Ingeniería Social
en Seguridad Informática

Resumen por Keiny Pacheco

Objetivos

- **Estudiar el comportamiento humano para saber cómo acceder a ellos en determinados contextos**
- Obtener cualquier tipo de información para acceder a un sistema o escalar privilegios en el
- **Burlar la seguridad de la información con diplomacia**

Los Ingenieros Sociales

1

Son mentirosos profesionales. Conocen su víctima y su entorno, lo cual le permite desempeñar un papel creíble

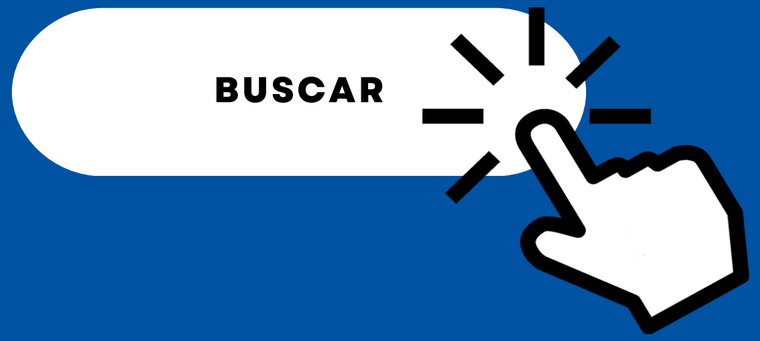
2

Suelen estudiar material relacionado a la psicología y a la sociología

3

Tienen muy desarrollada la escucha activa. De esta manera la víctima se abre al atacante

Maneras de recopilar información en internet



OSINT

Open Source Intelligence

Es toda la información que podemos encontrar en internet, sin tener que hackear o robar para acceder a ella.

Se puede buscar en páginas web personales, páginas de organizaciones policiales, revistas, blogs, redes sociales, la deep web, entre otros.

Datos de la página web

Usando WHOIS podemos consultar información sobre el dominio y los datos de quién registró la página web.

Existen plugins que permiten conocer que tecnologías hay detrás de esta. Conociendo el sistema operativo y lenguajes de programación, podemos mirar que vulnerabilidades podemos atacar.

Muchas veces en las páginas web se encuentran nombres, correros, fotos con información reveladora (pasada por alto), que permiten conocer instalaciones o recursos claves de la víctima

Trashing

Rebuscar información de la basura

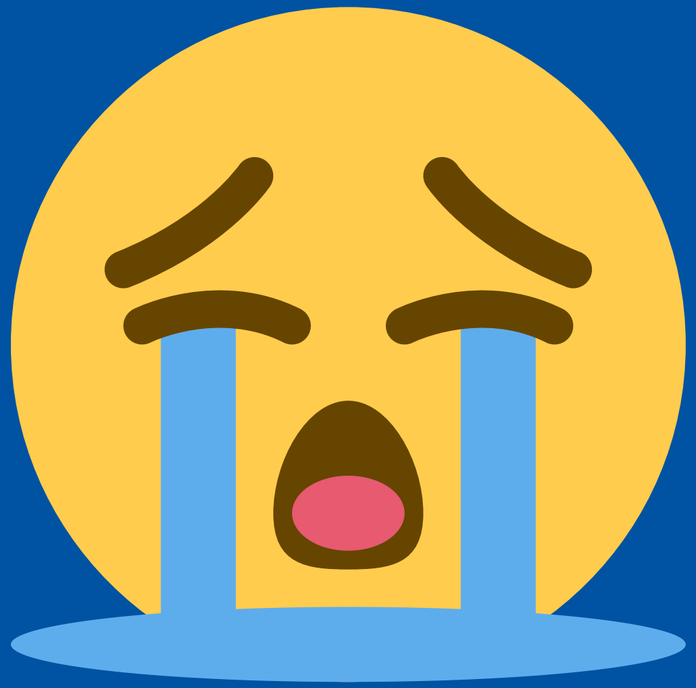
¿Has pensado que sucede cuando botas papeles como facturas, contratos, correos, entre otros? Hay alguien que estará dispuesto a buscarlos en la basura para extraer información. En ciertos lugares no es ilegal hacerlo...

Si nos vamos al mundo digital, cuando eliminas un archivo, en el disco duro también queda almacenada esa información que se puede extraer con software especializado.

