www.mexis.net

COMÓ EVITAR ATAQUES DE INGENIERÍA SOCIAL: ESTRATEGIAS ESENCIALES DE PROTECCIÓN

mexis aggity

La ingeniería social es una de las formas más frecuentes de ciberataques en la actualidad.

Dado que la mayor parte de nuestra vida transcurre en línea, el riesgo de sufrir ataques de ingeniería social aumenta cada día: solo en 2024, más del 80 % de todos los ciberataques en el Reino Unido fueron ataques de phishing , seguidos de suplantación de identidad (pretextos). En comparación, solo alrededor del 14 % de los ciberataques y las infracciones fueron causados por malware.

Los ataques de ingeniería social pueden tener consecuencias devastadoras , que van desde el robo de dinero hasta el robo de identidad o graves violaciones de seguridad con millones de puntos de datos filtrados y sistemas comprometidos. Es fundamental poder reconocer cuándo se está sufriendo un ataque de ingeniería social y cómo responder para prevenir daños graves de manera eficaz.

En este artículo, encontrará explicaciones detalladas de qué es la ingeniería social y cómo funciona , así como sugerencias sobre cómo evitar ataques de ingeniería social tanto a nivel individual como organizacional.

Entendiendo la ingeniería social

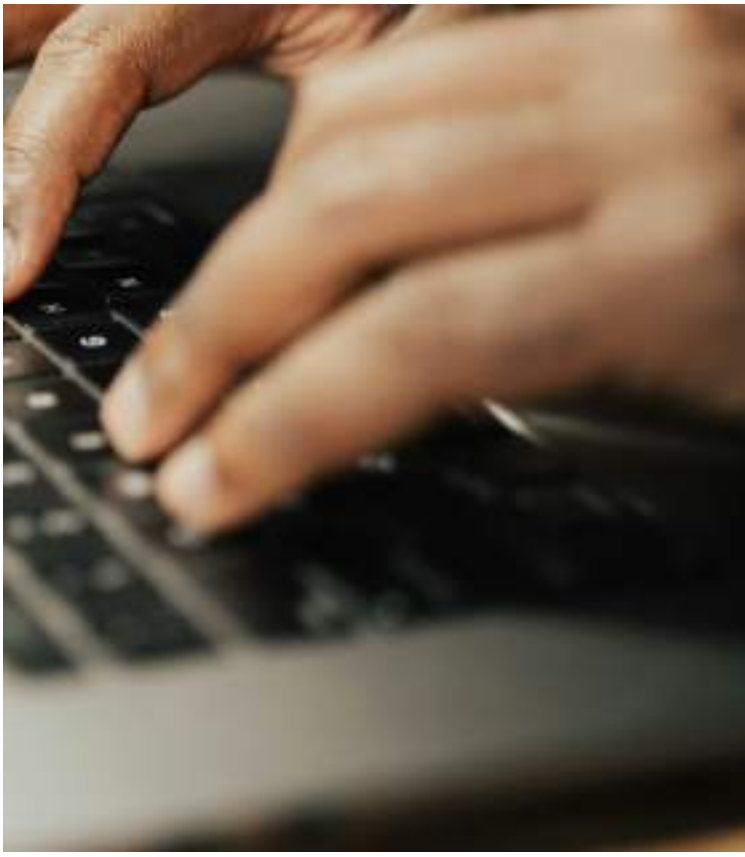
En términos generales, **la ingeniería social es una forma de influir en las actitudes y los comportamientos.** Implica diversas habilidades y técnicas sociales que se utilizan para convencer a alguien de que revele información o realice determinadas acciones. **Sin embargo, en diferentes contextos, la ingeniería social puede significar cosas diferentes.** Aquí, me refiero a la ingeniería social en el contexto de la seguridad de la información .

¿Qué es la ingeniería social?

