Social Engineering 101®

Student Handbook

Certified by csASC

Social Engineering 101™ Foundations SE101-FNS

csASC CYBERSECURITY ASSOCIATION COUNCIL

Copyright and Disclaimer

Social Engineering 101®| r1.5

Copyright

Disclaimer

Information provided about the course, modules, topics and any services for courses including simulations or handouts, are an expression of intent only and are not to be taken as a firm offer or undertaking. The Publisher reserves the right to discontinue or vary or maintain such course, modules, topics, or services at any time without notice and to impose limitations on enrolment in any course.

The course materials provided may have hypertext links to a number of other web sites as a reference to users. This service does not mean that the publisher endorses those sites or material on them in any way. The publisher is not responsible for the use of a hypertext link for which a commercial charge applies. Individual users are responsible for any charges that their use may incur.

The information in this course is written using a blend of British and American English. Although every effort has been made regarding the usage of correct spelling, punctuation, vocabulary, and grammar with regard to the Standard English, the publisher accepts no responsibility for any loss or inconvenience caused due to the regional differences in the usage of the spanish language.

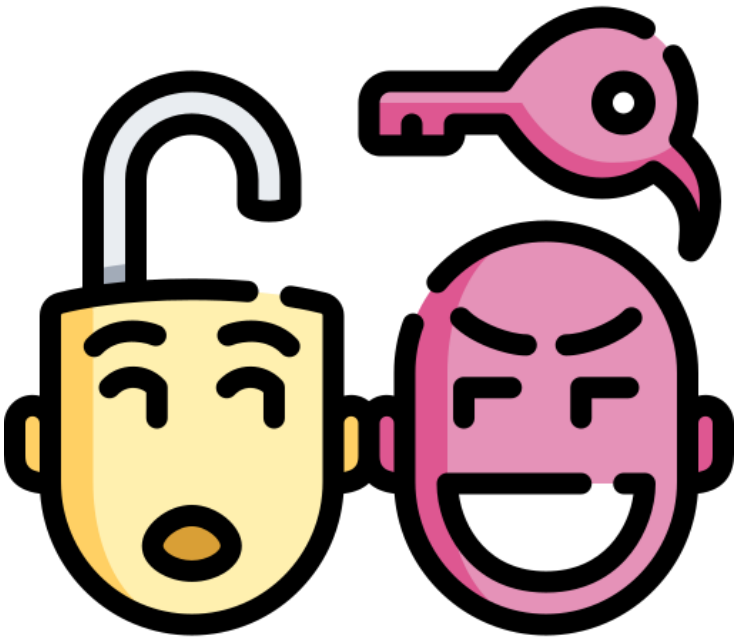
Contenido

Prólogo

En el campo de la seguridad de la información, la **Ingeniería Social** es la práctica para obtener datos confidenciales a través de la manipulación psicológica de usuarios legítimos**. La técnica se puede utilizar para conseguir información, acceso o privilegios en sistemas,** que permitan realizar algún acto que perjudique o exponga a una persona o empresa a riesgos y abusos.

El principio en el que se sustenta la ingeniería social afirma que en cualquier sistema los usuarios son el eslabón débil de la cadena, esto incrementa si la tecnología de la organización se encuentra insegura y facilita a un atacante crear un escenario más creíble.

En la práctica se utiliza el teléfono o Internet para engañar a la gente, por ejemplo, al simular ser el empleado de un banco o de una empresa, un compañero de trabajo, un técnico o un cliente y así obtener información. A través de Internet suelen enviarse solicitudes para renovar credenciales de acceso a sitios, e-mails falsos que piden respuestas e incluso las famosas cadenas que llevan a revelar información sensible o a violar políticas de seguridad.



Introducción

Vamos a conocernos

Preséntese siguiendo el siguiente formato:

- Nombre
- Compañía
- Rol y antecedentes
- Familiaridad con los conceptos Ciberseguridad y sus prácticas
- Experiencia en desarrollo de aplicaciones, desarrollo de infraestructura y/o operaciones
- Expectativas de este curso

Visión General

Este curso está orientado a profesionales y organizaciones que desean entender y concientizar a sus colaboradores, ante las amenazas que existen en el mundo de la tecnología y prepararlos para las técnicas de engaño usadas por los ciberdelincuentes para obtener acceso y/o control de sistemas y/o información.

Este es el primer escalón de varios, si empieza con pasos firmes, no tendrá problema cuando este en los escalones más altos, he ahí la vital importancia de este curso.

Objetivo

La principal defensa contra la ingeniería social es educar y concientizar a los usuarios en el uso y el cumplimiento de políticas de seguridad. En los años 80, la ingeniería social tuvo un impacto muy grande debido a que la gente era más inocente, los sistemas eran más vulnerables y las leyes relacionadas con la información eran menos rigurosas o inexistentes.

