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

Trade Marks

Social Engineering 101® is a registered trademark of CSASC Limited.

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.

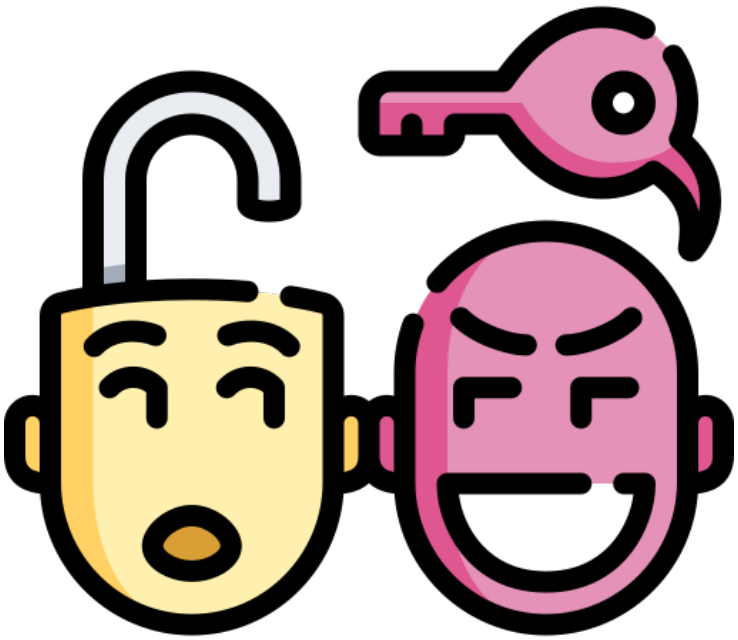
Contenido

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.

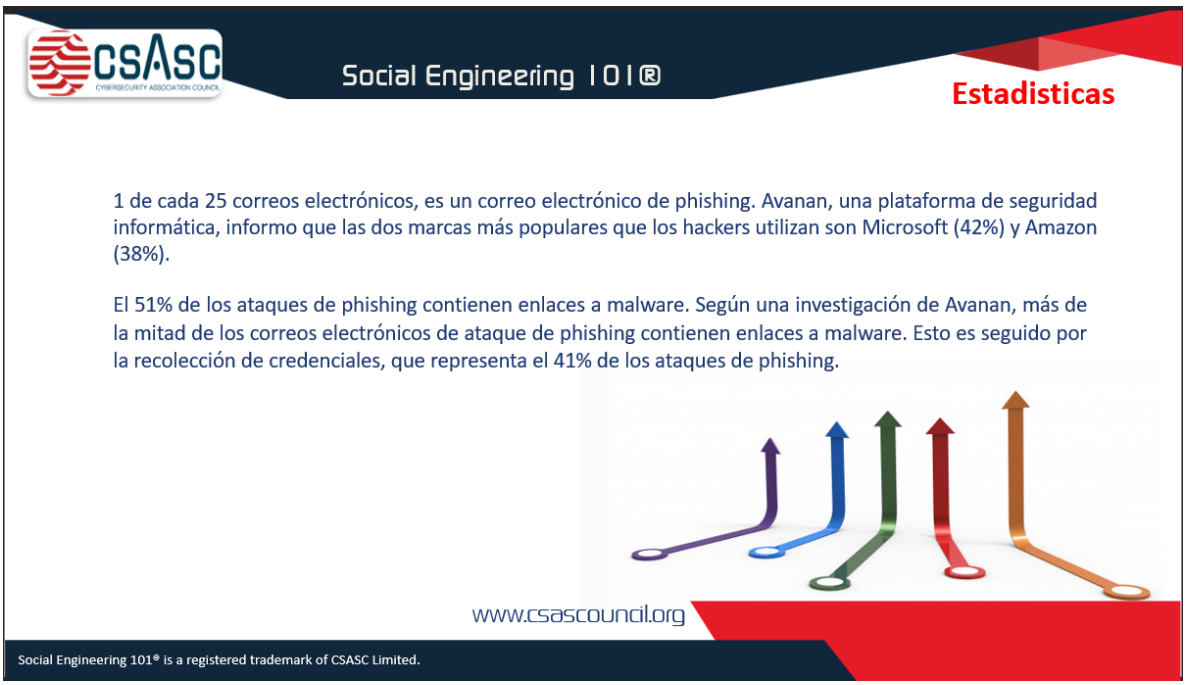
¿Qué es la ingeniería social?

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".

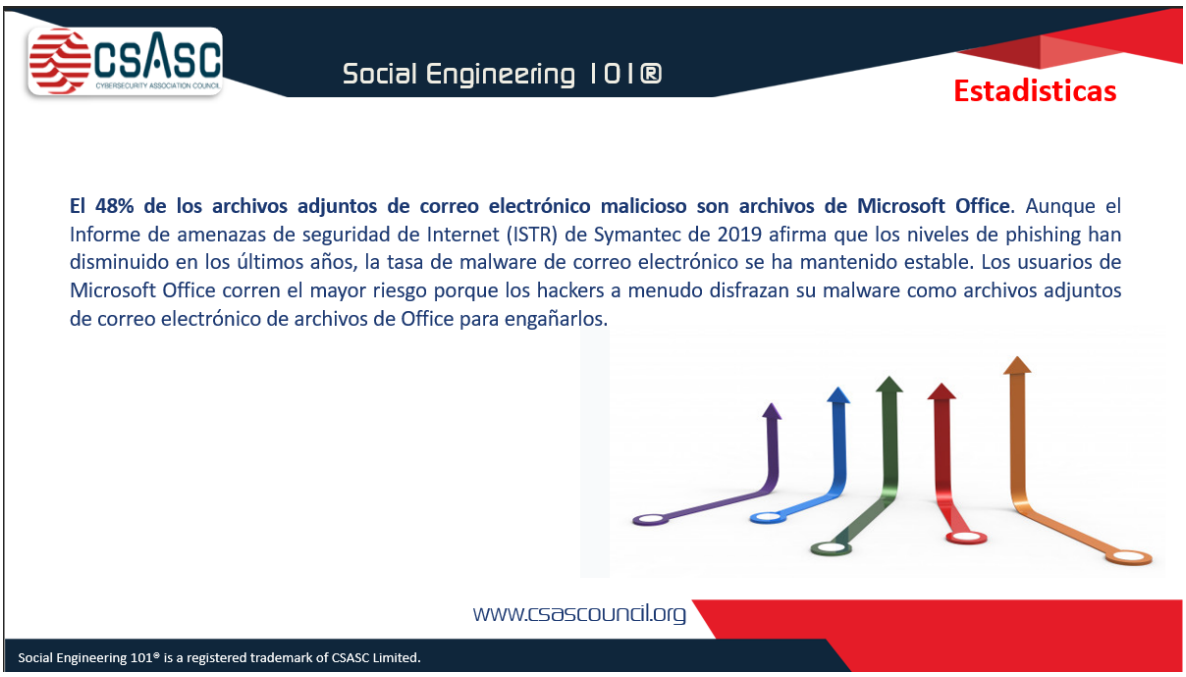
La idea detrás de la ingeniería social es aprovechar las tendencias naturales y las reacciones emocionales de una víctima potencial.



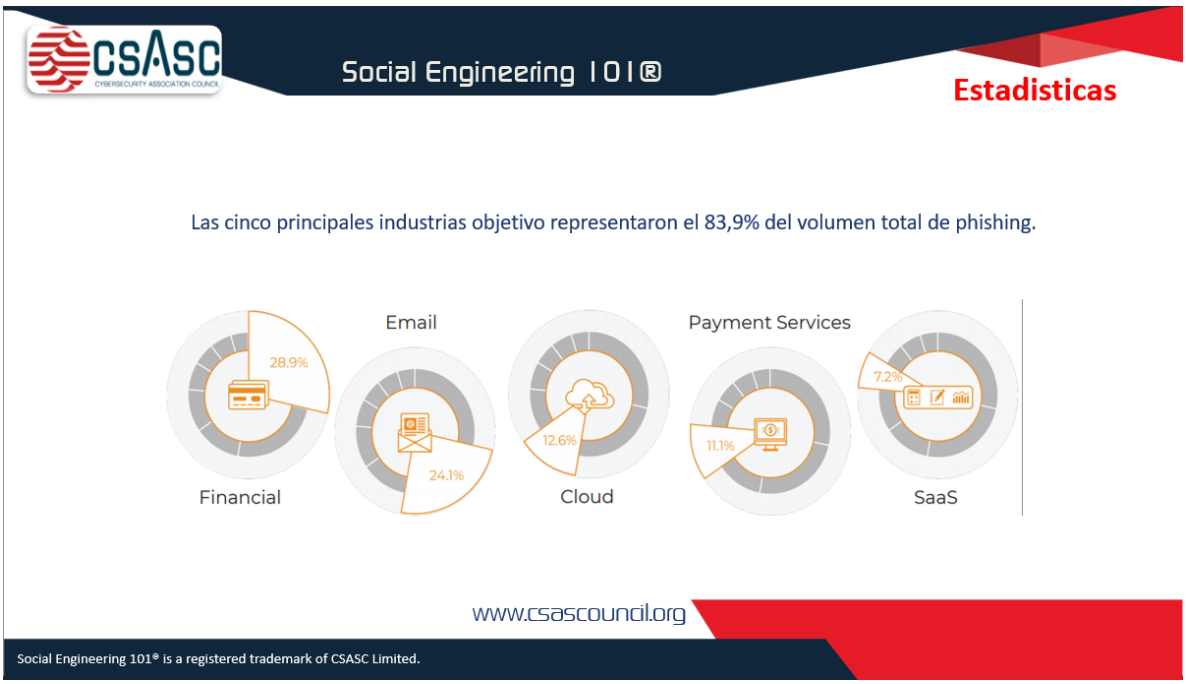
Estadísticas

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%).

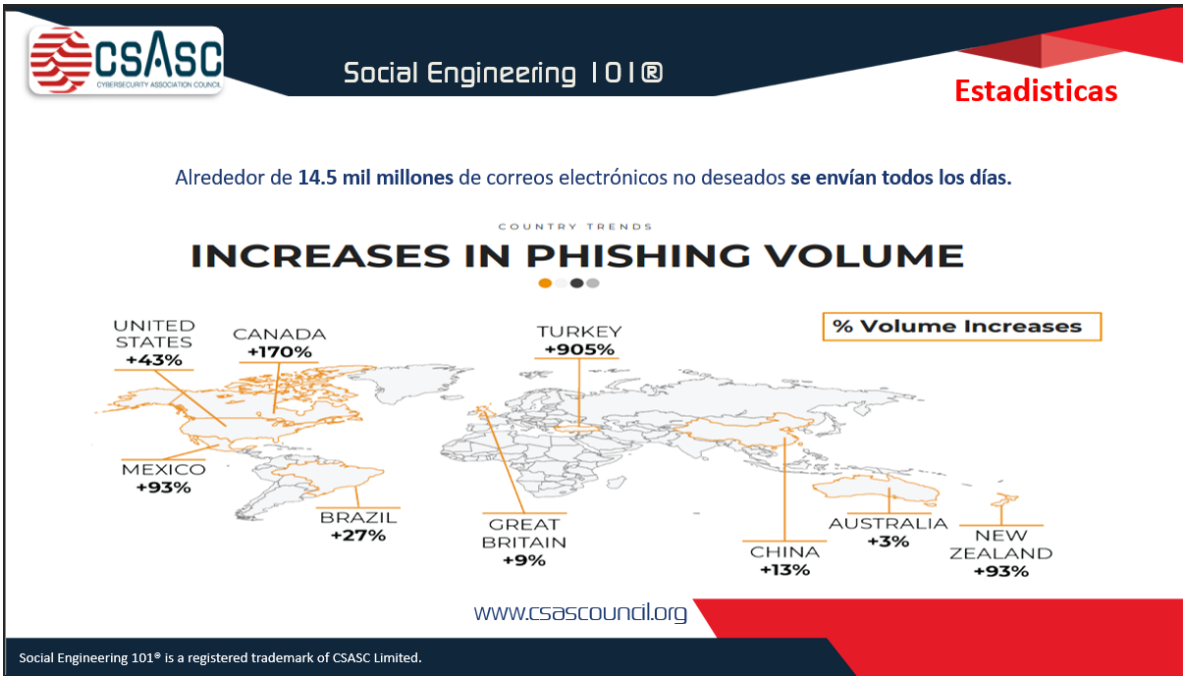
El 51% de los ataques **de phishing contienen enlaces a malware**. Según una investigación de **Avanan**, más de la mitad de los correos electrónicos de ataque de phishing contienen enlaces a malware. Esto es seguido por la recolección de credenciales, que representa el 41% de los ataques de phishing.



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.