En el contexto de la seguridad de la información, la ingeniería social es, ante todo, una táctica de manipulación psicológica. Por lo general, alguien puede utilizar ataques de ingeniería social para:

- **Obtener información sobre los sistemas informáticos o acceder a ellos con un objetivo de ataque posterior.** Por ejemplo, alguien puede hacerse pasar **por un agente de atención al cliente a través de una llamada telefónica o de una videollamada para conseguir que la víctima le entregue el control de su dispositivo para infectarlo con malware.** Estos ataques pueden ocurrir tanto en persona como en línea.

- **Utilizan tecnologías combinadas con técnicas de manipulación para lograr otros objetivos,** como el phishing a través de **correo electrónico o mensajes SMS para obtener datos bancarios, números de seguridad social y otra información para robar dinero e identidades.** Estos ataques suelen llevarse a cabo en línea, no en persona.

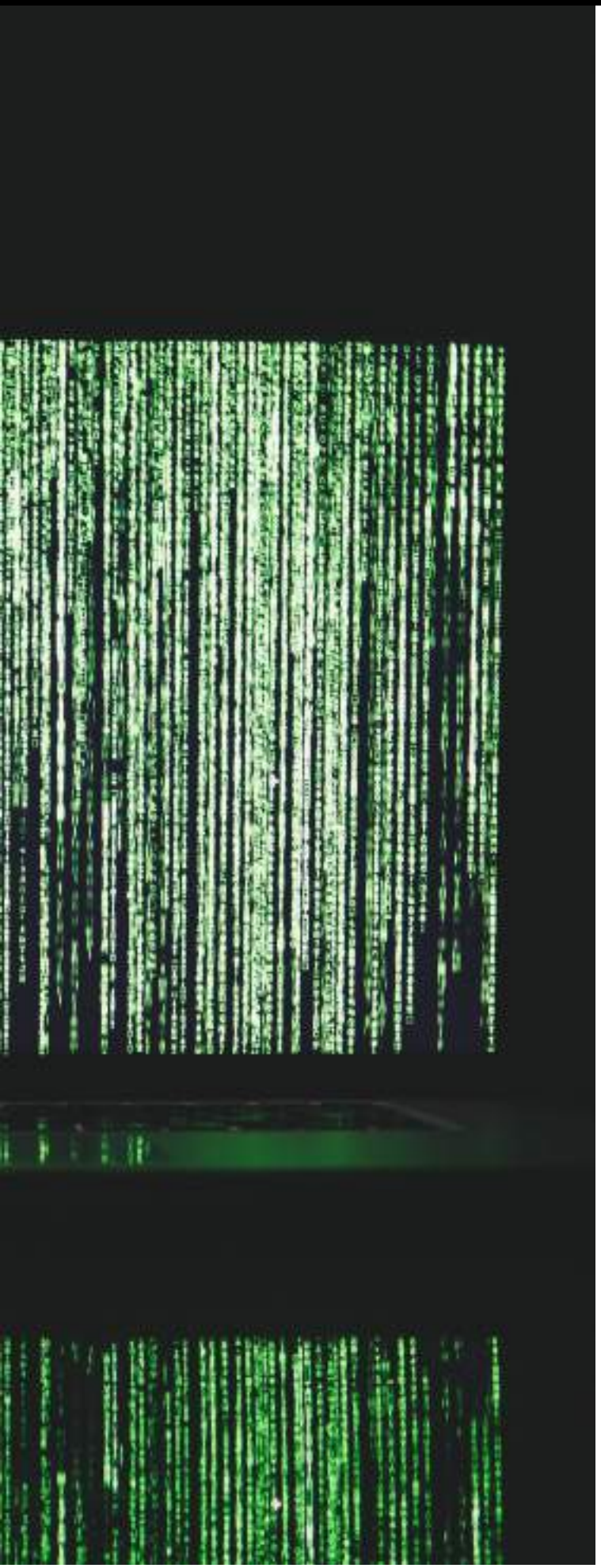


Tipos de ataques de ingeniería social

Existen muchos tipos de ataques de ingeniería social, algunos más frecuentes que otros.

Suplantación de identidad (phishing)

El phishing implica tanto ingeniería social como engaño para **atraer a víctimas desprevenidas para que revelen información confidencial,** como datos bancarios, credenciales y otros.