Familias y conocidos

Es común encontrar familiares y amigos que no son concientes de estos temas, el compartir información personal y profesional puede perjudicarlos, siendo más fácil vulnerar la seguridad en su entorno y círculo social.

Ellos se preocupan por nosotros, por lo tanto desean ayudarnos a cualquier costo. El ingeniero social, actuará de manera apropiada proponiendo situaciones irreales para obtener información confidencial.



Redes sociales

Podemos encontrar información como correos electrónicos, fechas de cumpleaños, fotos, contactos, ubicaciones, números telefónicos, entre otros.

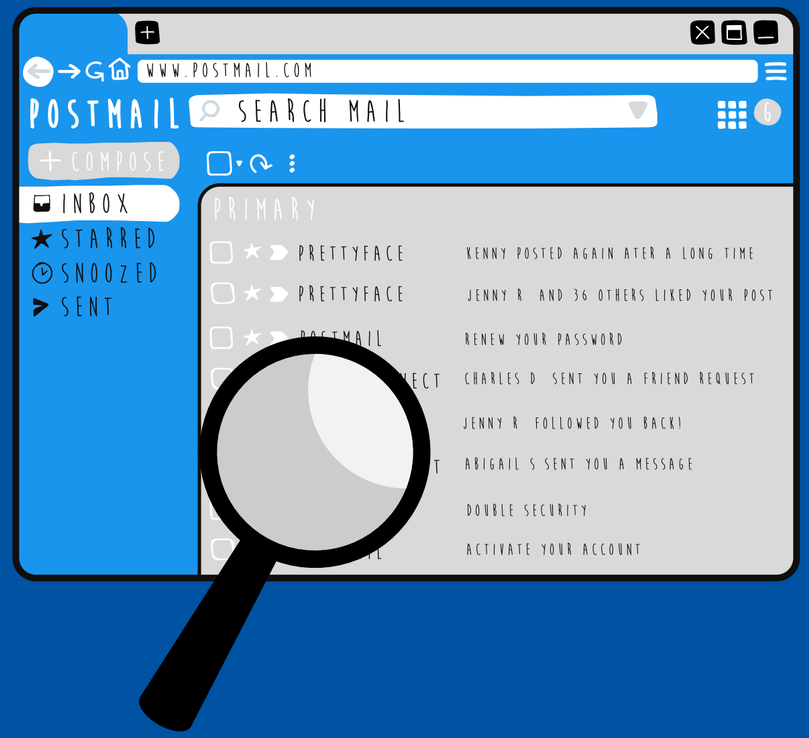
Con esta información podemos conocer a la víctima, ya que se conoce su cultura, sus comportamientos y pensamientos, información que le puede jugar en contra por un ingeniero social.

Correos Electrónicos

Si un ingeniero social tiene acceso a la plantilla de una empresa, podríamos decir que ya tiene todos los correos electrónicos de los mismos.

Esto es porque muchas empresas tienen los correos electrónicos normalizados, por ejemplo nombre.apellido@empresa.com.

Lo cual permite investigar mucho más fácil la organización y establecer estrategias de ataque según el perfil de cada empleado.



Metadatos

Los archivos guardan metadatos que contienen información como el autor, la fecha de edición, datos de contacto, idioma, entre otros, los cuales pueden revelar información de quién lo comparte. Lo ideal, es revisar bien estos metadatos para que no revelen información confidencial.

Lo mismo sucede con las cabeceras de los correos electrónicos.

Metadatos en imágenes

Una fotografía incluye metadatos como el modelo de la cámara, la fecha y hora, las coordenadas de la ubicación del fotógrafo, orientación de la cámara, por mencionar algunas.

Esta información es útil para saber si ciertas fotos fueron manipuladas, o para seguirle el rastro a una persona.

Afortunadamente, las redes sociales suelen borrar estos metadatos, pero en otros sitios como páginas web, las imágenes conservan la información.

Doxing

Cuando se requiere investigar la identidad de una persona detrás de un alias o cuentas de usuario online, estamos haciendo "doxing". Para encontrar dicha información, se usa OSINT como herramienta.

Una de las causas es la justicia social, por lo tanto se quiere desenmascarar a esta persona u organización para que puedan ser judicializados.

También hay otras motivaciones, como conocer quien administra o tiene ciertos privilegios en un sistema, de esta manera armar el plan de ataque.

Herramientas para la ingeniería social

Algunas de ellas...

FOCA

Fingerprinting Organizations with Collected Archives

Es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que escanea. Estos documentos pueden estar en páginas web y pueden descargarse y analizarse con FOCA.

Analiza las relaciones del mundo real entre la información que es públicamente accesible en Internet.

Ofrece la capacidad de conectar fácilmente datos y funcionalidades de diversas fuentes utilizando Transforms. A través de Transform Hub, puede conectar datos de más de 80 socios de datos, una variedad de fuentes públicas (OSINT), así como sus propios datos.

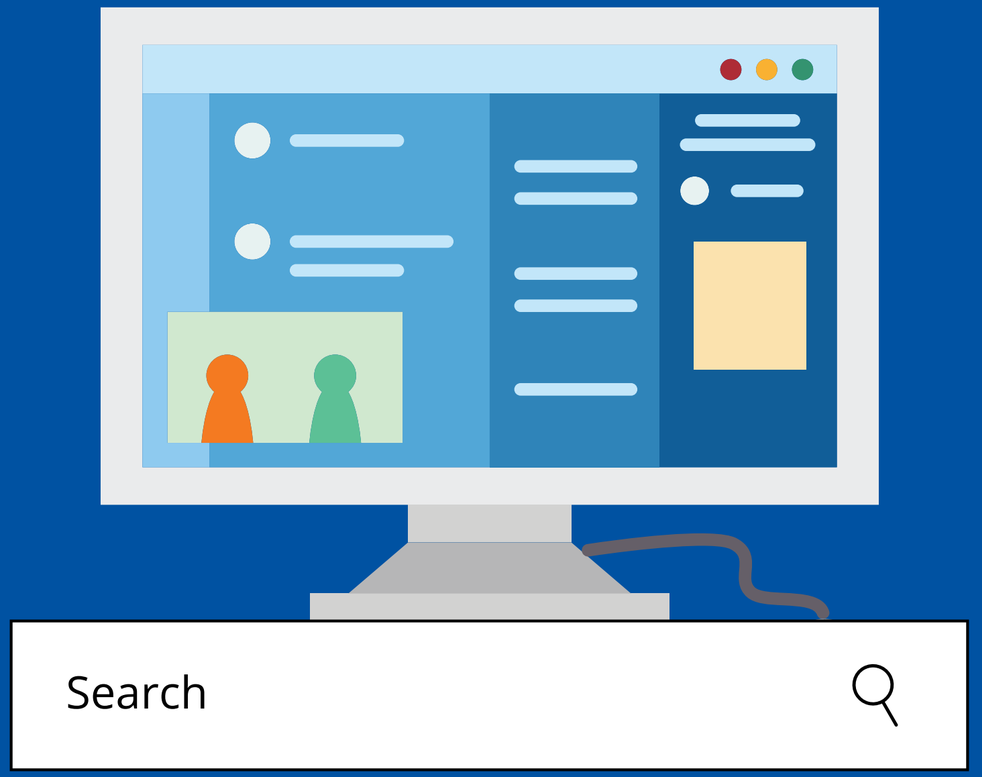
Operadores de búsqueda

Buscadores como Google permiten realizar búsquedas en internet con distintos operadores para filtrar la información.

Por ejemplo, si queremos buscar páginas que en su URL tenga determinada palabra, usamos inurl.

inurl:android

Esto retornará una lista de páginas que tengan la palabra "android".



theHarvester

Aplicación desarrollada por Christian Martorella. La herramienta recopila nombres, correos electrónicos, IP, subdominios y URL mediante el uso de múltiples recursos públicos como motores de búsquedas y ataques de fuerza bruta.

