vishing es una combinación de la palabra “voice” (voz, en inglés) y “phishing”, ya que se trata de una estafa que se da a partir de una llamada telefónica. En este tipo de ataques de la ingeniería social, el ciberdelincuente se hace pasar por un familiar, personal de una empresa o de soporte técnico, y de esta forma busca sacarle información personal o valiosa a la víctima.

¿Cómo suele llevarse a cabo este tipo de ataque? Es muy común que la persona atacante llame a la víctima simulando por ejemplo, trabajar en un call center, o que le haga creer que un familiar está en peligro y que necesita ayuda urgente, o bien ofreciendo alguna ayuda económica. A partir de alguna de estas situaciones ficticias, y gracias a algunas técnicas de manipulación, busca conseguir información, ya sean datos personales y/o financieros, nombres de familiares, contraseñas, etc.

Puede ser que el atacante haya conseguido información tuya a través de redes sociales, y por ende tenga algunos datos tuyos o de tus conocidos, que le sirvan para simular conocerte o formar parte de una empresa. No hay que dejarse engañar, y bajo ningún punto brindarles más información.

3. Concursos falsos

Otro de los ataques más comunes de la ingeniería social son las invitaciones a participar en concursos, promociones o encuestas falsas en redes sociales. Los atacantes, haciéndose pasar por empresas, prometen premios, beneficios o cupones de descuento para las personas que participan. Con la excusa del concurso, suelen solicitar la descarga de un archivo o aplicación (con un código malicioso que ataca los dispositivos), pedir dinero para entregar el premio, o robar datos personales, contraseñas, números de tarjetas de crédito, números de celular, etc.

Te recordamos que toda la información oficial relacionada a trámites, servicios y beneficios de organismos públicos nacionales podés encontrarla en el portal del Estado argentino argentina.gob.ar.

¿Cómo prevenir los ataques de la ingeniería social?

Como los ataques de la ingeniería social se basan en técnicas persuasivas y engañosas que apuntan al eslabón más débil de la cadena de seguridad, es decir el ser humano, no existen herramientas informáticas que puedan protegernos. Por esa razón, es fundamental estar alerta para no cometer errores que puedan poner en riesgo nuestra privacidad, identidad e integridad.

A continuación, compartimos algunos consejos para prevenir posibles ataques de la ingeniería social:

1. Nunca entregues información tuya de ninguna índole a personas extrañas que te contacten por teléfono, correo electrónico o redes sociales. Esta es la regla de oro.
Las empresas, los bancos, y los organismos públicos nunca te van a contactar por los medios mencionados para que llenes formularios o brindes algún tipo de información personal.

2. Configurá la privacidad de las redes sociales de forma privada para que tus datos no estén expuestos en forma pública. Aunque parezcan datos inocentes y sin relevancia, los atacantes pueden utilizar cualquier tipo de información (como teléfonos, nombres de familiares o gustos personales) para manipularnos y chantajearnos Y aún así, ser precavidos con la información que compartimos.

3. Usá contraseñas seguras. Cuanto menos obvias y repetidas sean tus contraseñas, más difícil será para los ciberatacantes adivinarlas o acceder a ellas. En las próximas unidades veremos con mayor detenimiento algunos consejos para crear contraseñas seguras.

4. Asegurate de navegar por páginas web seguras. Para eso, verificá que tengan el candadito cerrado con su certificado de seguridad (veremos este punto en detalle en la unidad 4). Además, asegurate que la dirección de Internet, también llamado “url”, sea correcta y que no le falten o sobren letras.

5. Prestá atención a los remitentes de correos electrónicos, mensajes de Whatsapp o redes sociales, y a quienes te llamen telefónicamente. Si recibís mensajes o llamadas de personas

desconocidas, o que hablan en nombre de empresas con las que vos no te contactaste, nunca pases información personal. Es preferible parecer "descortés", antes que brindarle información a personas que puedan poner en riesgo tu privacidad. Si tenés dudas, comunicate con los servicios de atención al cliente antes de contestar cualquier comunicación por correo electrónico (por ejemplo, llamando al número oficial de la empresa).

6. **No descargues archivos adjuntos de remitentes que no conozcas, ni hagas click en enlaces o links dudosos.** Muchas veces, pueden causar la descarga de software malicioso, por lo que es fundamental tener actualizados los antivirus. En las siguientes unidades profundizaremos sobre este tema.

7. **Activar el doble factor de autenticación**. Es una medida de seguridad que agrega una capa adicional de protección a las cuentas en línea y a los dispositivos que usas de forma habitual. Generalmente, se encuentra en el sector de configuraciones.

¿Qué hacer ante un caso de ataque de la ingeniería social?

Si fuiste víctima de un fraude online:

1. Realizá la denuncia ante la dependencia policial o fiscalía más cercana a tu domicilio.

2. No borres, destruyas ni modifiques los mensajes intercambiados con el ciberdelincuente, ni cualquier información relacionada con el hecho. Mantener la evidencia sin alteraciones es importante a los fines de cualquier acción judicial que pudiera iniciarse.

3. Cambiá periódicamente las contraseñas de tus cuentas y servicios, para evitar que los ciberdelincuentes accedan a ellas.

¡Esperamos que hayas disfrutado esta segunda unidad! En la próxima, trabajaremos sobre el concepto de código malicioso, también conocido como malware o software maligno. Veremos algunos de sus principales tipos y cómo identificar su presencia en un dispositivo electrónico.

Plataforma de
Aprendizaje Virtual

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología