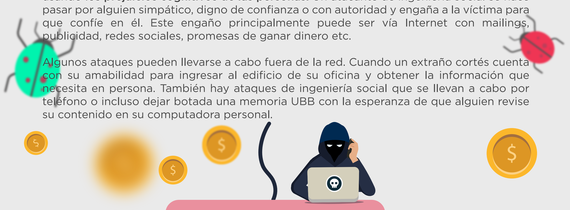
¿Que es la INGENIERÍA SOCIAL?

La **ingeniería social** es el uso de métodos no tecnológicos para **engañar** a las posibles víctimas para que c**ompartan su información personal con un hacker.** Los piratas informáticos utilizan prácticas engañosas para que sus objetivos estén dispuestos a brindarles información tal como: **contraseñas, detalles de cuentas bancarias y otra información personal.**

¿Como ocurre LA INGENIERÍA SOCIAL?

La ingeniería social se manifiesta de muchas maneras y formas. Pero principalmente usando los **prejuicios cognitivos de las personas.** Un atacante de ingeniería social se hace pasar por alguien simpático, digno de confianza o con autoridad y engaña a la víctima para que confíe en él. Este engaño principalmente puede ser vía Internet con mailings, publicidad, redes sociales, promesas de ganar dinero etc.

Algunos ataques pueden llevarse a cabo fuera de la red. Cuando un extraño cortés cuenta con su amabilidad para ingresar al edificio de su oficina y obtener la información que necesita en persona. También hay ataques de ingeniería social que se llevan a cabo por teléfono o incluso dejar botada una memoria UBB con la esperanza de que alguien revise su contenido en su computadora personal.



¿Que tipos de Ingeniería Social existen?

Si bien existe muchos tipos de ataques de ciberseguridad comunes creemos que es necesario conocer cuales son considerados ingeniara social y los métodos más utilizados que no implican contacto con el internet en el momento del ataque.

Phishing

El phishing es un tipo de ataque de ingeniería social en el que las comunicaciones se disfrazan para que parezcan proceder de una fuente de confianza. Estos mensajes –a menudo correos electrónicos– están diseñados para engañar a las víctimas y conseguir que den información personal o financiera. Después de todo, ¿por qué habríamos de dudar de la autenticidad de un mensaje que llega de un amigo, un familiar o una tienda que visitamos a menudo? Las estafas de phishing se aprovechan de esta confianza.

Vishing

El vishing, también conocido como «phishing por voz», es un tipo sofisticado de ataque de phishing. En estos ataques, se suele falsificar un número de teléfono para que parezca legítimo; los atacantes pueden presentarse como personal informático, compañeros de trabajo o banqueros. Algunos atacantes también pueden utilizar cambiadores de voz para ocultar aún más su identidad.

Whaling

El whaling es uno de los ataques de phishing más ambiciosos que existen, con consecuencias catastróficas. Este tipo de ataque de ingeniería social suele estar dirigido a un objetivo de alto valor. A veces se habla de «fraude de los directores generales», lo que da una idea de la marca típica. Los ataques de whaling son más difíciles de identificar que otros ataques de phishing, porque adoptan con éxito un tono de voz apropiado para los negocios y utilizan el conocimiento interno de la industria en su beneficio.

Scareware

El scareware es un tipo de malware que utiliza la ingeniería social para asustar a las personas y conseguir que descarguen un falso software de seguridad o visiten un sitio infectado con malware. El scareware suele aparecer en forma de ventanas emergentes, que dicen ayudar a eliminar un virus informático que supuestamente existe en su dispositivo. Una vez que se hace clic en la ventana emergente, se le redirige a un sitio malicioso o se instala aún más malware sin que lo sepa.

Si sospecha que tiene scareware, u otro tipo de ventana emergente molesta, analice de forma periódica su PC con una herramienta de eliminación de virus de confianza. Analizar periódicamente su dispositivo en busca de amenazas es una buena higiene digital. Puede evitar futuros ataques de ingeniería social, e incluso puede ayudar a mantener sus datos privados a salvo.

Honey trap

Una honey trap es un tipo de esquema de ingeniería social en el que un atacante atrae a una víctima a una situación sexual vulnerable. El atacante aprovecha la situación como una oportunidad para la sextorsión u otro tipo de chantaje. Los ingenieros sociales suelen tender trampas enviando correos electrónicos de spam en los que afirman haber estado «observando a través de su cámara web» o algo igualmente siniestro.

Como pudo observar los ataque de ingeniería social son variados y no siempre son realizados por medio de internet y sus objetivos pueden ser variados sin embargo lo que buscan son la misma cosa encontrar un vulnerabilidad psicológica o física para dar con sus onjetivo.

Si algo parece demasiado bueno para ser cierto, seguramente sea falso

Conoce más sobre casos de ingeneria social escaneando el código QR.

Pasaje N44B E10-26 y Av. 6 de Diciembre
Quito - Ecuador
096 972 9361 / 02 382 7390
www.competencia.com.ec

LA COMPETENCIA S.A
SOLUCIONES TECNOLÓGICAS DESDE 1983