Técnicas de ataques de la ingeniería social

Llamadas telefónicas

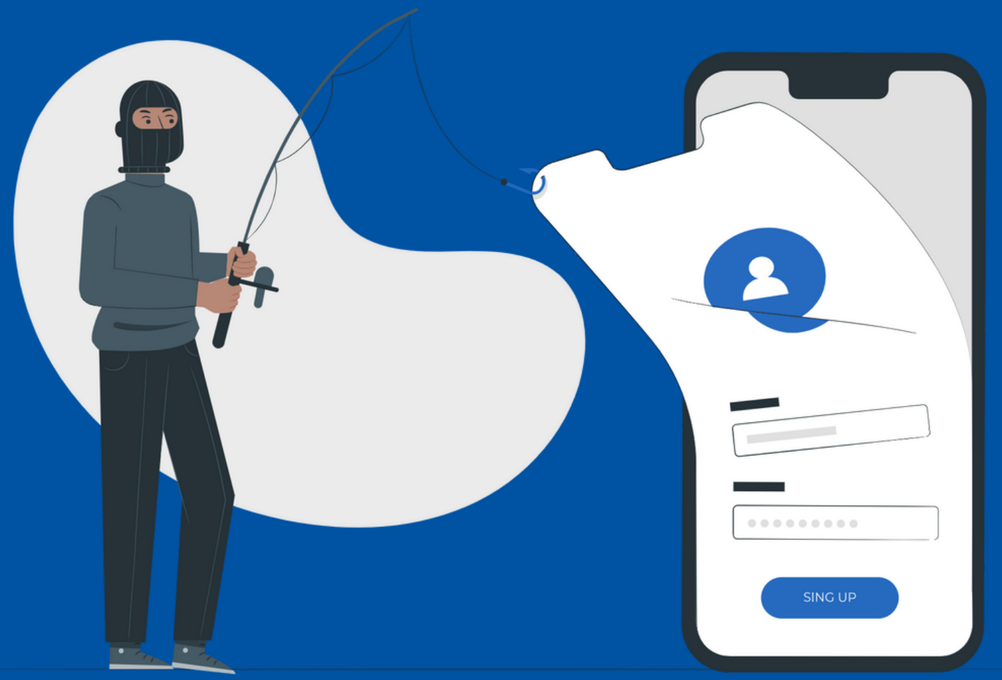
Forma presencial

Chats

Phishing

El atacante replica las identidades corporativas o personales para crear correos electrónicos en los que se pueda captar a la víctima.

El objetivo se "engancha" ya que el correo se le hace familiar y procede hacer click en enlaces, responde enviando información confidencial, abre los archivos adjuntos (estos internamente contienen programas con fines maléficos), entre otros.



Scareware

En forma de ventanas emergentes te avisan que tienes malwares o archivos maliciosos en tu computador y te indican que hagas click en ellos para que descargues aplicaciones que solucionan el problema (antivirus falsos) o ejecutes acciones predeterminadas por el programa (como ir a determinado sitio web infectado)

Muchas personas caen en este tipo de ataques ya que suelen estar en páginas web muy concurridas y suelen ser bastante llamativas.

Dominios engañosos

El atacante tiene dominios, correos electrónicos y cuentas de usuario que tienen alteraciones en algunas de sus letras haciendolo imperceptible para la víctima.

www.banmco.com --- Original
www.banrnco.com --- Alterado

La idea es que no solamente las urls sean imperceptibles, sino también el contenido que contiene la página web o el correo electrónico para que el objetivo crea que está interactuando con la página real.

La técnica del USB

La curiosidad pone en jaque al humano. Esta técnica consiste en dejar abandonado una usb con malware para que el objetivo la encuentre. La curiosidad le hará conectar la usb a un computador para ver de quién es y qué contiene. Este irá más allá y abrirá los archivos; esa será la oportunidad perfecta para comenzar a ejecutar el malware.

El fallo informático

El ingeniero social, generalmente por llamadas, se hace pasar por técnico en sistemas y emplea frases como "hay que actualizar su computador", "hay que reparar tal hardware", ya que sus víctimas son personas que no tienen un conocimiento amplio en computadores.

Aprovechandose de ello, hace que la víctima descargue software malicioso para "solucionar el problema", o la confianza va más allá que este le comparte información confidencial, sin levantar sospechas.

Prevención ante la ingeniería social

1

Concienciar sobre la seguridad en cada puesto de trabajo o vida personal

2

Mantenernos actualizados para prevenir riesgos y minimizar daños

3

Crear registros (logs) y controlar accesos a los sistema

4

Guardar copias de seguridad para evitar perder la base de datos

5

Usar comunicación segura: VPN, conexiones SSL. Tener una lista de apps permitidas

6

No usar recursos de la empresas para actividades privadas.

7

Tener un plan de contigencia en caso de ataque

“

Los humanos somos vulnerables, entonces las empresas también lo son

¡Gracias!

Resumen por Keiny Pacheco