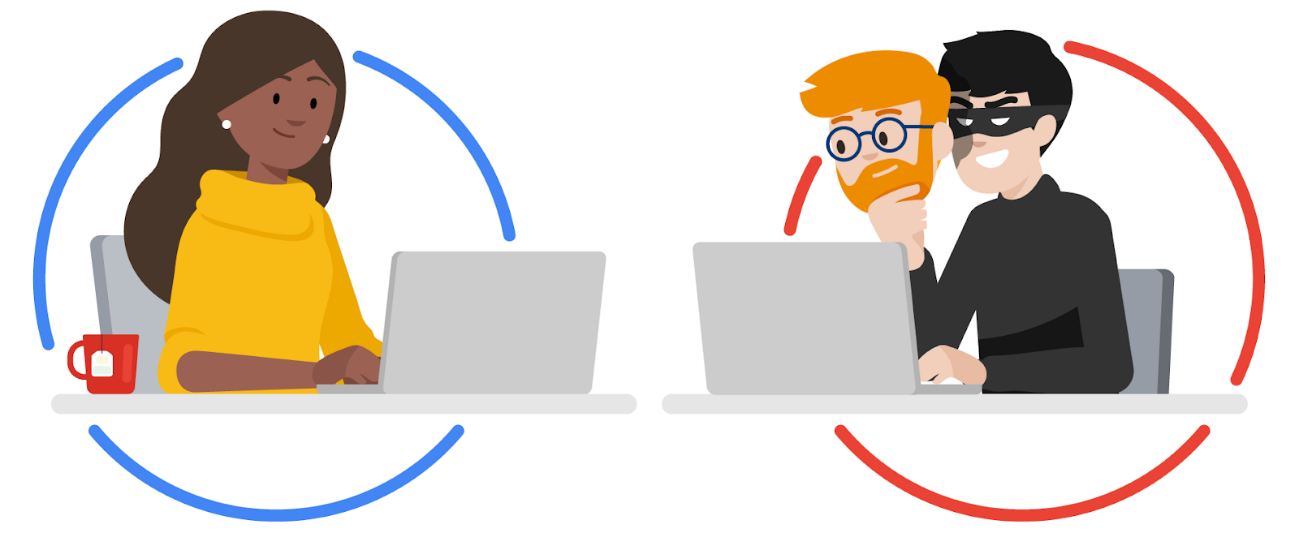
**Tácticas de ingeniería social**

Los ataques de ingeniería social son muy comunes entre los agentes de amenazas. Esto se debe a que, a menudo, es más fácil engañar a las personas para que les proporcionen acceso, información o dinero que explotar una vulnerabilidad de software o red.

Como recordarás, la **ingeniería social** es una técnica de manipulación que aprovecha errores humanos para obtener información privada, acceso a sistemas o bienes de valor. Es un término general que puede aplicarse a una amplia gama de ataques. Cada técnica está diseñada para aprovechar la naturaleza de las personas a ser confiadas y su disposición a ayudar. En esta lectura, aprenderás sobre tácticas específicas de ingeniería social que debes tener en cuenta. También conocerás las formas en que las organizaciones contrarrestan estas amenazas.

**Riesgos de la ingeniería social**



La ingeniería social es una forma de engaño que se aprovecha de la forma en que la gente piensa; de los sentimientos naturales de curiosidad, generosidad y entusiasmo de las personas. Los agentes de amenaza aprovechan esos sentimientos y los utilizan en su contra, al afectar su buen juicio. Los ataques de ingeniería social pueden ser muy dañinos porque suelen ser muy fáciles de lograr.

Uno de los ataques de ingeniería social de más alto perfil de los últimos años fue el [*hack de Twitter* *de 2020*](https://www.dfs.ny.gov/Twitter_Report). Durante ese incidente, un grupo de hackers hizo llamadas telefónicas a empleados de Twitter en las que fingían ser del departamento de TI. Con esta estafa básica, el grupo logró obtener acceso a la red y las herramientas internas de la organización, lo cual les permitió hacerse cargo de las cuentas de usuarios de alto perfil, como políticos, celebridades y empresarios.

Ataques como este son solo un ejemplo del caos que los agentes de amenaza pueden crear mediante el uso de técnicas básicas de ingeniería social. Estos ataques presentan serios riesgos porque no se necesitan habilidades informáticas sofisticadas para ser llevados a cabo. Defenderse contra ellos requiere de un enfoque de múltiples capas que combine los controles tecnológicos con la conciencia del usuario.

**Señales de un ataque**

A menudo, las personas no se dan cuenta de que está ocurriendo un ataque hasta que es demasiado tarde. La ingeniería social es una amenaza muy peligrosa porque, por lo general, permite a los atacantes eludir las defensas tecnológicas que se interponen en su camino. Aunque estas amenazas son difíciles de prevenir, reconocer las señales de un ataque de ingeniería social es clave para reducir la probabilidad de que este se lleve a cabo de forma exitosa.