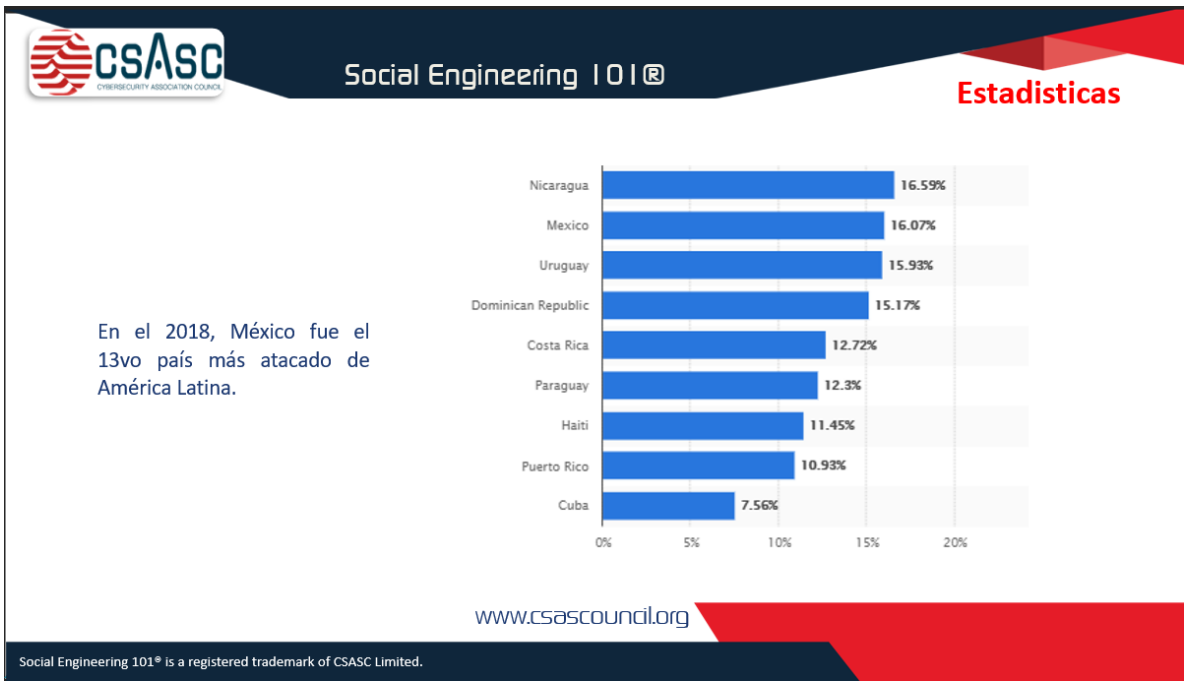
Alrededor de **14.5 mil millones** de correos electrónicos no deseados **se envían todos los días.**

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

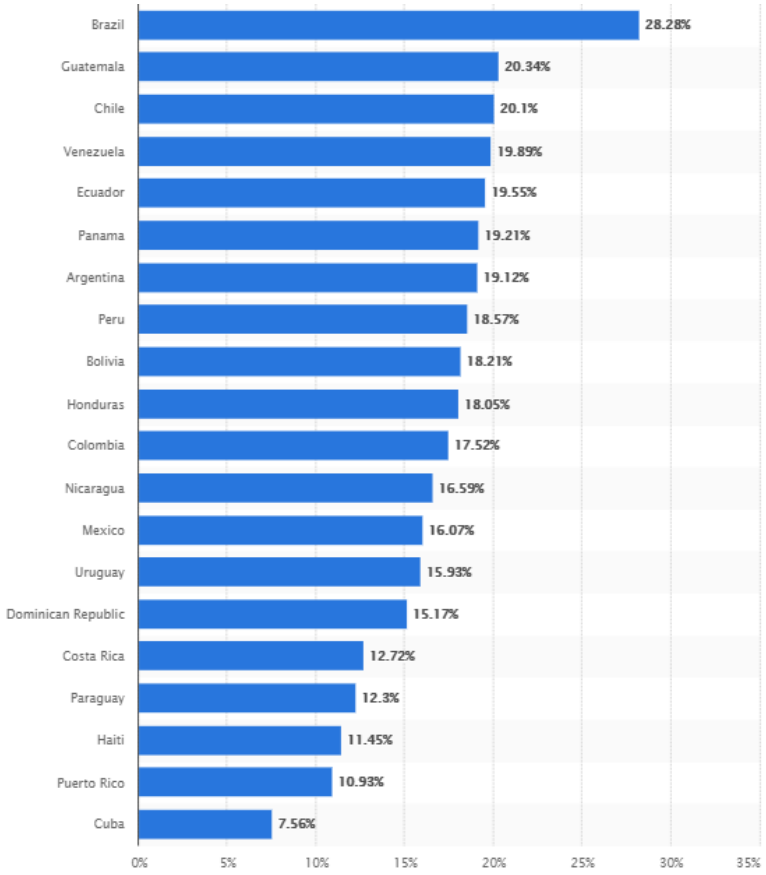
Según **Check Point Software Technologies LTD**, las fuentes más comunes de ingeniería social son los correos electrónicos de phishing.

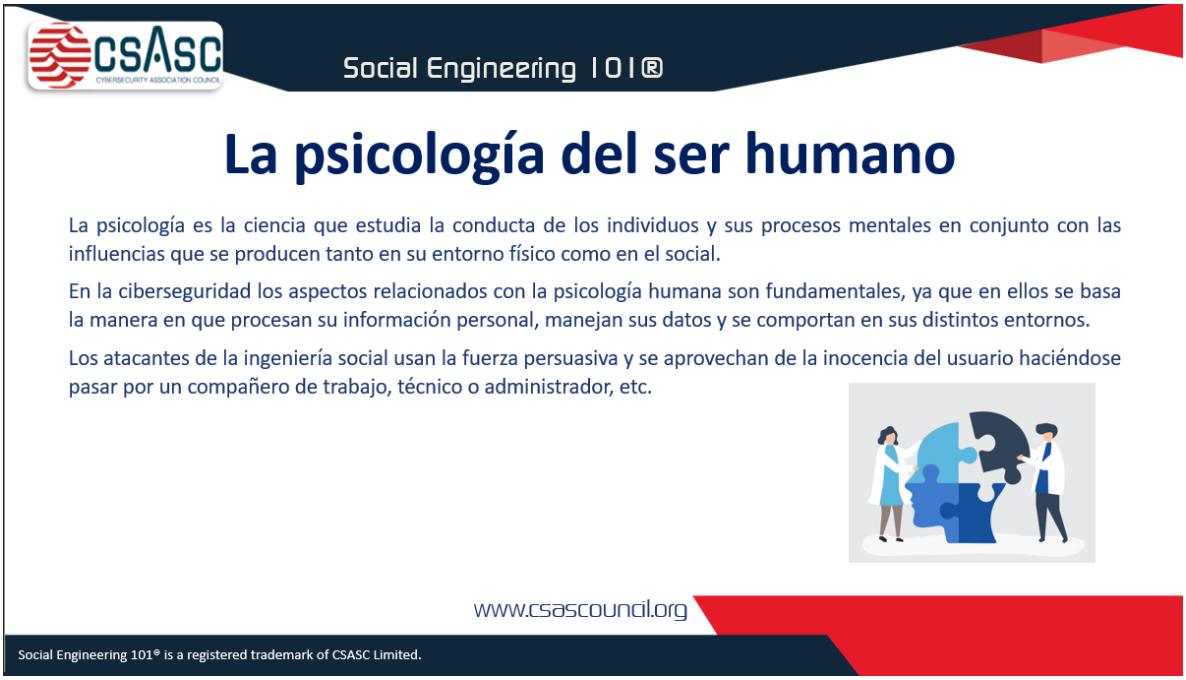
Check Point Software Technologies LTD, también encontró que solamente el **86% de las empresas reconocen a la ingeniería social como una preocupación creciente**, mientras que el 51% de las organizaciones cita las ganancias financieras como la motivación principal de ataques, seguido por ventajas competitivas 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.



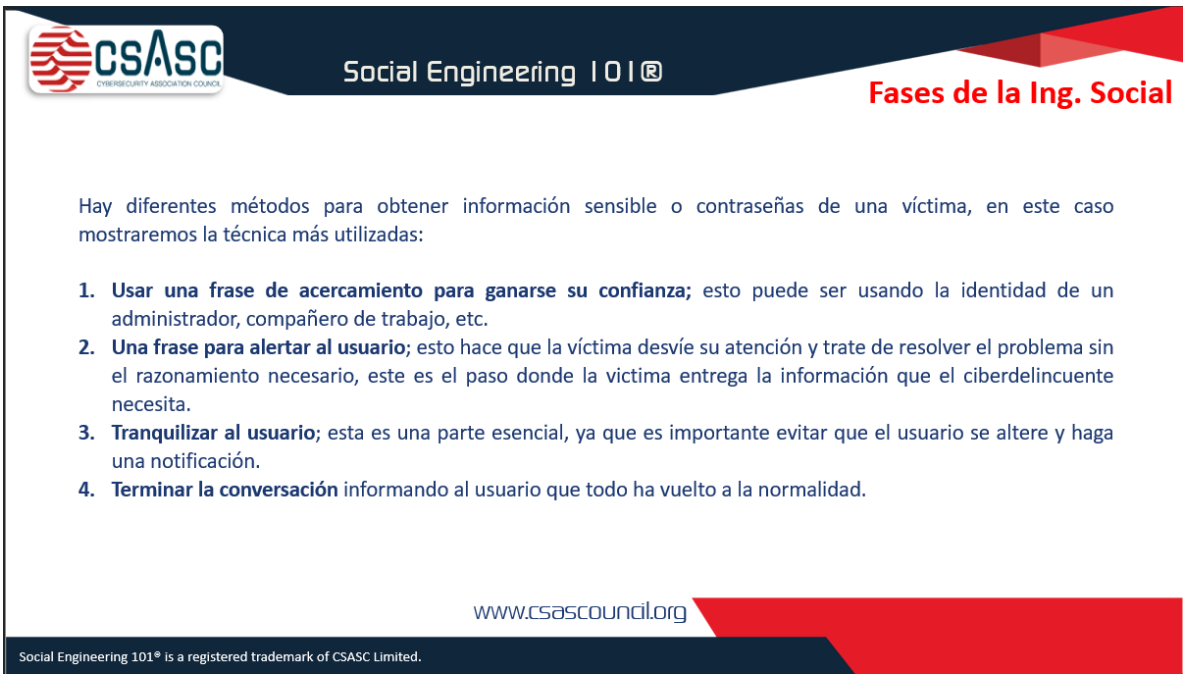


La psicología del ser humano

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.

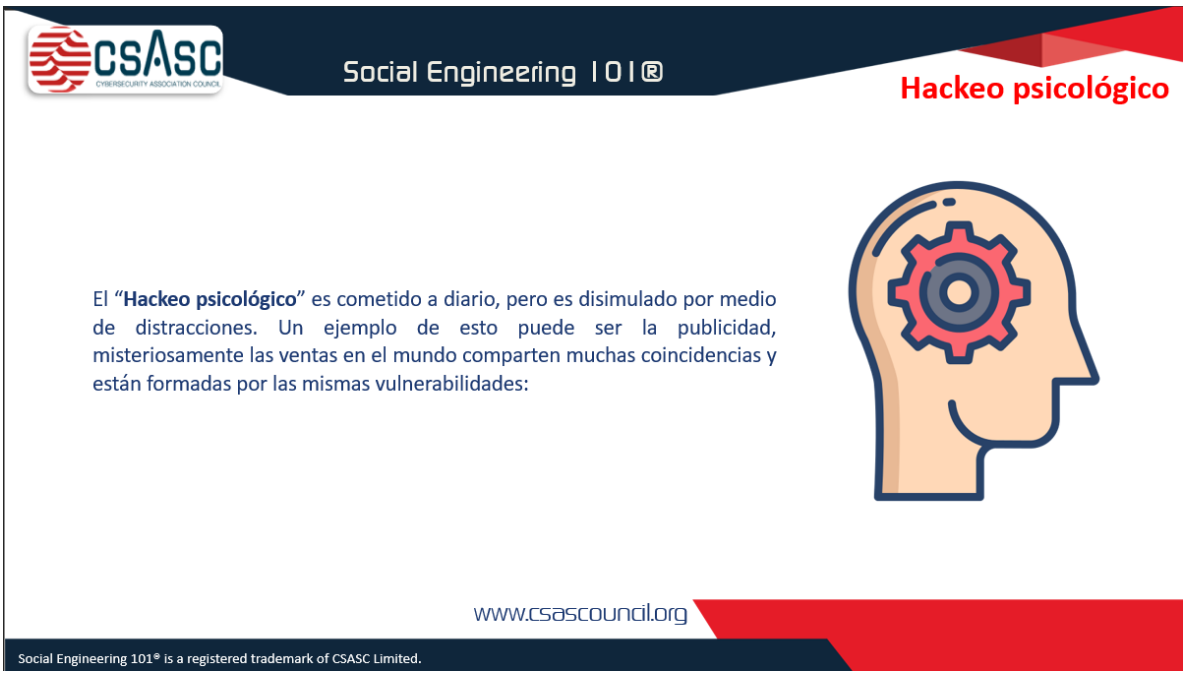
Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, técnico o administrador, etc.



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

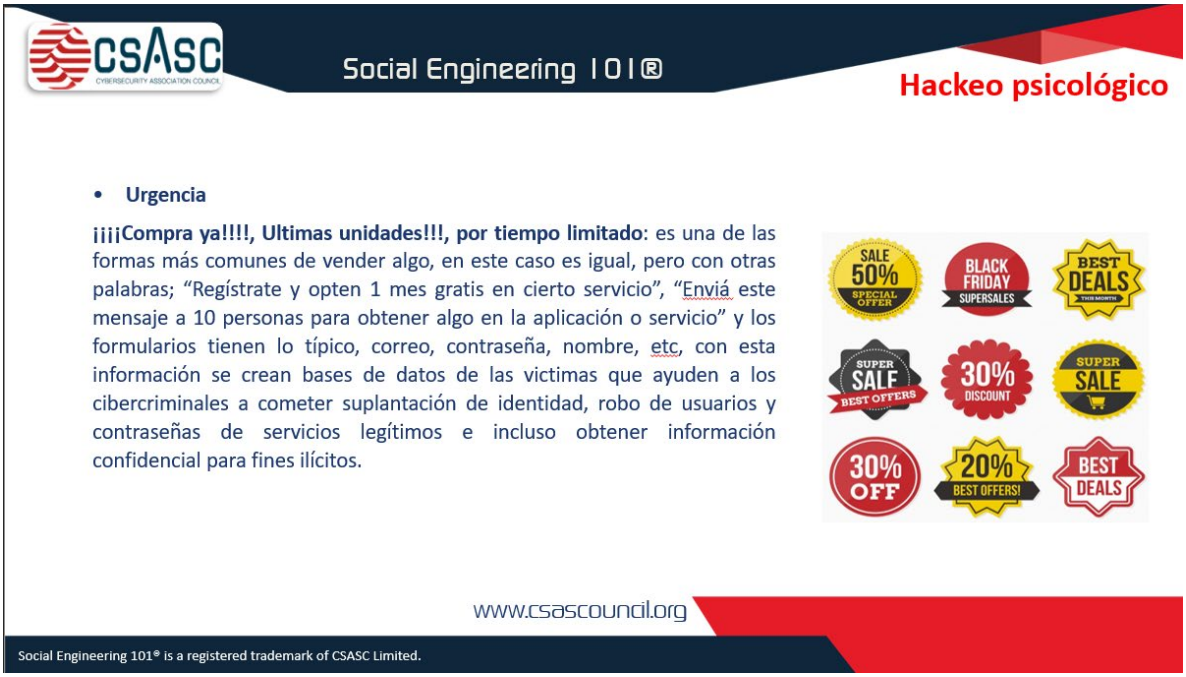
1. **Usar una frase de acercamiento para ganarse su confianza;** esto puede ser usando la identidad de un administrador, compañero de trabajo, etc.
2. **Una frase para alertar al usuario**; esto hace que la víctima desvíe su atención y trate de resolver el problema sin el razonamiento necesario, este 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.