Los ataques de phishing más comunes se presentan en forma de **correos electrónicos no deseados, mensajes o sitios web que parecen ser fuentes legítimas .** Por ejemplo, pueden parecer un banco, un sitio de redes sociales, un servicio de entrega y otros. Los mensajes suelen parecer urgentes, pero son bastante genéricos al mismo tiempo.

Los ataques de phishing tienen distintos niveles: algunos pueden ser más elaborados y sofisticados. Por ejemplo, en un ataque de phishing personalizado llamado **spear phishing**, un atacante puede hacerse pasar por una persona específica que usted podría conocer o usar otra información disponible públicamente sobre la víctima para hacer que el ataque sea más personal. **El spear phishing tiende a ser más difícil de identificar y tiene una tasa de éxito mucho mayor que los ataques de phishing normales.**

Pretextos

Esta técnica de ingeniería social implica el uso de un **escenario inventado (un pretexto) para ganarse la confianza de la víctima y engañarla para que revele información.** El pretexto suele implicar una investigación por parte del atacante. Por ejemplo, podrían usar su información personal para hacerse pasar por usted u ofrecerle credenciales que demuestren la legitimidad de su pretexto. Un ejemplo de este tipo de ataque puede ser **alguien que se hace pasar por un agente de atención al cliente o un empleado de un banco** para conseguir que revele información personal o le dé acceso a dispositivos y sistemas de seguridad.

Scareware

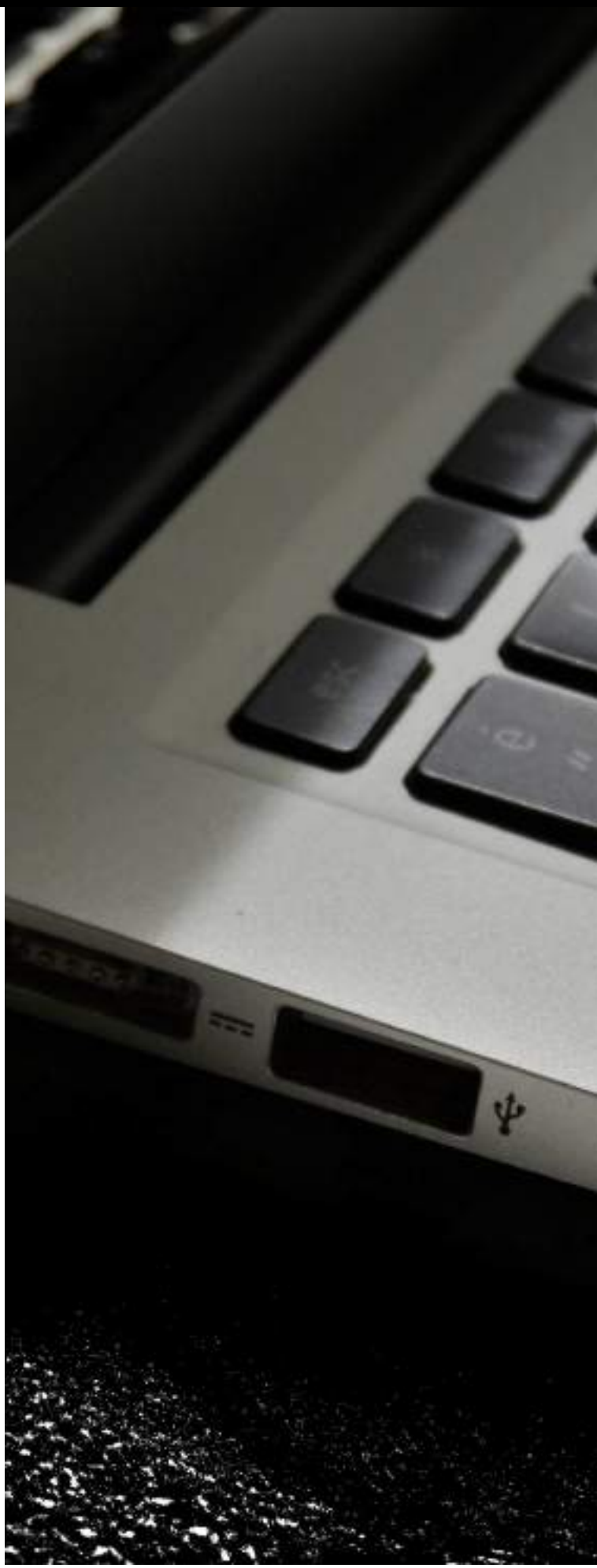
Scareware es un tipo de ataque que utiliza **amenazas, alarmas u ofertas falsas que le piden que tome medidas urgentes.** Por ejemplo, puede aparecer una ventana emergente que le diga que su dispositivo ha sido infectado con malware y un botón que le solicite que instale un software antivirus, que a menudo estará infectado con malware real.