Estos son tipos comunes de ingeniería social que deben tenerse en cuenta:

* El **cebo** (o baiting) es una táctica de ingeniería social que incita a las personas a poner en riesgo su seguridad. Un ejemplo común es el cebo USB, que se basa en que una persona encuentre una unidad USB infectada y la conecte a su dispositivo.
* La **suplantación de identidad (o phishing)** es el uso de comunicaciones digitales para engañar a las personas de manera que revelen datos confidenciales o instalen software malicioso en sus equipos. Es una de las formas más comunes de ingeniería social, y suele realizarse por correo electrónico.
* **Quid pro quo** es un tipo de cebo que se utiliza para engañar a alguien haciéndole creer que recibirá una recompensa si comparte acceso, información o dinero. Por ejemplo, un atacante puede hacerse pasar por un gestor de préstamos en un banco, llamar a los clientes para ofrecerles una tasa de interés más baja en su tarjeta de crédito y decirles que simplemente tienen que proporcionar los detalles de su cuenta para acceder a la oferta.
* **Tailgating** es una táctica de ingeniería social en la que personas no autorizadas siguen a una autorizada hasta ingresar a una zona restringida. Esta técnica también se conoce como “piggybacking”.
* El **ataque de “agujero de agua”** (o watering hole) es un tipo de ataque en el que un agente de amenaza compromete un sitio web visitado con frecuencia por un grupo específico de usuarios. A menudo, estos sitios están infectados con software malicioso. Un ejemplo es el *ataque Holy Water de 2020*, que infectó varios sitios web religiosos, benéficos y de voluntariado.

Los atacantes pueden usar cualquiera de estas técnicas para obtener acceso no autorizado a una organización. Todas las personas son vulnerables, desde empleados de nivel inicial hasta altos ejecutivos. Sin embargo, puedes reducir los riesgos de los ataques de ingeniería social en cualquier empresa enseñando a las personas a estar prevenidas.

**Fomenta la precaución**

Para generar conciencia, se suele empezar con una capacitación integral en seguridad. En lo que respecta a la ingeniería social, hay tres áreas principales en las que enfocarse, a la hora de enseñar a otras personas:

* **Mantente alerta** ante comunicaciones sospechosas y personas desconocidas, en especial, cuando se trata de correo electrónico. Por ejemplo, busca errores de ortografía y verifica más de una vez el nombre y la dirección de correo electrónico del remitente.
* **Ten cuidado** al compartir información, sobre todo en las redes sociales. Los agentes de amenaza suelen buscar en estas plataformas algún dato que puedan usar para su ventaja.
* **No dejes que te gane la curiosidad** cuando algo parezca demasiado bueno para ser verdad. Esto incluye evitar hacer clic en archivos adjuntos o enlaces en correos electrónicos y anuncios.

**Consejo profesional:** Implementar tecnologías como cortafuegos (firewalls), autenticación de múltiples factores (MFA), listas de bloqueo, filtrado de correo electrónico, entre otras, ofrece una capa de defensa adicional en caso de que alguien cometa un error.

Lo ideal es que la capacitación en seguridad se extienda más allá de los empleados. Enseñarles a los clientes acerca de las amenazas de ingeniería social también es clave para mitigarlas. Y los analistas de seguridad desempeñan un papel importante en la promoción de prácticas seguras. Por ejemplo, una gran parte del trabajo de un analista es probar sistemas y documentar las mejores prácticas para que otros miembros de una organización las sigan.

**Conclusiones clave**

La disposición de las personas a ayudarse entre sí y su naturaleza a ser confiadas es lo que hace que la ingeniería social sea una táctica tan atractiva para los delincuentes. Solo se necesita la intención de hacer un acto de bondad o una acción sin pensar para que un ataque funcione. Los criminales hacen todo lo posible para que sus ataques sean difíciles de detectar. Se apoyan en una gran variedad de técnicas de manipulación para engañar a sus objetivos de modo que les otorguen acceso. Por esa razón, la implementación de controles efectivos y el reconocimiento de los signos de un ataque contribuyen en gran medida a prevenir amenazas.

**Recursos para obtener información adicional**

Estos son dos recursos adicionales que puedes revisar para continuar aprendiendo acerca de las tendencias de ingeniería social y las prácticas de seguridad:

* [OUCH!](https://www.sans.org/newsletters/ouch/) es un boletín informativo mensual y gratuito del Instituto SANS que informa sobre las tendencias de ingeniería social y otros asuntos relacionados con la seguridad.
* [Scamwatch](https://www.scamwatch.gov.au/) es un recurso de noticias y herramientas para reconocer, evitar y denunciar estafas de ingeniería social.