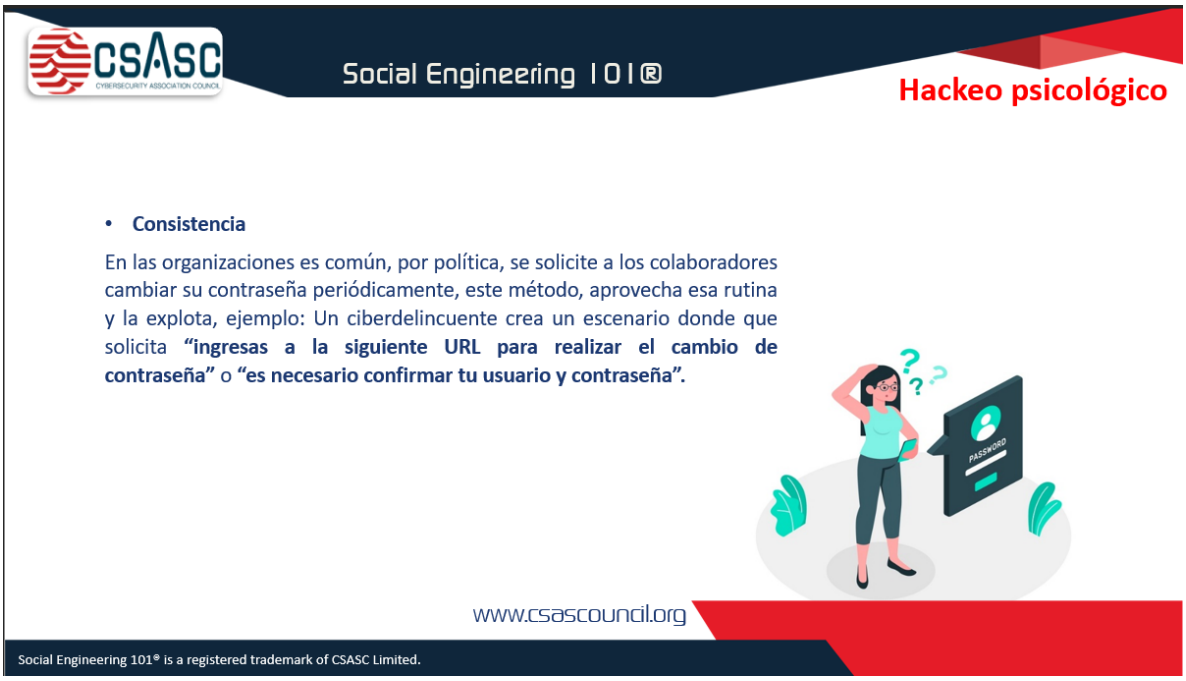
¿Algún ejemplo?

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**

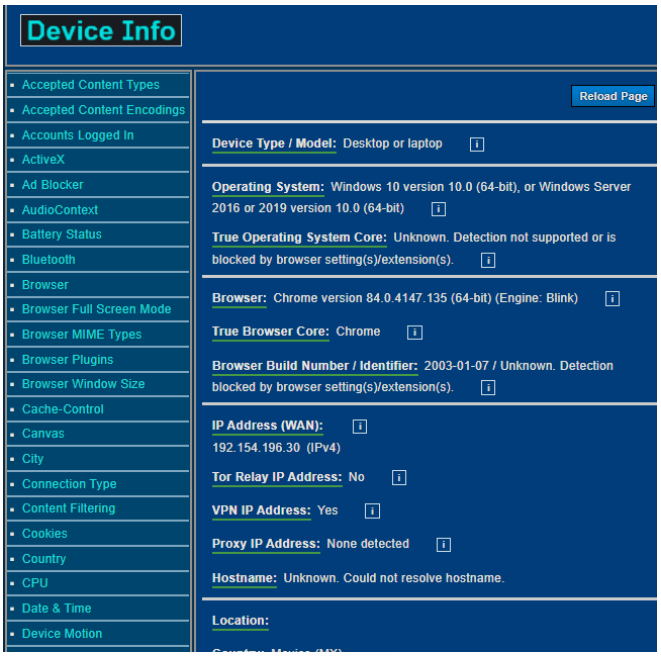
Establecer lazos de confianza, permite obtener información que difícilmente lograrían extraer de sistemas con robustos controles de seguridad, como información estratégica, financiera o confidencial de una organización, esto es aprovechado por cibercriminales que normalmente muestran falsa afinidad en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

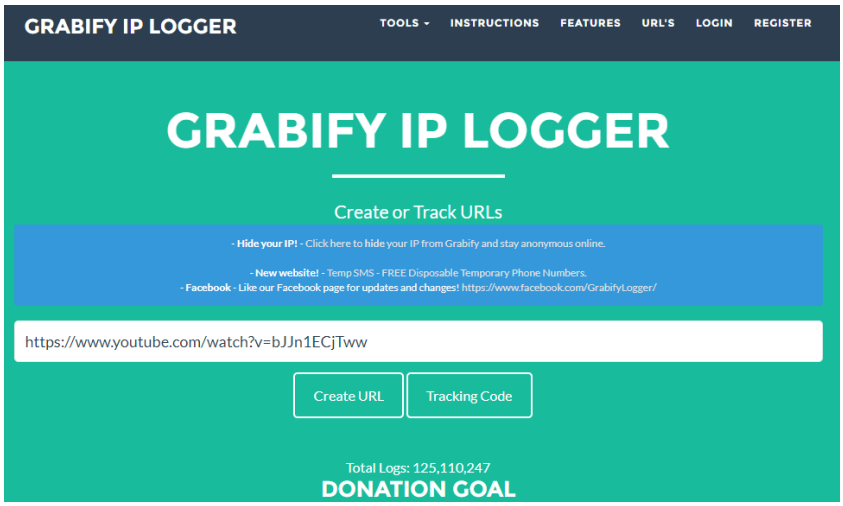


Grabify

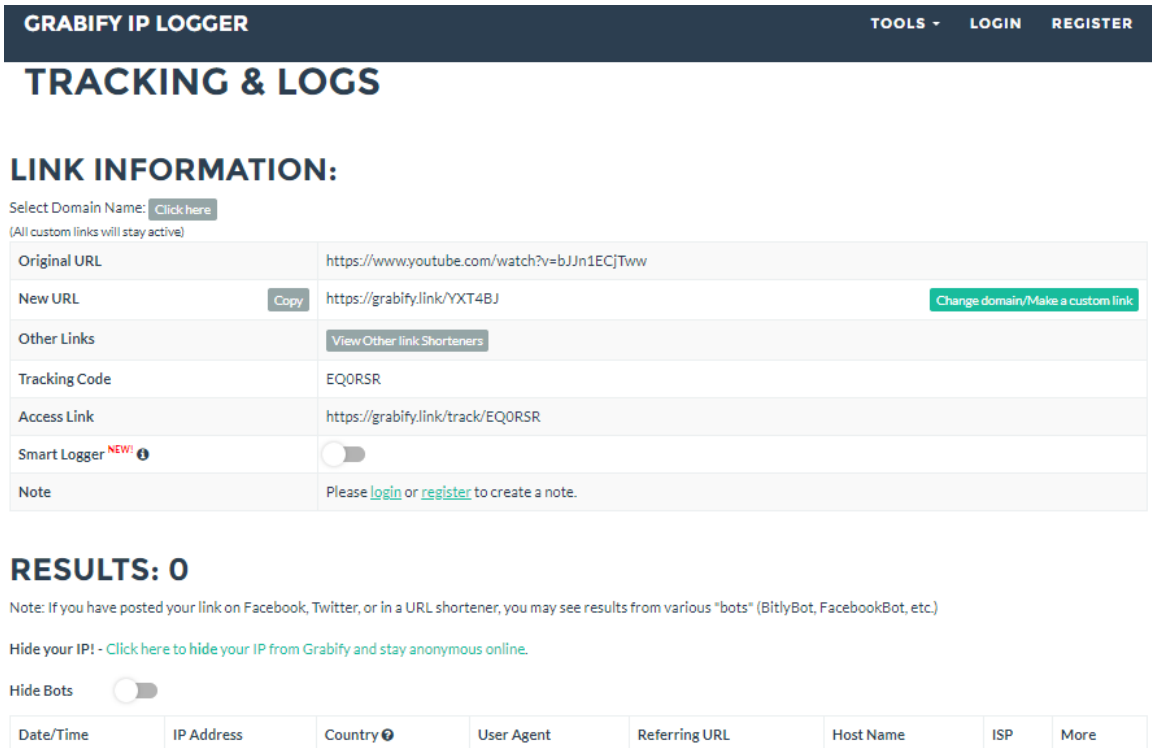
Grabify es una herramienta gratuita de captura de IP/acortamiento de URL basada en la web disponible en https://grabify.link/ (La captura de IP simplemente significa obtener / capturar las direcciones IP de las victimas), es útil en dispositivos móviles y computadoras, para utilizarlo, basta enviar un link.

Los pasos para usar esta herramienta son los siguientes:

- Encontrar un enlace a cualquier tema de interés que la víctima no se resistiría a visitar, pegar ese vínculo en el cuadro de dialogo: "***Enter URL or tracking code***".



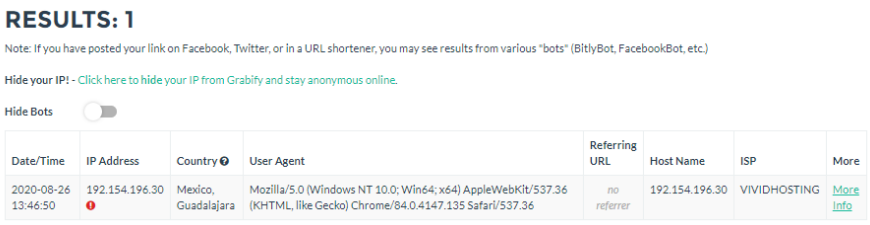
- Hacer clic en "Create URL", emergerá una ventana que le pedirá aceptar los términos de uso, si la URL se creó con éxito, será llevado a una página donde podrá monitorear la información de las victimas que abran el link.



En esta página aparecen los siguientes parámetros:

I. **New URL**. - URL que se deberá enviar a las víctimas.
II. **Tracking Code**. - Codigo para poder acceder a los logs.
III. **Access Link. -** Permite acceder a los logs de manera directa.
IV. **Smart Logger. -** Permite obtener información extra de las víctimas.

- Compartir la liga a las víctimas; en cuanto estas ingresen los resultados empezarán a llegar.