El factor humano es el eslabón más débil de la seguridad informática, no hay un solo equipo en el mundo que no dependa de un ser humano, esto es una vulnerabilidad universal e independiente de la plataforma tecnológica. Es por eso, que se debe dar un tratamiento especial e independiente de la tecnología.

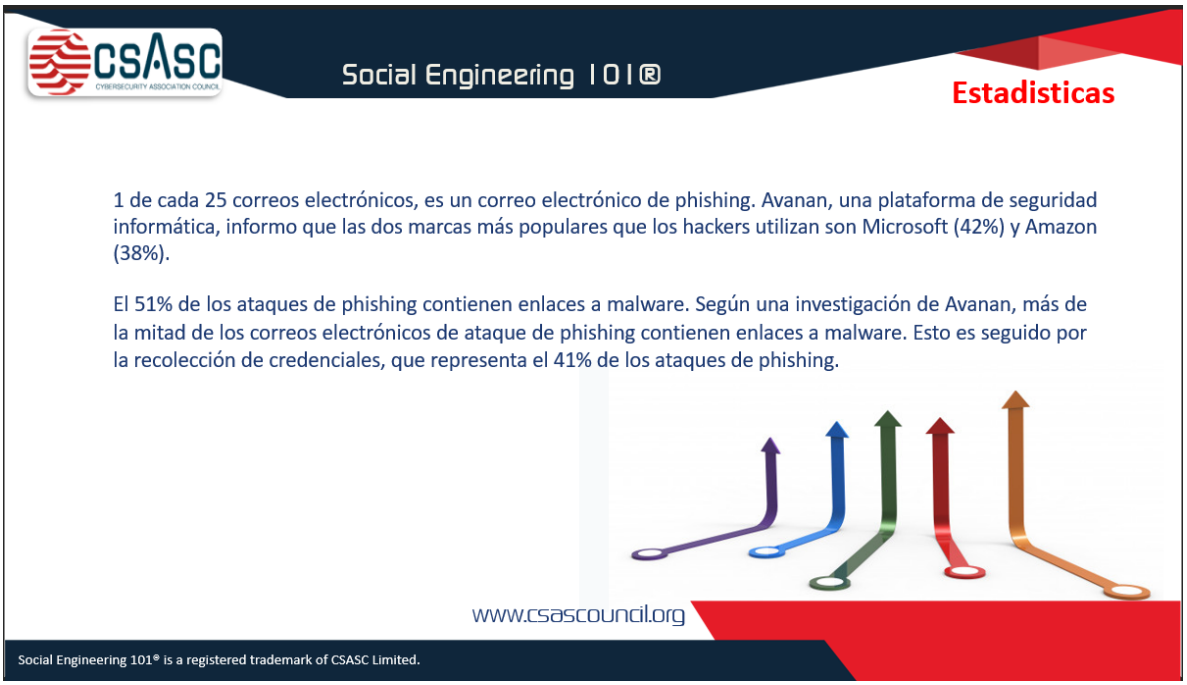
¿Qué es la ingeniería social?

La Ingeniería Social (Social Engineering) es una mezcla de ciencia, psicología y arte. Si bien es sorprendente y compleja, también es bastante simple.

Lo definimos como:

"Cualquier acto que influye en una persona para tomar una acción que puede ser o no en su mejor interés".