Cebo

Los ataques de cebo, como sugiere su nombre, implican el uso de cebos para despertar la curiosidad de la víctima. En el mundo físico, estos cebos suelen ser **unidades flash USB infectadas con malware** que se dejan en áreas visibles y dispositivos similares que podrían infectar dispositivos con malware. En línea, el cebo adopta la forma de **anuncios atractivos que llevan a sitios web maliciosos** o alientan a los usuarios a instalar aplicaciones infectadas con malware.

Pozo de agua

Los ataques de water-holing **se basan en la confianza que los usuarios tienen en los sitios web que visitan con regularidad.** Un atacante puede observar qué sitios web visita una organización o un individuo con más frecuencia e infectarlos con malware o enlaces maliciosos. Una vez que una víctima hace clic en un enlace o interactúa de alguna otra manera con el sitio infectado, su dispositivo se infecta y el atacante obtiene acceso a todo el sistema de la empresa. Esta estrategia de ingeniería social se ha utilizado para ingresar a sistemas que se consideraban muy seguros.



¿Por qué es efectiva la ingeniería social?

El éxito de la ingeniería social radica en el hecho de que los humanos somos criaturas propensas a cometer errores y, por lo tanto, caemos en tácticas manipuladoras. Según una encuesta sobre ataques de ingeniería social de 2019 , “los ataques basados en las redes sociales se realizan a través de relaciones con las víctimas para jugar con su psicología y emociones. [Son] los más peligrosos y exitosos [ya que] involucran interacciones humanas”. **Estos ataques se basan en el factor humano en lugar de las vulnerabilidades técnicas de los sistemas.** Es más fácil explotar las debilidades humanas como la confianza, la sensación de seguridad y la tendencia a ayudar a los demás o buscar el camino más conveniente.

Los humanos tienden a cometer más errores cuando están distraídos, se sienten presionados, apurados o empáticos. Por eso, los ataques que exigen una acción urgente (como advertencias intermitentes sobre un dispositivo infectado) o piden compasión (como recaudaciones de fondos falsas o alguien que quizás conozcas pidiendo ayuda) tienden a tener altas tasas de éxito.

Además, los ataques de ingeniería social también son más difíciles de detectar y prevenir. **No dejan rastros técnicos** y la mayoría de los métodos de prevención se basan en una formación continua. **La falta de conocimientos técnicos o generales** es otro problema: alguien que no esté familiarizado con el malware o el phishing caerá en un ataque con mayor facilidad. Formar a alguien para que reconozca y resista los ataques de ingeniería social es más complicado que implementar medidas de seguridad técnicas.

Cómo prevenir ataques de ingeniería social

Prevenir ataques de ingeniería social suele ser bastante difícil y las soluciones técnicas no siempre son la respuesta. **Una prevención exitosa depende casi exclusivamente de capacitar a las personas para que reconozcan los signos de un ataque de ingeniería social y lo resistan y lo denuncien.** Por lo tanto, el riesgo de error humano nunca desaparece del todo.

Pero esto no significa que los ataques de ingeniería social no se puedan prevenir. Enseñar a los usuarios **las señales de advertencia y cómo responder** es el primer paso para protegerse a sí mismo, a su empresa y a su información de los actores maliciosos.

Fuente de información: cybernews.com