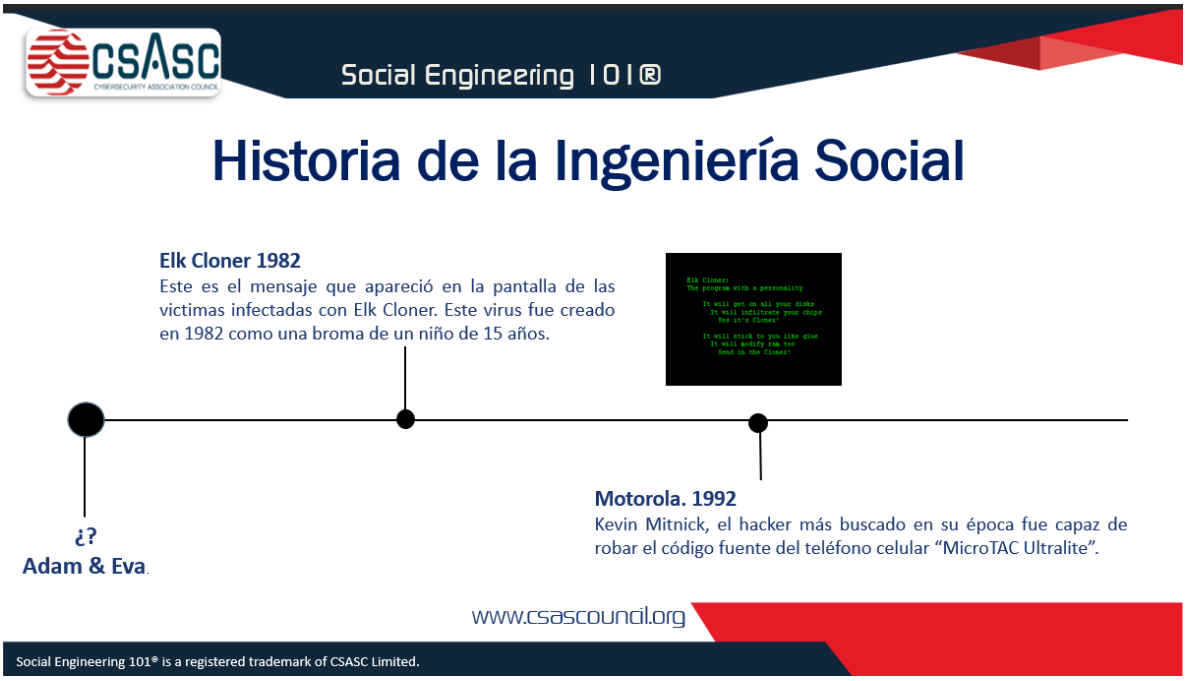
ADVANCED LOG

Date/Time	2020-08-26 13:51:14
IP Address	192.154.196.30
VPN/Proxy Detection NEW!	This IP may be a VPN or Proxy
Country	Mexico, Guadalajara
Orientation	landscape-primary
Timezone	America/Mexico_City CDT
User Time	Tue Aug 25 2020 20:51:15 GMT-0500 (hora de verano central)
Language	es-ES
Incognito/Private Window	No
Ad Blocker	No
Screen Size	1366 x 768
Local IP	fc27af23-5854-4265-9cc5-cec30f53e79b.local
GPU	AMD Radeon R7 Graphics
Browser	Chrome (84.0.4147.135)
Operating System	Windows 10 x64
Touch Screen	No
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36
Platform	Win32
Referring URL	*no referrer*
Host Name	192.154.196.30
ISP	VIVIDHOSTING

Historia de la Ingeniería Social

La ingeniería social ha estado presente desde los albores de la humanidad, claro, no era conocida con ese nombre, la popularización del término ingeniería social se debe al experto en ciberseguridad **Kevin Mitnick** en la época de los 90´s, aunque en realidad es un término que surgió por primera vez en las ciencias sociales y fue acuñado en 1894 por **Jacob Van Marken** (empresario y filántropo holandés), para resaltar la idea de que para manejar los problemas humanos, se necesitaban profesionales.

Quizás el primer relato registrado de la ingeniería social está en el libro del **Génesis**, donde el Diablo, interpretada por la codicia de Eva, con forma de una serpiente, logra convencerla de que Dios se estaba reservando poderes específicos para él, al prohibirle a ella y a Adam comer fruta del árbol de la vida. En realidad, si analizamos, la historia está llena de casos donde se usó ingeniería social, un claro ejemplo es el **caballo de troya** o la **venta de la Torre Eiffel (Victor Lustig 1925)**, todos estos ataques dejan evidencia de que los seres humanos siempre vamos a ser vulnerables, lo importante, es generar conciencia y reducir el riesgo de ser afectado por estos ataques.

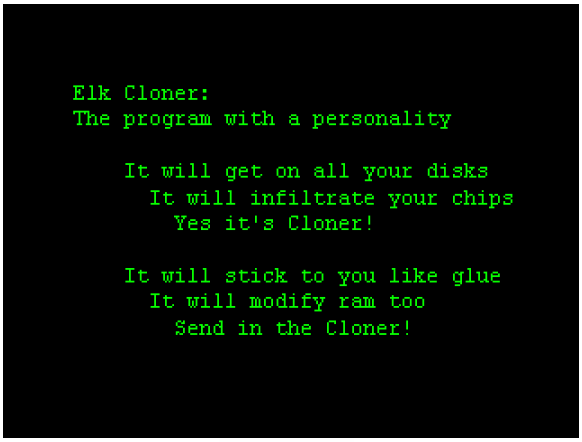


Casos de ingeniería social en la era del internet

Elk Cloner 1982

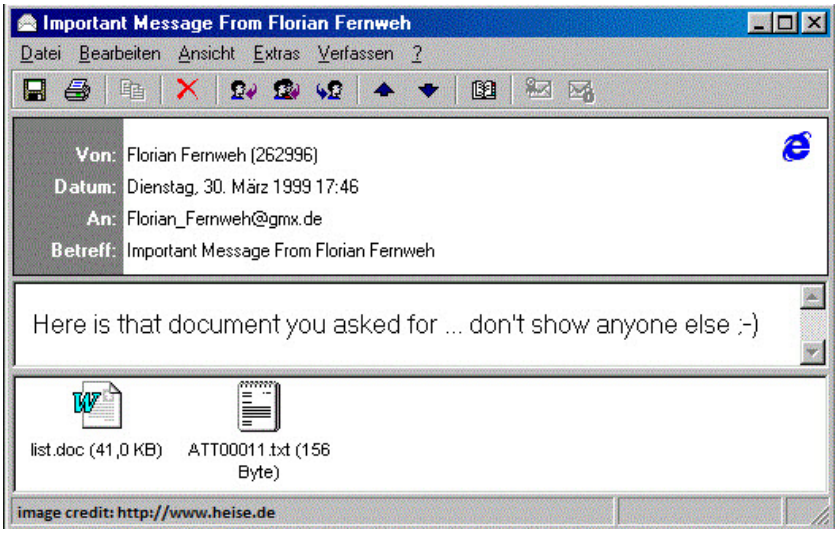
"Llegará a todos tus discos. Se infiltrará en tus fichas. ¡Sí, es Cloner! Se te pegará como pegamento. También modificará la RAM. ¡Envía el clonador!".

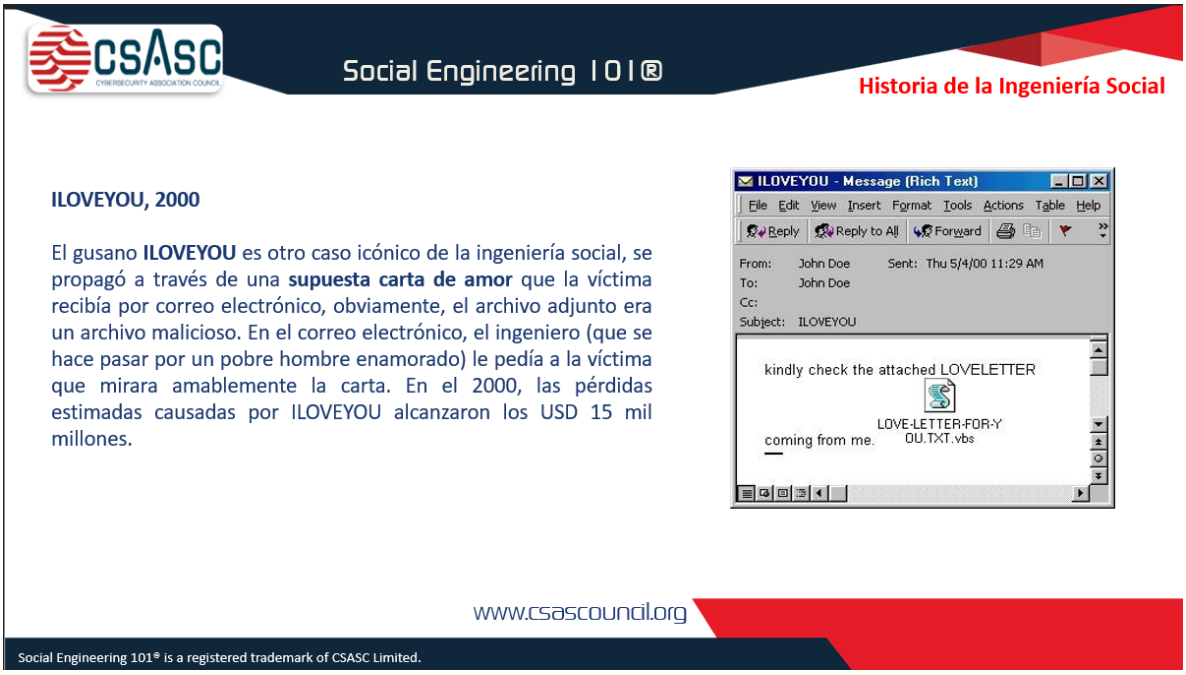
Este es el mensaje que apareció en la pantalla de las victimas infectadas con **Elk Cloner**. Este virus fue creado en 1982 como **una broma de un niño de 15 años**. Se transmitió a través de un disquete y puede citarse como uno de los primeros casos de ingeniería social en la era electrónica, las víctimas creían que era solo un juego, las victimas no podía controlar aquel mensaje que aparecía en la pantalla de sus ordenadores y tenía un fácil arreglo: con unos pocos conocimientos de informática cualquiera podía eliminarlo.



Melissa, 1999

El virus Melissa se considera uno de los primeros casos de ingeniería social en la historia y un hito porque **infectó miles de computadoras** a fines de la década de 1990. Melissa se propagó a través de un ataque de **phishing** utilizando un archivo adjunto malicioso de Microsoft Word. El correo electrónico engañaba al usuario con el siguiente tema: "Mensaje importante de (nombre de alguien conocido)". El daño causado por Melissa se estima en USD 80 millones.





ILOVEYOU, 2000

El gusano **ILOVEYOU** es otro caso icónico de la ingeniería social, se propagó a través de una **supuesta carta de amor** que la víctima recibía por correo electrónico, obviamente, el archivo adjunto era un archivo malicioso. En el correo electrónico, el ingeniero (que se hace pasar por un pobre hombre enamorado) le pedía a la víctima que mirara amablemente la carta. En el 2000, las pérdidas estimadas causadas por ILOVEYOU alcanzaron los USD 15 mil millones.

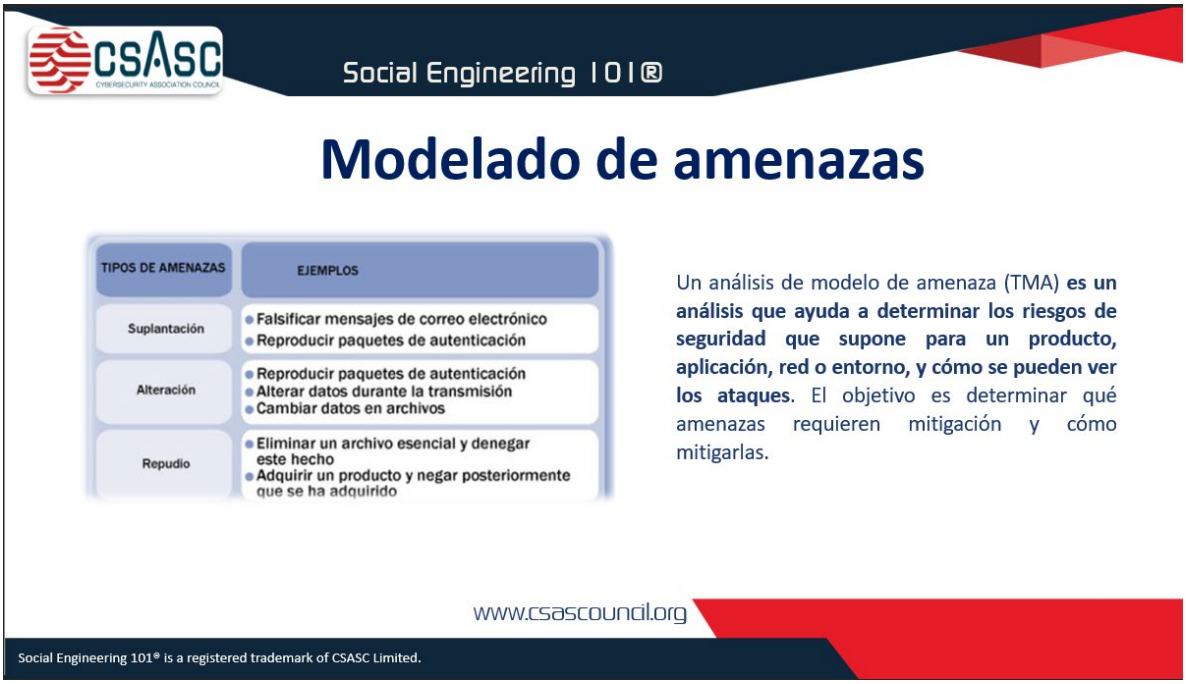
Casos modernos de la Ing. Social

Empresa afectada y año	Tipo de ataque	Descripción del ataque	Perpetrador	Datos curiosos
CIA 2017	Vishing	Gamble logró persuadir a Verizon para obtener información sobre John O. Brennan (director de la CIA 2013-2017), que luego usó para hacerse pasar por Brennan cuando contactó a AOL. Con ellos cambió preguntas y números de seguridad además de obtener acceso a muchas otras cuentas de correo electrónico como las del director de la CIA John Brennan y James Clapper, director de inteligencia nacional, entre otros. Esto le dio acceso a documentos militares altamente sensibles y operaciones de inteligencia en Irak y Afganistán.	Kane Gamble.	Kane Gamble tenía 15 años cuando llevo a cabo el ataque y fue sentenciado a dos años de prisión en 2018.
RSA 2011	Phishing	Los atacantes enviaron un correo electrónico con una dirección falsificada que pretendía estar en un sitio web de reclutamiento laboral, aquí adjuntaron un archivo de Excel titulado: “Plan de reclutamiento 2011”, 2 empleados lo abrieron y desataron una macro que instaló una puerta trasera en sus dispositivos a través de un 0day, lo que permitía a los atacantes infectar a otras computadoras para así, entrar y salir de los dispositivos infectados a su gusto.	Desconocido.	Este ataque le costó a RSA $66 millones de dólares.