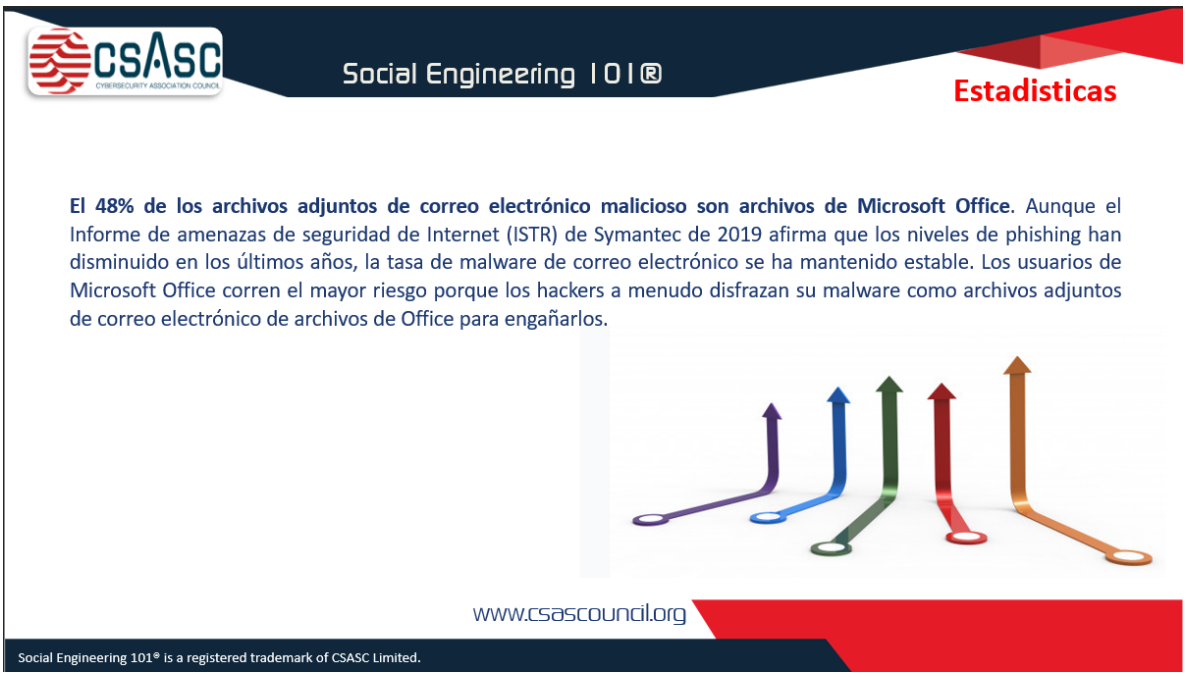
La idea detrás de la ingeniería social es aprovechar las tendencias naturales y las reacciones emocionales de una víctima potencial.



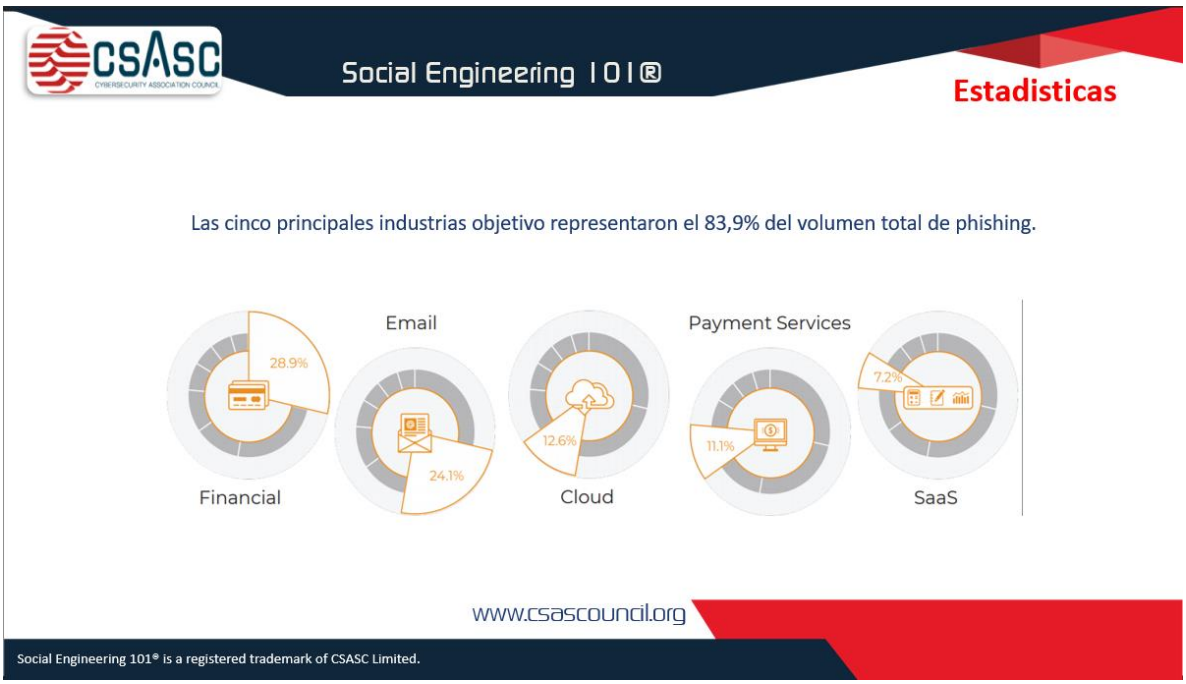
Estadísticas

1 de cada 25 correos electrónicos, es un correo electrónico de phishing. **Avanan**, una plataforma de seguridad informática, informo que las dos marcas más populares que los hackers utilizan son **Microsoft** (42%) y **Amazon** (38%).