Toyota Boshoku Corporation. 2019	BEC (Business Email Compromise)	En este caso los atacantes se hicieron pasar por un socio comercial de la subsidiaria de Toyota. Enviaron correos electrónicos a miembros del departamento de finanzas y contabilidad solicitando fondos para su pago y especificó que fueran enviados a una cuenta bancaria, en este caso esa cuenta estaba siendo controlada por los atacantes.	Desconocido.	Se estima que se perdió más de $37 millones de dólares.
Elecciones presidenciales en USA. 2016	phishing	Los hackers crearon un correo electrónico falso de Gmail, desde donde invitaban a los usuarios, a través de un enlace, a cambiar sus contraseñas debido a una actividad inusual detectada. Gracias a esta técnica lograron tener acceso a cientos de correos electrónicos que contenían información confidencial sobre la campaña de Clinton. Gracias a la filtración de correos electrónicos e información del Partido Demócrata se cree que puede haber influido en el resultado de las elecciones, con la victoria de Donald Trump sobre Hillary Clinton.	Desconocido.	Se cree que hackers rusos fueron los responsables de este ataque.
Motorola. 1992	vishing	Kevin Mitnick, el hacker más buscado en su época fue capaz de robar el código fuente del teléfono celular "**MicroTAC Ultralite**", esto para intentar cambiar los datos de identificación en el teléfono, o incluso desactivar la capacidad de las torres de teléfonos celulares para conectarse y dar su ubicación a los policías. Para hacer esto realizó llamadas a Motorola, donde pidió hablar con el Project Manager del modelo celular, después de ser transferido	Kevin Mitnick Alias "The Condor"	El cóndor decidió no hacer público su descubrimiento, por lo que no fue una carga para la empresa Motorola. Fue detenido en 1995, llevado a la cárcel y fue liberado en el 2000 después de pasar casi 5 años en prisión.

		con varias personas habló con el vicepresidente de Motorola, el cual le mencionó que su asistente, Pam, era la encargada del proyecto y le brindó su extensión. Al marcar la extensión contestó la secretaria de Pam, la cual dijo que Pam estaba de vacaciones, Mitnick aprovechó esto y le comentó: "Oye, Pam quedó en mandarme el código fuente del MicroTAC Ultralite y mencionó que en caso de que ella no pudiera tú me ibas a ayudar." Con esas palabras es que nuestro hacker logró convencer a la secretaria de enviarle el código fuente. Al llevar a cabo un envío fallido, la secretaria fue a avisar al Security Manager, situación que preocupó a Mitnick, pues esperaba lo peor y resultó que este Manager le había otorgado su usuario y contraseña del servidor proxy a la secretaria, por lo que pudo compartir el código fuente sin ningún problema.		
Numerosas empresas telefónicas, la armada israelí. 90´s	vishing	A través de técnicas de ingeniería social, como llamar a las oficinas centrales de las compañías telefónicas donde fingían ser ingenieros o chatear con secretarias para obtener detalles sobre su jefe que los ayudaría a adivinar las contraseñas. Los Badir tenían habilidades que eran absolutamente únicas: podían causar estragos imitando perfectamente las voces y podían decir el PIN de un teléfono simplemente escuchando a alguien escribirlo desde el otro lado de la habitación.	Badir Brothers. Muzher, Shadde and Munther.	Los 3 hermanos eran ciegos de nacimiento.

HP	Pretexting	En 2005 y 2006, HP se vio afectado por las luchas internas corporativas, y la gerencia estaba convencida de que un miembro de la junta estaba filtrando información privilegiada a los medios. HP contrató investigadores privados para investigar la comunicación de su propia junta, lo que hicieron a través de pretexting. Armados solo con los nombres de los miembros de la junta y los últimos cuatro dígitos de sus números de seguro social, los investigadores pudieron llamar a AT&T y convencerlos de proporcionar acceso a registros detallados de las llamadas de las víctimas.	Investigadores privados.	HP afirmó que no habían autorizado estas técnicas, las consecuencias resultaron en múltiples renuncias; el escándalo también resultó en una ley federal más fuerte contra la práctica.



Metodología de la ingeniería social

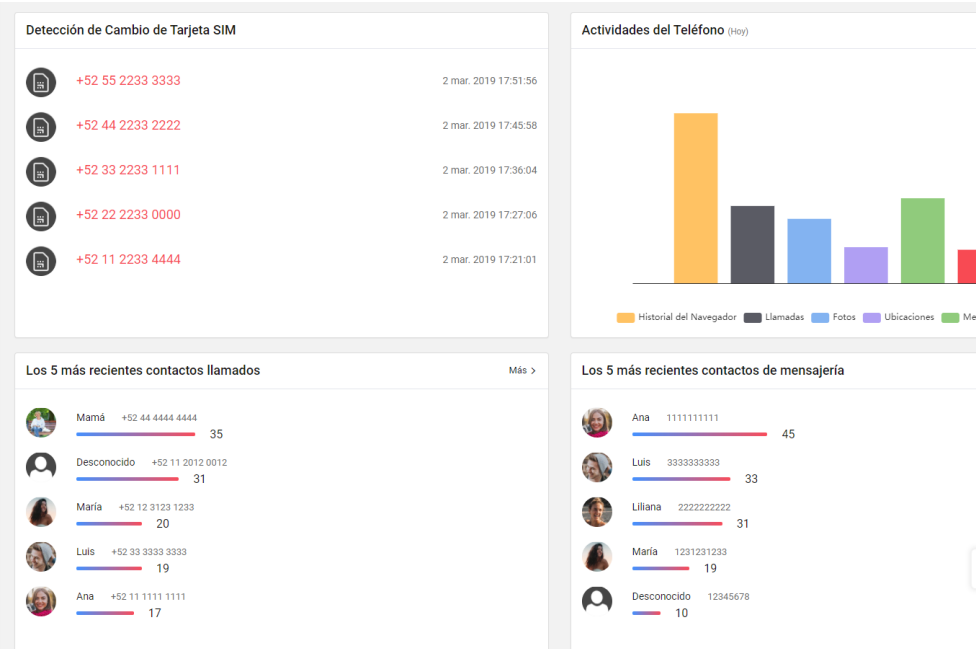
La metodología de la ingeniería social está compuesta por cinco pasos:

1. ***Modelado de amenazas:*** un análisis de modelo de amenaza (TMA) **es un análisis que ayuda a determinar los riesgos de seguridad que supone para un producto, aplicación, red o entorno, y cómo se pueden ver los ataques**. El objetivo es determinar qué amenazas requieren mitigación y cómo mitigarlas.

2. ***Reconocimiento***: el reconocimiento **es la parte de enumerar y obtener toda la información posible del individuo,** ya sea obteniendo información de fuentes públicas o privadas (técnicas sigilosas). Para así poder dibujar un diagrama de cómo está relacionado, sus gustos y como poder explotar su confianza con la información obtenida.
   *La técnica usada en esta fase es conocer lo mejor posible a la víctima, esto se puede realizar **investigando** y **vigilando**, un ejemplo es:*
   https://www.insecam.org/

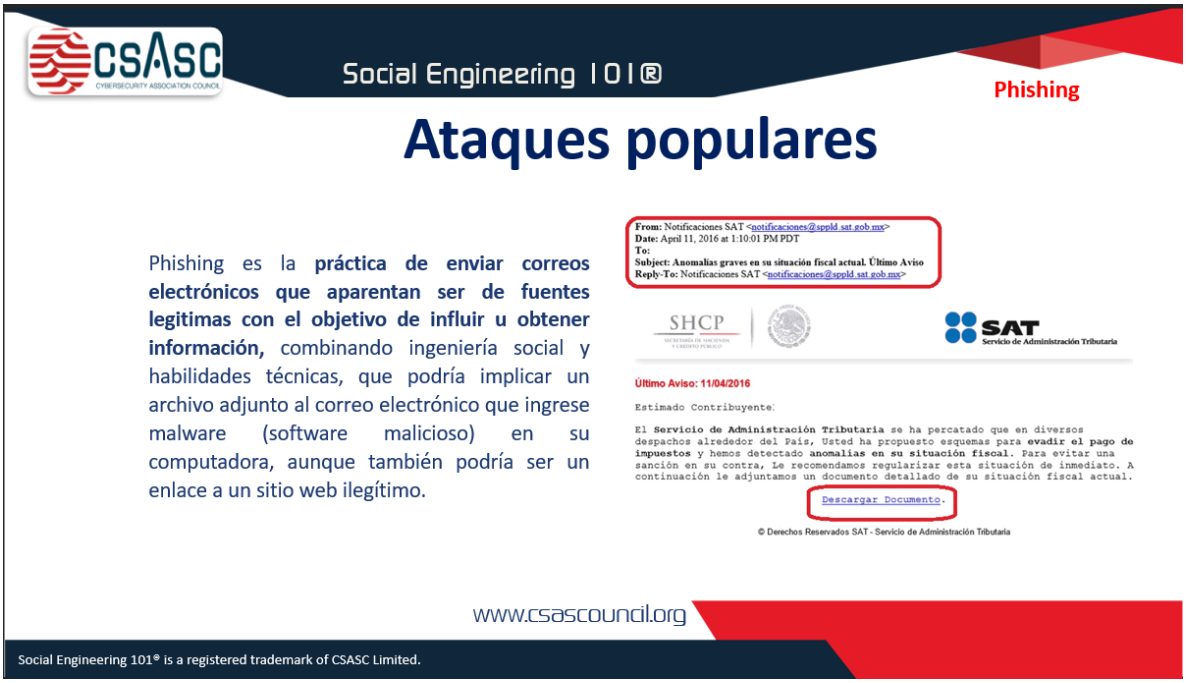
3. ***Creación de escenarios:*** **crear hipótesis de posibles escenarios,** para poder comprometer o atacar a la víctima, de esta forma se escogerá el mejor escenario donde la probabilidad de tener éxito sea mayor.
    - Si alguien le regalara un iPhone con malware podría estar exponiendo la información confidencial de su organización, como los datos de contacto de sus clientes.

https://www.spyzie.com/es/



4. ***Ejecución de escenarios:*** esta fase se enfoca en la ejecución del escenario seleccionado, aquí el atacante aplica sus mejores técnicas para conseguir éxito.

5. ***Reportaje/Documentación:*** en esta fase se documenta todo lo sucedido desde, la fase 1.



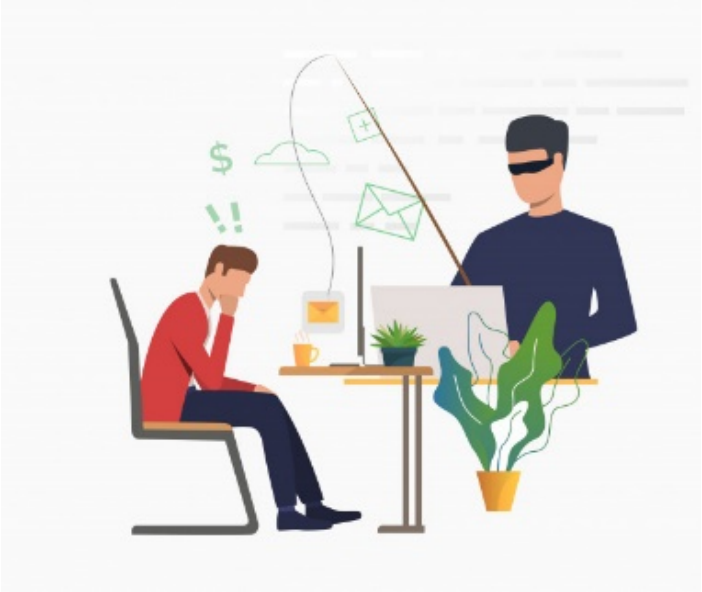
Ataques populares

Phishing

Phishing es la **práctica de enviar correos electrónicos que aparentan ser de fuentes legitimas con el objetivo de influir u obtener información,** combinando ingeniería social y habilidades técnicas, que podría implicar un archivo adjunto al correo electrónico que ingrese malware (software malicioso) en su computadora, aunque también podría ser un enlace a un sitio web ilegítimo.

Ejemplo

Demostración en vivo de phishing avanzado.



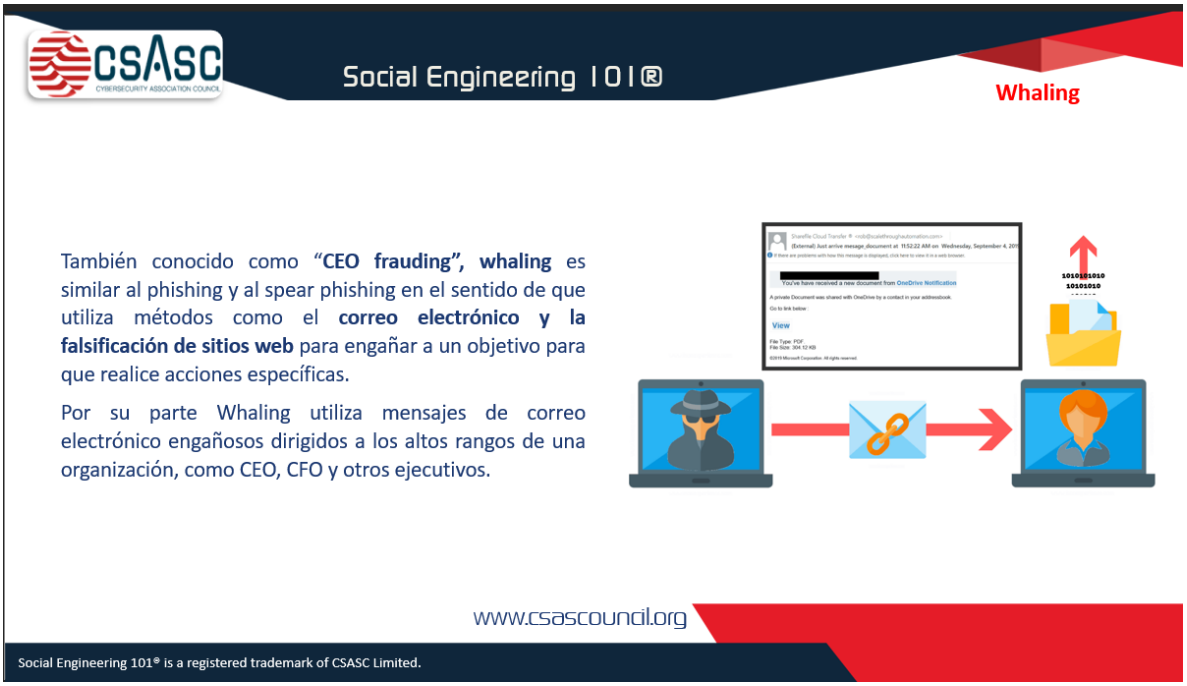
Spear Phishing

El spear phishing **es una forma muy específica de phishing**, los atacantes se toman el tiempo para realizar investigaciones sobre objetivos y crean mensajes personales y relevantes, esto quiere decir que **va dirigido específicamente a una persona**.

Debido a esto, el spear phishing puede ser muy difícil de detectar y aún más difícil de defender.

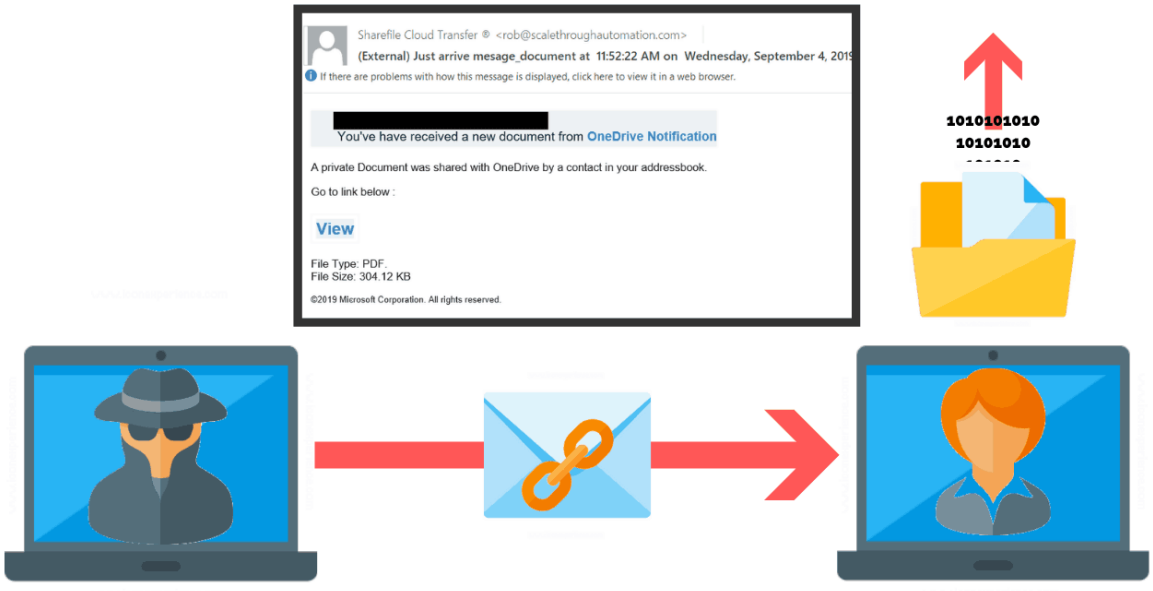
Ejemplo

Demostración en vivo de Spear Phishing avanzado.



Whaling

También conocido como "**CEO frauding", whaling** es similar al phishing y al spear phishing en el sentido de que utiliza métodos como el **correo electrónico y la falsificación de sitios web** para engañar a un objetivo para que realice acciones específicas. Por su parte Whaling utiliza mensajes de correo electrónico engañosos dirigidos a los altos rangos de una organización, como CEO, CFO y otros ejecutivos.



Ejemplo

Demostración en vivo de Whaling avanzado haciéndonos pasar por una institución.

Notificación BBVA

BBVA

Hola, EDGAR:

Acabas de hacer un retiro de tu **apartado**, te compartimos el comprobante. Si tu no hiciste este retiro, favor de mandar el comprobante de estado de cuenta, junto con una identificacion oficial o pasaprte.

Importe cobrado: $13,500.00

DETALLES DE OPERACIÓN

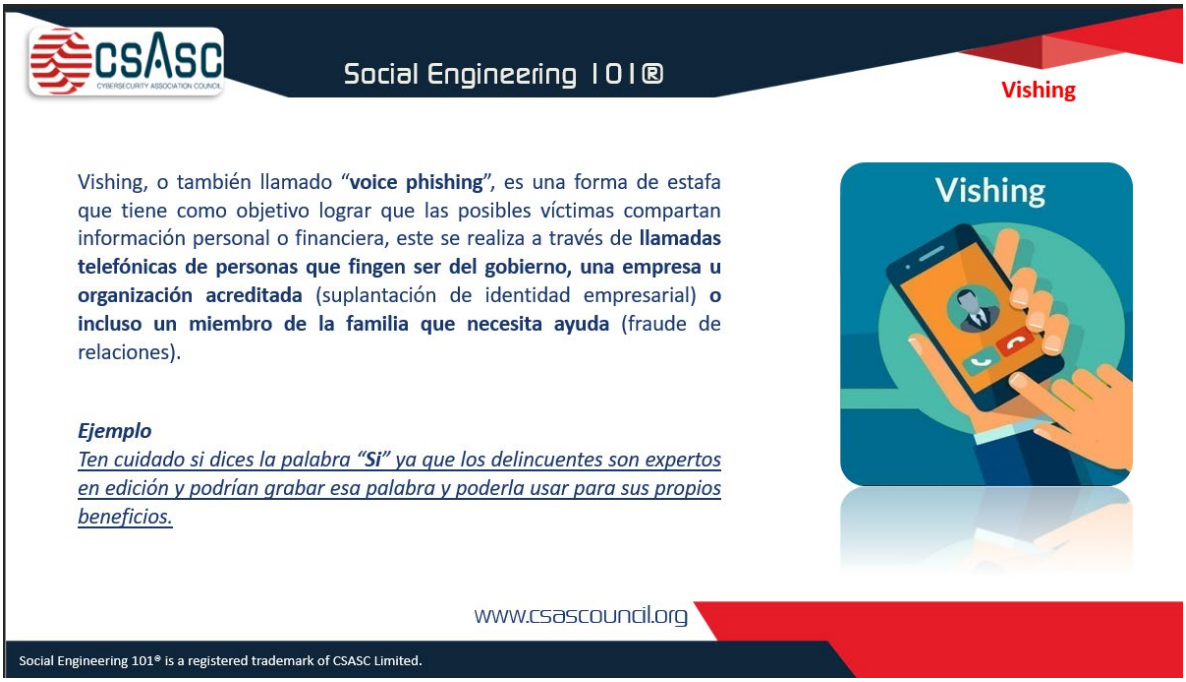
Fecha:
2020-07-21

Hora:
10.43.20 hrs.

Folio:
004317000692400489

Saludos,

Equipo BBVA.



Vishing

Vishing, o también llamado "**voice phishing**", es una forma de estafa que tiene como objetivo lograr que las posibles víctimas compartan información personal o financiera, este se realiza a través de **llamadas telefónicas de personas que fingen ser del gobierno, una empresa u organización acreditada** (suplantación de identidad empresarial) **o incluso un miembro de la familia que necesita ayuda** (fraude de relaciones).

Ejemplo

*Ten cuidado si dices la palabra "**Si**" ya que los delincuentes son expertos en edición y podrían grabar esa palabra y poderla usar para sus propios beneficios.*

Smishing

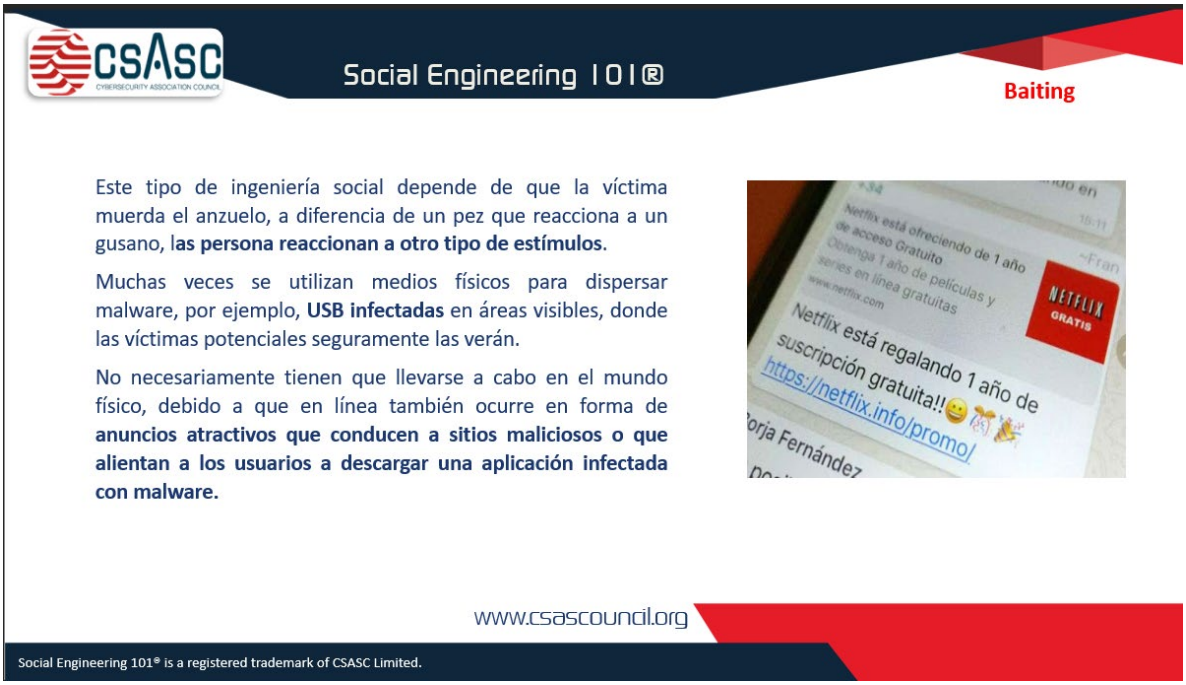
Smishing **es cuando alguien intenta engañarte para obtener información privada a través de un mensaje de texto o SMS**, es lo equivalente a phishing, pero con otro medio de comunicación. Es muy utilizado para ataques de bancamóvil de cualquier banco.

Ejemplo

Mensajes haciéndose pasar por alguna institución regalando algo.

Pretexting

Se define como **la práctica de presentarse con otra identidad para obtener información privada.**
Es más que solo crear una mentira, en algunos casos puede **ser crear una identidad completamente nueva** y luego usar esa identidad para manipular la recepción de información. Esta técnica también se puede utilizar para hacerse pasar por personas en ciertos trabajos y roles que ellos mismos nunca han hecho.



Baiting

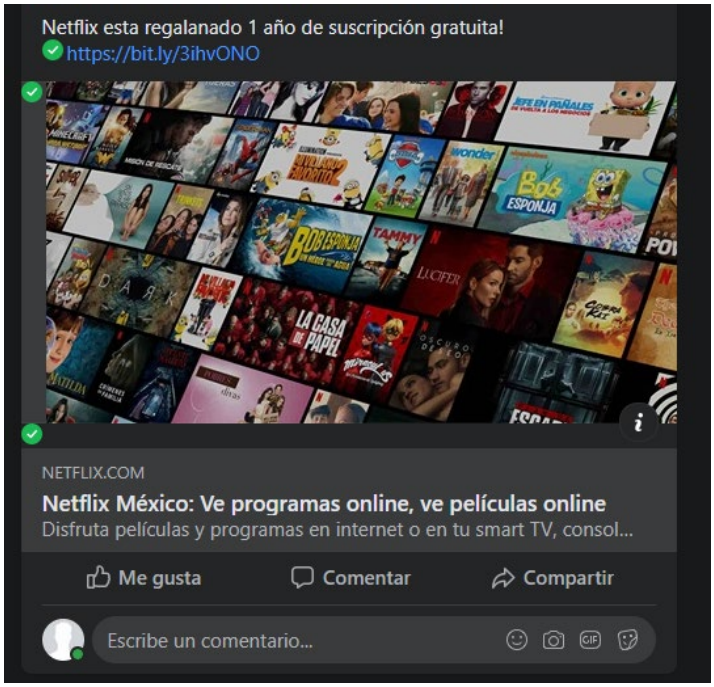
Este tipo de ingeniería social depende de que la víctima muerda el anzuelo, a diferencia de un pez que reacciona a un gusano, l**as persona reaccionan a otro tipo de estímulos**.