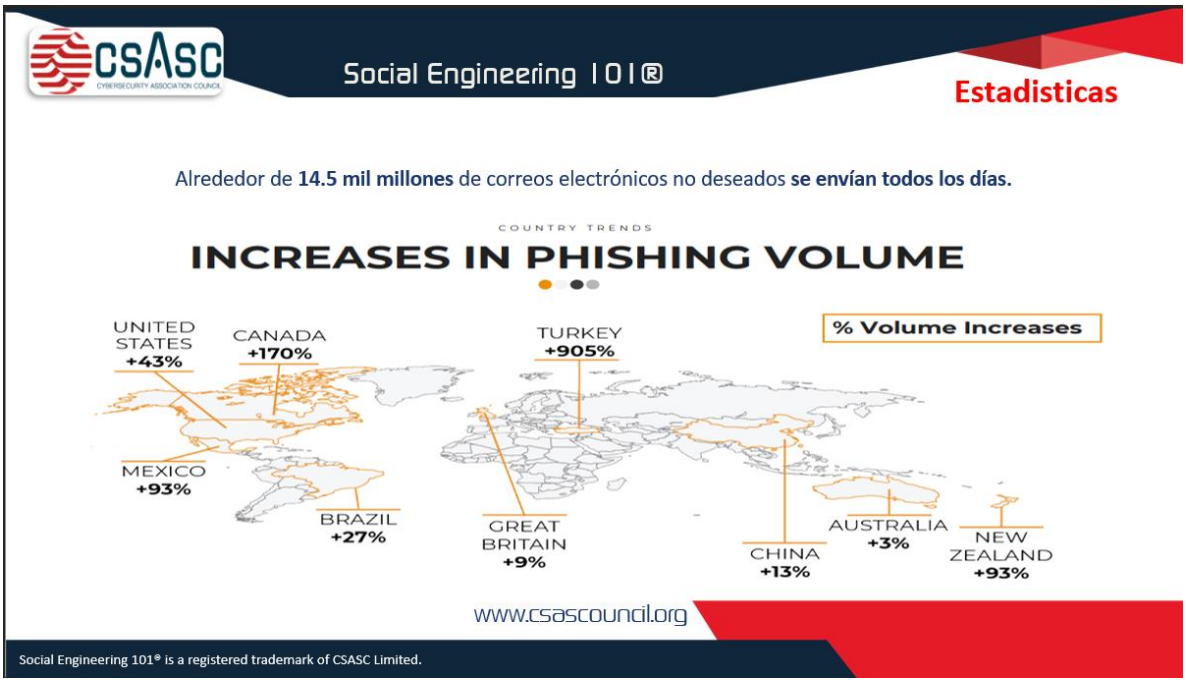
El 51% de los ataques **de phishing contienen enlaces a malware**. Según una investigación de **Avanan**, más de la mitad de los correos electrónicos de ataque de phishing contienen enlaces a malware. Esto es seguido por la recolección de credenciales, que representa el 41% de los ataques de phishing.



El 48% de los archivos adjuntos de correo electrónico malicioso son archivos de Microsoft Office. Aunque el Informe de amenazas de seguridad de Internet (ISTR) de Symantec de 2019 afirma que los niveles de phishing han disminuido en los últimos años, la tasa de malware de correo electrónico se ha mantenido estable. Los usuarios de Microsoft Office corren el mayor riesgo porque los hackers a menudo disfrazan su malware como archivos adjuntos de correo electrónico de archivos de Office para engañarlos.



Las cinco principales industrias objetivo representaron el 83,9% del volumen total de phishing.



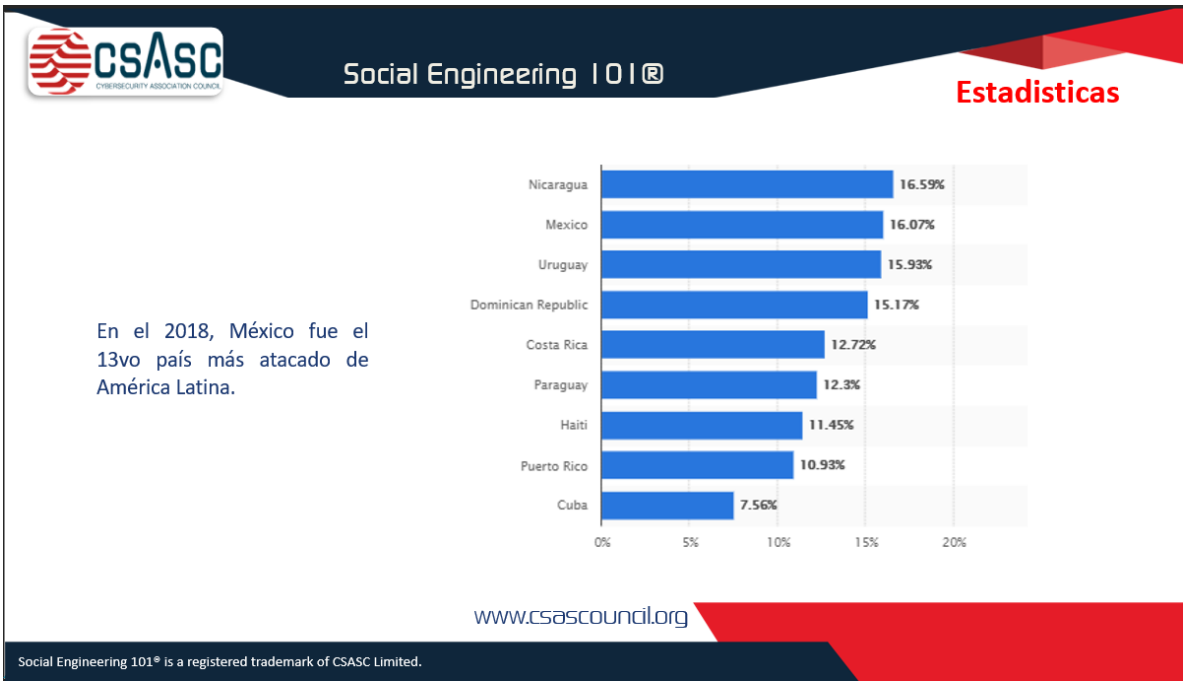
Alrededor de **14.5 mil millones** de correos electrónicos no deseados **se envían todos los días.**