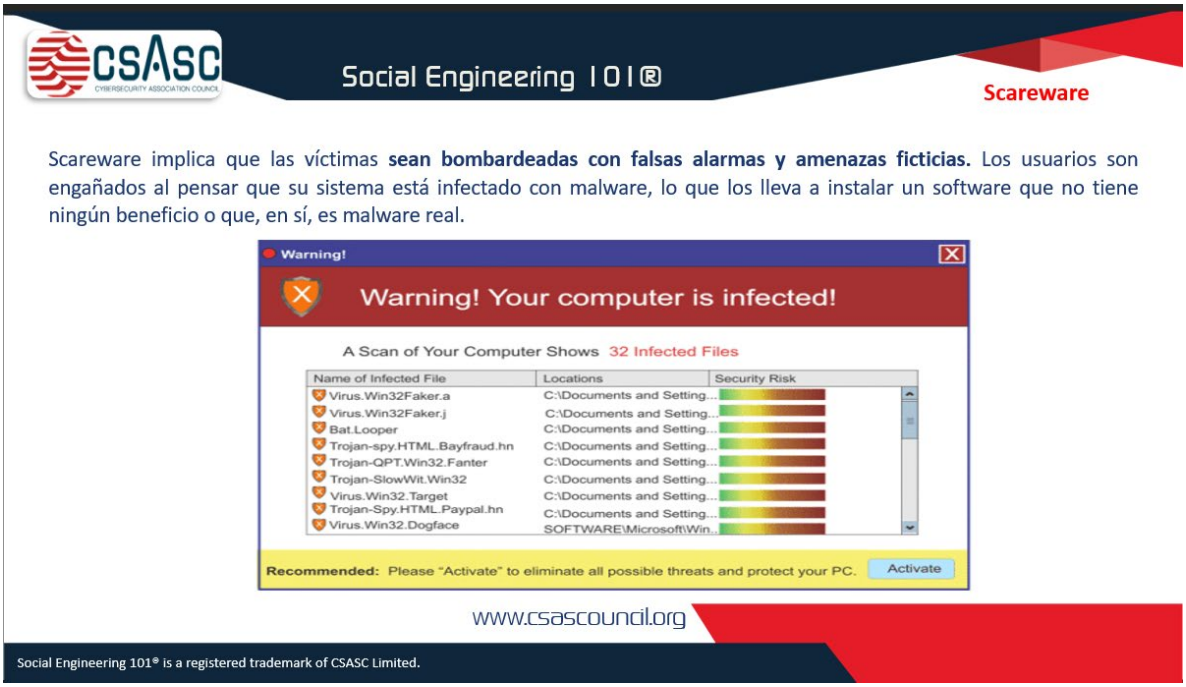
Muchas veces se utilizan medios físicos para dispersar malware, por ejemplo, **USB infectadas** en áreas visibles, donde las víctimas potenciales seguramente las verán.

No necesariamente tienen que llevarse a cabo en el mundo físico, debido a que en línea también ocurre en forma de **anuncios atractivos que conducen a sitios maliciosos o que alientan a los usuarios a descargar una aplicación infectada con malware.**

Ejemplo

Abusando de los metadatos en redes sociales.





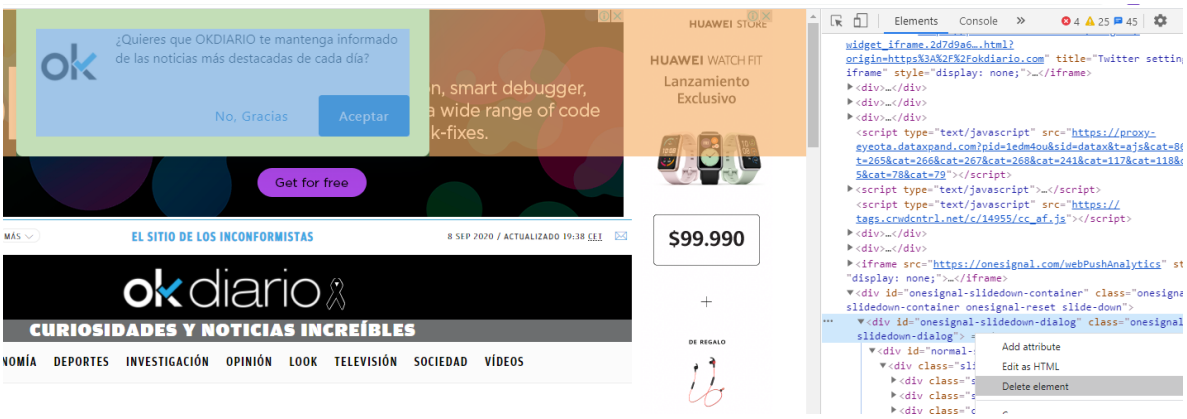
Scareware

Scareware implica que las víctimas **sean bombardeadas con falsas alarmas y amenazas ficticias.** Los usuarios son engañados al pensar que su sistema está infectado con malware, lo que los lleva a instalar un software que no tiene ningún beneficio o que, en sí, es malware real.

Ejemplo

Se pueden borrar todos esos mensajes molestos que salen, sin tener que darle en el botón de "**Si**" o "**No**".

https://okdiario.com/curiosidades/feliz-dia-madre-2020-frases-bonitas-felicitar-hoy-tu-madre-5548745



Tailgating

También conocido como "***piggybacking***", este ataque es ejecutado por un ciberdelincuente que busca entrar a un área restringida que carece de la seguridad adecuada. **El atacante puede simplemente caminar detrás de una persona autorizada para acceder al área**.

Quid Pro Quo

Esta estafa implica un intercambio, **los estafadores hacen que la víctima crea que es un intercambio justo,** el ataque quid pro quo más común ocurre cuando un hacker se hace pasar por un miembro del personal de TI de una organización, ese hacker contacta por teléfono a los empleados de esta organización y les ofrece algún tipo de actualización o instalación de software.

Sitios clonados

El uso de sitios clonados es una de las técnicas favoritas de los ciberdelincuentes para robar información confidencial de las personas. Existen múltiples formas de clonar un sitio web, a continuación, se verán de dos formas para clonar una página web.

Ejemplo 1

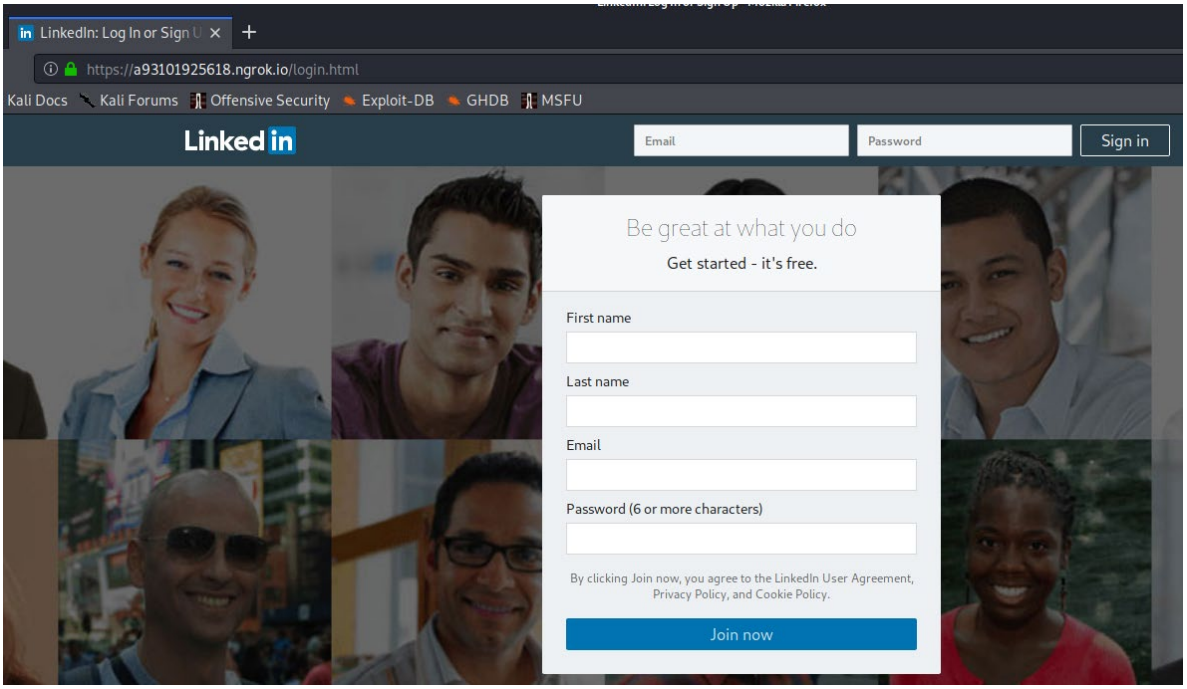
Por medio del sistema operativo Kali Linux, haciendo uso de código de **Github** y plantilla clonadas, es posible colocar la web clonada en Internet con un dominio temporal, para lograr, captura todos los datos relevantes de las victimas que ingresen.

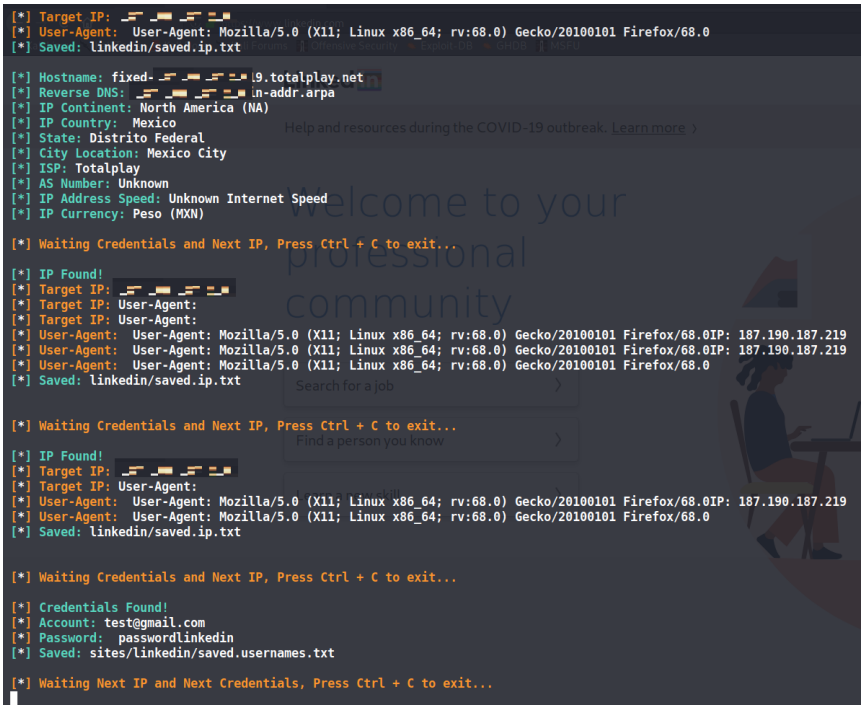
- ***git clone https://github.com/thelinuxchoice/shellphish.git***

```
root@kali ~/Desktop# git clone https://github.com/thelinuxchoice/shellphish.git
Cloning into 'shellphish'...
remote: Enumerating objects: 521, done.
remote: Total 521 (delta 0), reused 0 (delta 0), pack-reused 521
Receiving objects: 100% (521/521), 13.13 MiB | 470.00 KiB/s, done.
Resolving deltas: 100% (189/189), done.
root@kali ~/Desktop#
```

```
root@kali ~/Desktop# cd shellphish/
root@kali ~/D/shellphish (master)# chmod +x shellphish.sh
root@kali ~/D/shellphish (master)# ./shellphish.sh

                                                                  v1.8

    .:.:. Phishing Tool coded by:  @linux_choice .:.:.

 :: Disclaimer: Developers assume no liability and are not    ::
 :: responsible for any misuse or damage caused by ShellPhish ::

[01] Instagram      [09] Origin         [17] Gitlab
[02] Facebook       [10] Steam          [18] Pinterest
[03] Snapchat       [11] Yahoo          [19] Custom
[04] Twitter        [12] Linkedin       [99] Exit
[05] Github         [13] Protonmail
[06] Google         [14] Wordpress
[07] Spotify        [15] Microsoft
[08] Netflix        [16] InstaFollowers

[*] Choose an option:
```

Con solo acceder a la página empezará **a capturar los datos**, como **Target IP, User-Agent, Hostname, DNS, ISP, entre otros datos.**

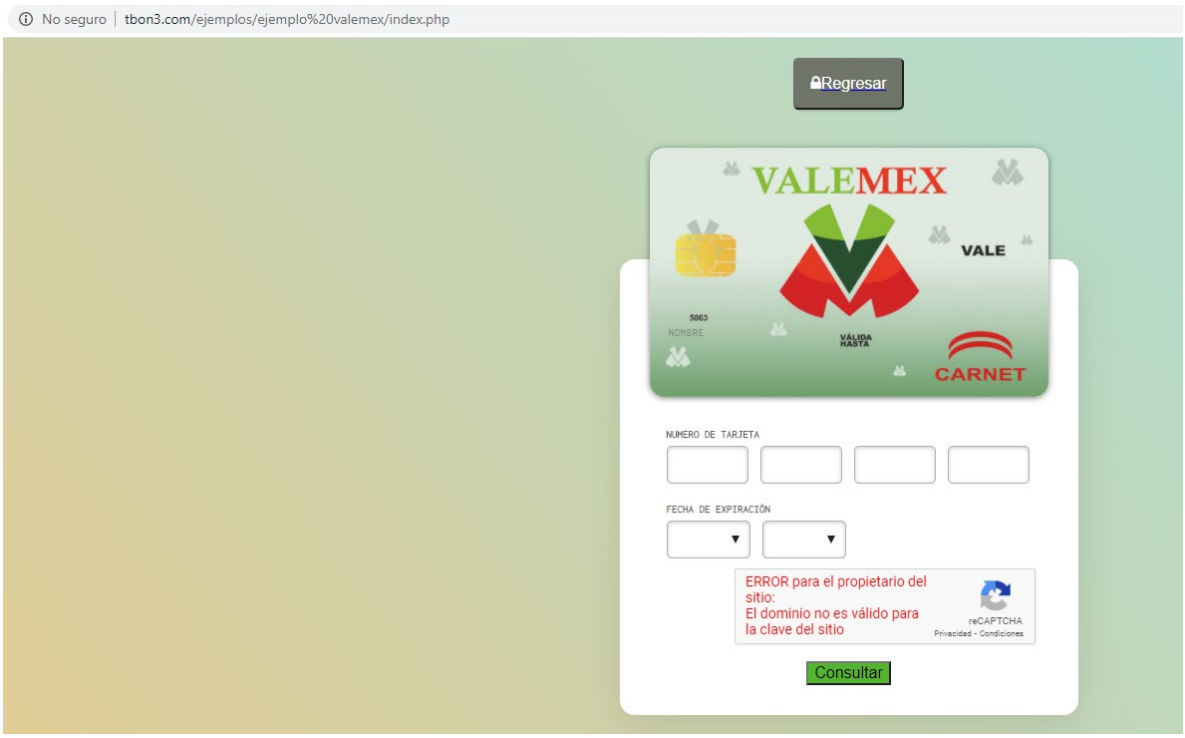




Ejemplo 2

Programar el código en **html, php, javascript, css** y subirlo a un servidor web (hosting).

http://tbon3.com/ejemplos/ejemplo%20valemex/index.php



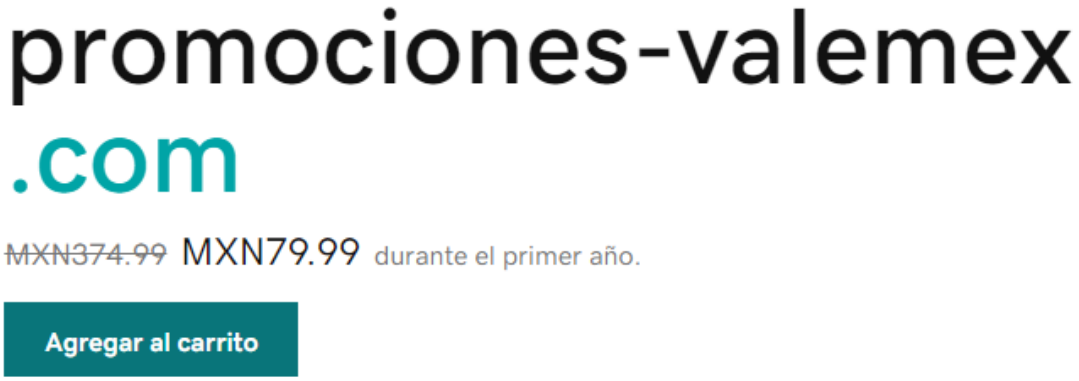
Tal vez la página es idéntica, pero ¿Qué pasa con el nombre del dominio?