Según **Intel**, el 97% de las personas en todo el mundo no pueden identificar un correo electrónico de phishing sofisticado.

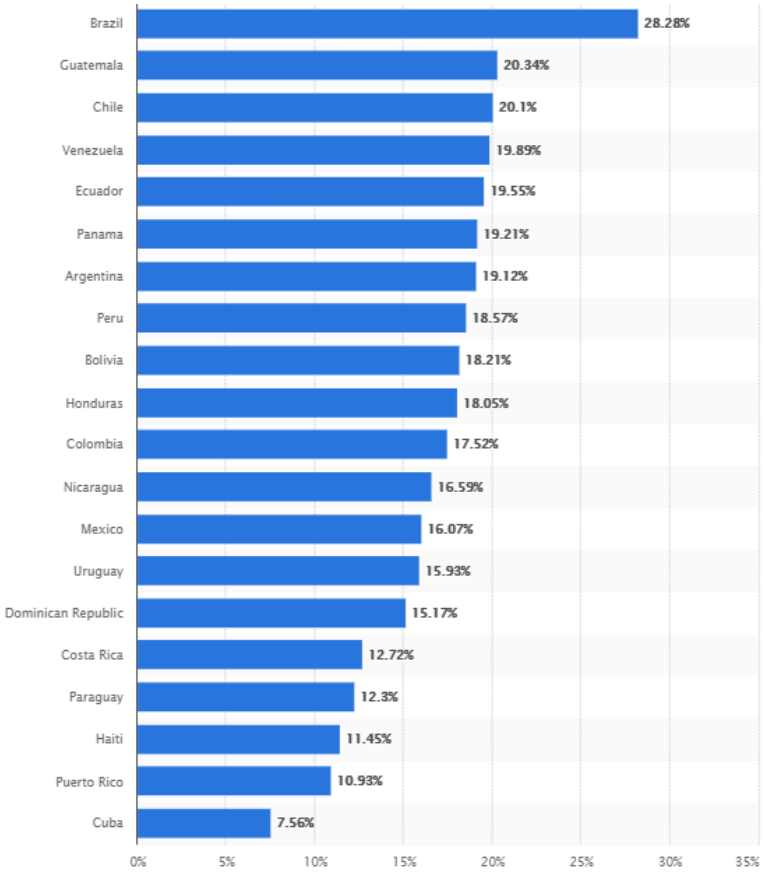
Según **Check Point Software Technologies LTD**, las fuentes más comunes de ingeniería social son los correos electrónicos de phishing.

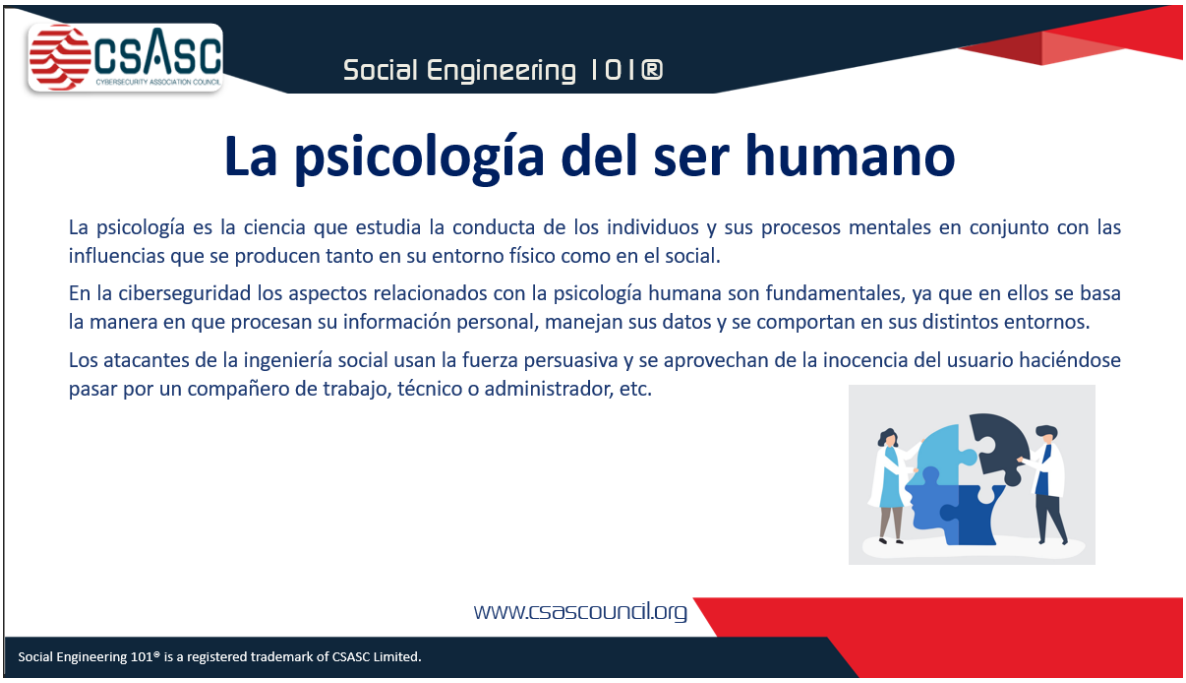
Check Point Software Technologies LTD, también encontró que solamente el **86% de las empresas reconocen a la ingeniería social como una preocupación creciente**, mientras que el 51% de las organizaciones cita las ganancias financieras como la motivación principal de ataques, seguido por ventajas competitivas y venganzas. Además, 48% de las empresas han reconocido ser víctimas de la ingeniería social más de 25 veces en los últimos años, por último, el 34% de las empresas no entrena a sus empleados ni tienen políticas de seguridad para prevenir técnicas de ingeniería social.

Las empresas estiman que cada incidente de seguridad cuesta desde $25,000 dólares hasta más de $100,000 dólares.



1. En el 2018, México fue el 13vo país más atacado de América Latina.



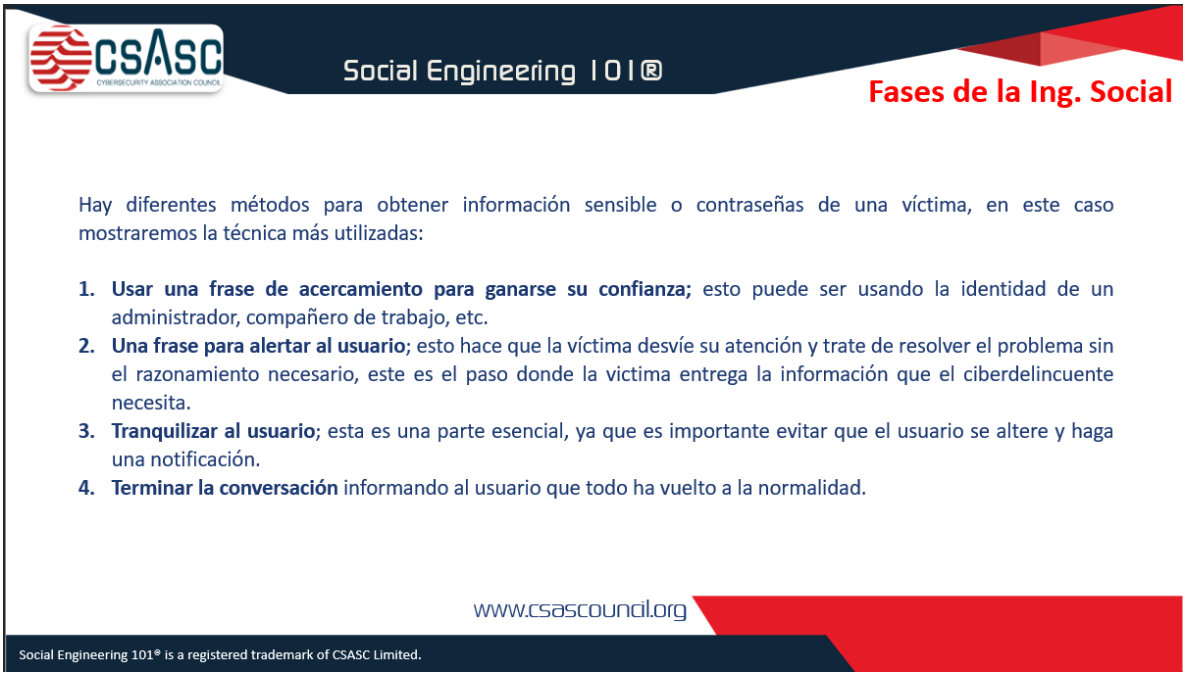


La psicología del ser humano

La psicología es la ciencia que estudia la conducta de los individuos y sus procesos mentales en conjunto con las influencias que se producen tanto en su entorno físico como en el social.

En la ciberseguridad los aspectos relacionados con la psicología humana son fundamentales, ya que en ellos se basa la manera en que procesan su información personal, manejan sus datos y se comportan en sus distintos entornos.

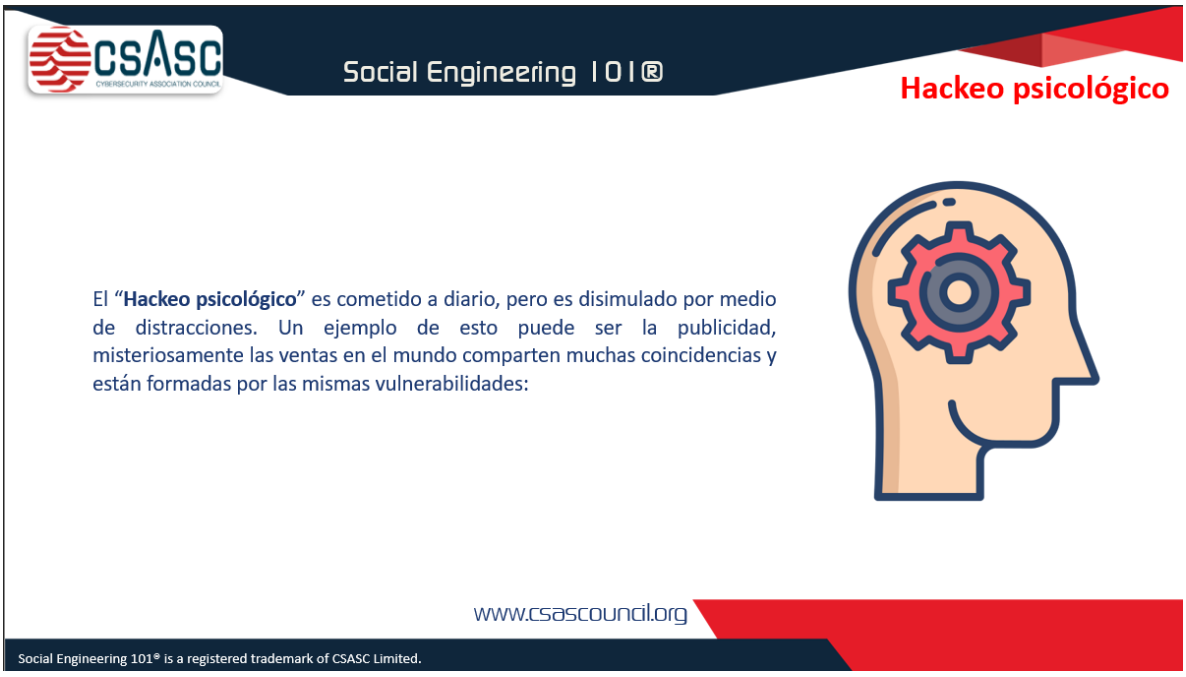
Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, técnico o administrador, etc.



Hay diferentes métodos para obtener información sensible o contraseñas de una víctima, en este caso mostraremos la técnica más utilizadas:

1. **Usar una frase de acercamiento para ganarse su confianza;** esto puede ser usando la identidad de un administrador, compañero de trabajo, etc.
2. **Una frase para alertar al usuario**; esto hace que la víctima desvíe su atención y trate de resolver el problema sin el razonamiento necesario, este es el paso donde la victima entrega la información que el ciberdelincuente necesita.
3. **Tranquilizar al usuario**; esta es una parte esencial, ya que es importante evitar que el usuario se altere y haga una notificación.
4. **Terminar la conversación** informando al usuario que todo ha vuelto a la normalidad.

Cuando un usuario es presionado y se altera, no piensa con claridad, es una reacción humana, el cerebro lo trata de entender y buscar una solución.

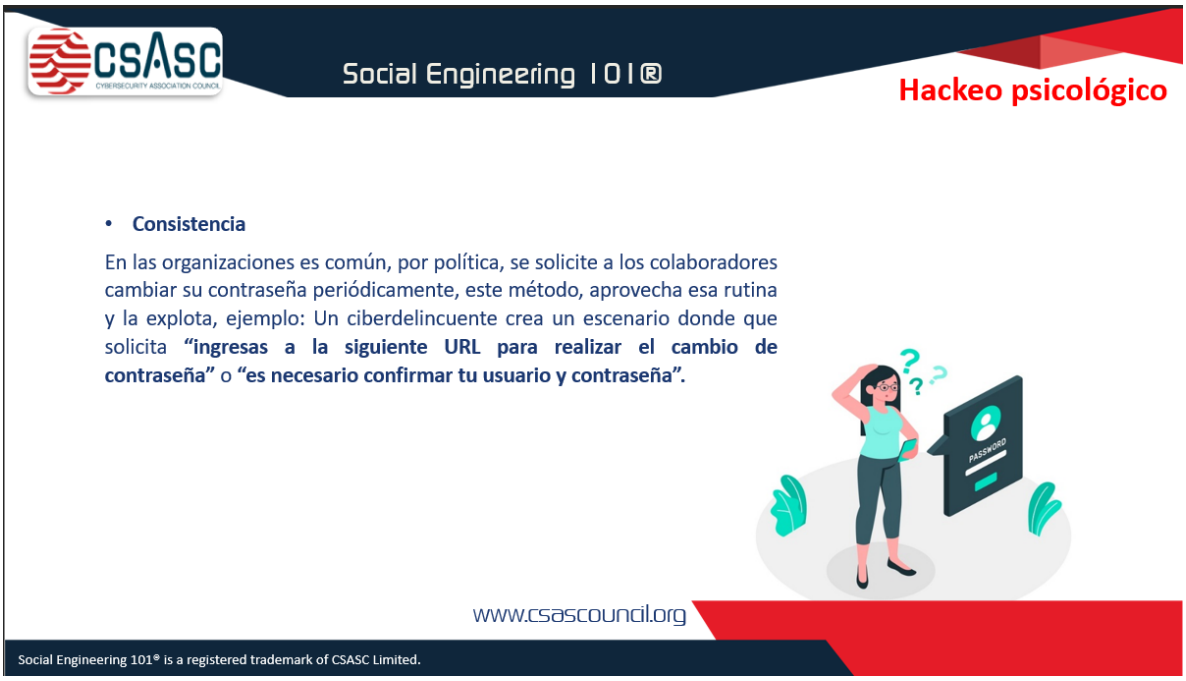


¿Algún ejemplo?

El "**Hackeo psicológico**" es cometido a diario, pero es disimulado por medio de distracciones. Un ejemplo de esto puede ser la publicidad, misteriosamente las ventas en el mundo comparten muchas coincidencias y están formadas por las mismas vulnerabilidades:

- **Urgencia**

¡¡¡¡Compra ya!!!!, Ultimas unidades!!!, por tiempo limitado: es una de las formas más comunes de vender algo, en este caso es igual, pero con otras palabras; "Regístrate y opten 1 mes gratis en cierto servicio", "Enviá este mensaje a 10 personas para obtener algo en la aplicación o servicio" y los formularios tienen lo típico, correo, contraseña, nombre, etc, con esta información se crean bases de datos de las victimas que ayuden a los cibercriminales a cometer suplantación de identidad, robo de usuarios y contraseñas de servicios legítimos e incluso obtener información confidencial para fines ilícitos.



- **Consistencia**

En las organizaciones es común, por política, se solicite a los colaboradores cambiar su contraseña periódicamente, este método, aprovecha esa rutina y la explota, ejemplo: Un ciberdelincuente crea un escenario donde que solicita **"ingresas a la siguiente URL para realizar el cambio de contraseña"** o **"es necesario confirmar tu usuario y contraseña".**

- **Confianza**

Establecer lazos de confianza, permite obtener información que difícilmente lograrían extraer de sistemas con robustos controles de seguridad, como información estratégica, financiera o confidencial de una organización, esto es aprovechado por cibercriminales que normalmente muestran falsa afinidad en temas de interés que investigaron en redes sociales de su víctima.

Lo que las páginas web saben de nosotros

Hoy en día la sociedad está conectada a la red con intenciones profesionales o de ocio, pero sin saberlo, **puede estar entregando más información de la necesaria,** los sitios Web en la mayoría de los casos acceden a estos datos sin ninguna autorización o notificación, aunque la mayoría de los datos son conjeturas fundamentadas y no se consideran precisas.

Deviceinfo

Device Info es una herramienta de prueba de seguridad, de privacidad y solución de problemas del navegador web, se especializa en la información que entregan las computadoras personas y dispositivos móviles al conectarse a Internet, basta con acceder a esta liga para consultar la información, esto, puede estar siendo ejecutado por cualquier sitio web que se visita.