Se ha descubierto que los ciberdelincuentes han estado recurriendo a comprar dominios de la siguiente forma:

Usar palabras claves como:

- Support
- Secure
- Promos
- Promociones
- Sustituir la l (L) por I (i)
- Sustituir m por rn
- Agregar o quitar alguna letra

Todo esto mencionado complica y confunde la vista lo cual cualquier persona podría caer en esta trampa.



Data Breaches

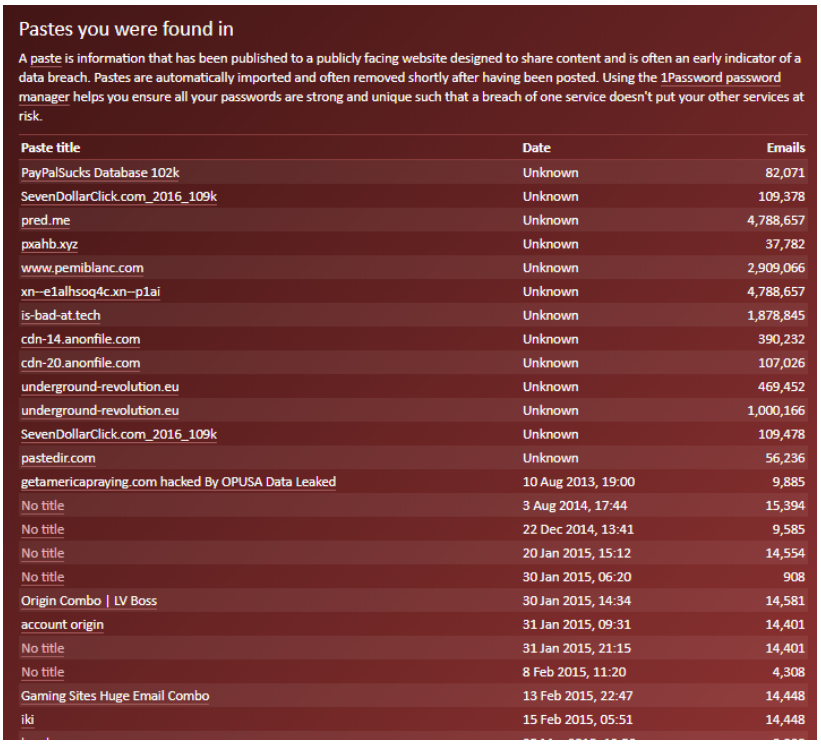
Una data breach (violación de datos) es un incidente de seguridad en el que se accede a la información sin autorización. Las filtraciones de datos pueden perjudicar a las empresas y a los consumidores de diversas formas. Además, son un gasto costoso para la entidad afectada y pueden dañar la vida de las personas o afectar la reputación de las empresas y su reparación requiere tiempo para ser concretada.

Cada vez que un empleado hace clic en un enlace de phishing, sin saberlo, pone en riesgo a toda la organización. Por eso existen páginas que se encargan de recopilar bases de datos de correos electrónicos que han sido comprometidos a través de los data breaches, así como otra información de suma importancia para la parte afectada. Las principales páginas encargadas de esto son: https://haveibeenpwned.com/ y https://emailrep.io/.

Have I been pwned

Esta página ofrece un servicio gratuito para que los usuarios verifiquen si sus nombres de usuario y contraseñas se han visto comprometidos en una violación de datos. Para usarla basta visitar https://haveibeenpwned.com/ en su navegador web y escribir el correo electrónico del cual se desea obtener la información para de inmediato obtener las plataformas donde los datos del usuario fueron comprometidos.

Además, brinda los enlaces donde sus credenciales fueron publicadas por parte de los atacantes. Se recomienda, en caso de ser necesario, vaya y cambié la contraseña de su correo.



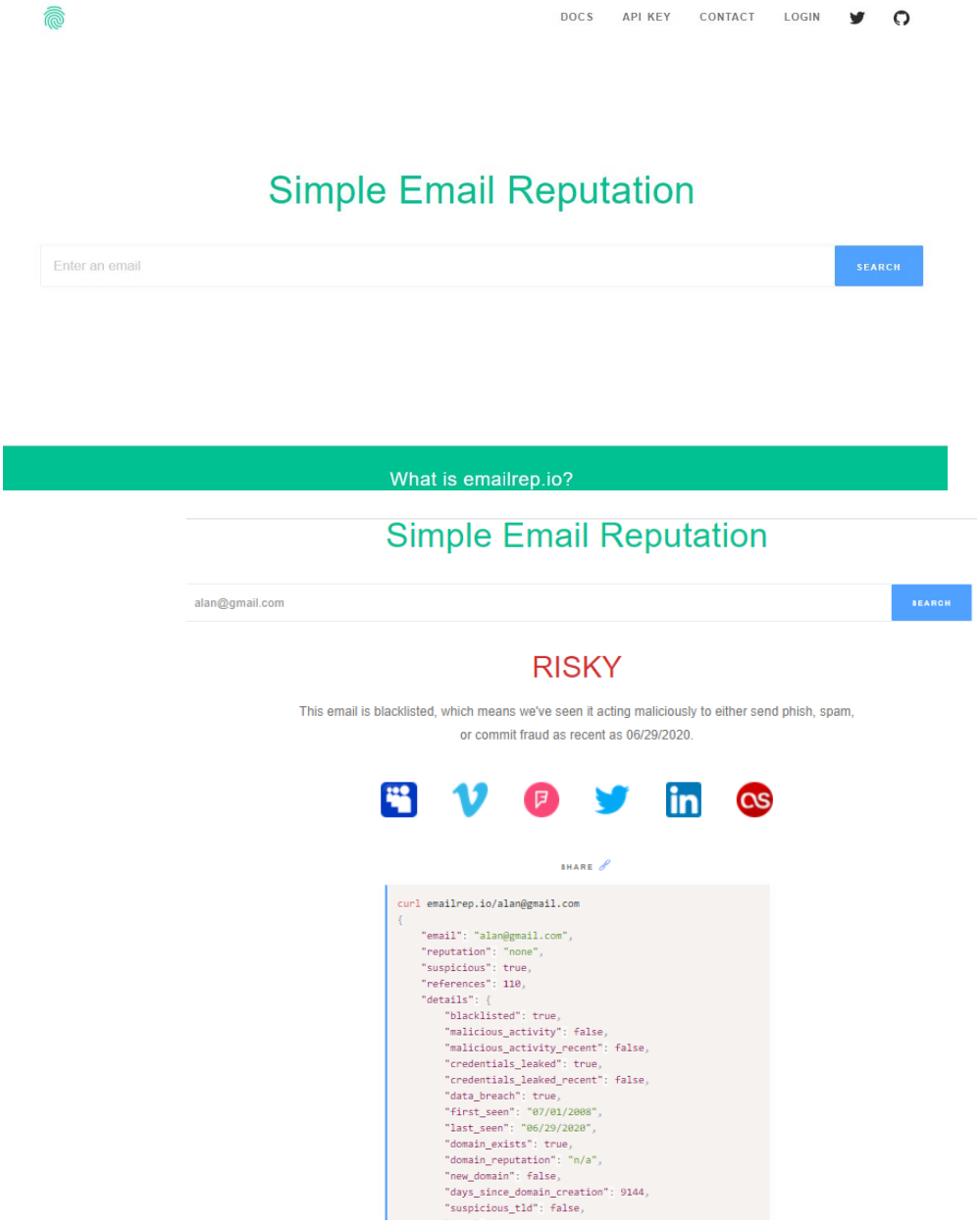
Pastes you were found in

A paste is information that has been published to a publicly facing website designed to share content and is often an early indicator of a data breach. Pastes are automatically imported and often removed shortly after having been posted. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Paste title	Date	Emails
PayPalSucks Database 102k	Unknown	82,071
SevenDollarClick.com_2016_109k	Unknown	109,378
pred.me	Unknown	4,788,657
pxahb.xyz	Unknown	37,782
www.pemiblanc.com	Unknown	2,909,066
xn--e1alhsoq4c.xn--p1ai	Unknown	4,788,657
is-bad-at.tech	Unknown	1,878,845
cdn-14.anonfile.com	Unknown	390,232
cdn-20.anonfile.com	Unknown	107,026
underground-revolution.eu	Unknown	469,452
underground-revolution.eu	Unknown	1,000,166
SevenDollarClick.com_2016_109k	Unknown	109,478
pastedir.com	Unknown	56,236
getamericapraying.com hacked By OPUSA Data Leaked	10 Aug 2013, 19:00	9,885
No title	3 Aug 2014, 17:44	15,394
No title	22 Dec 2014, 13:41	9,585
No title	20 Jan 2015, 15:12	14,554
No title	30 Jan 2015, 06:20	908
Origin Combo | LV Boss	30 Jan 2015, 14:34	14,581
account origin	31 Jan 2015, 09:31	14,401
No title	31 Jan 2015, 21:15	14,401
No title	8 Feb 2015, 11:20	4,308
Gaming Sites Huge Email Combo	13 Feb 2015, 22:47	14,448
iki	15 Feb 2015, 05:51	14,448

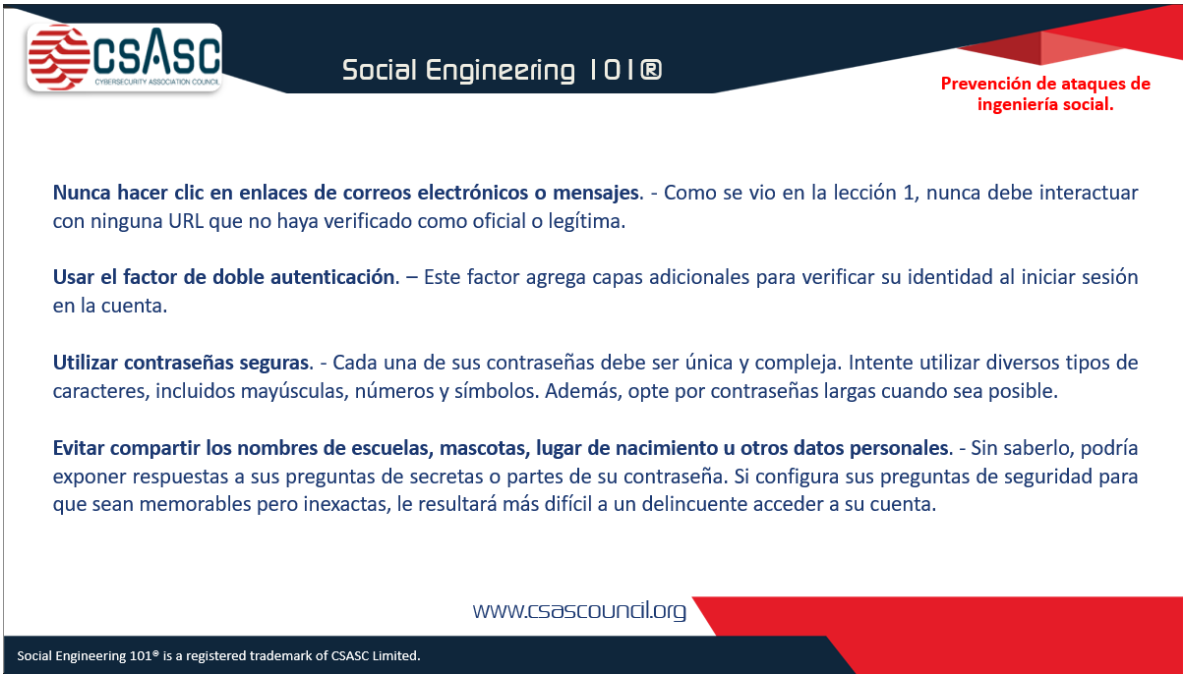
Emailrep

Esta página tiene una función similar a la anterior y su forma de utilizar es la misma, solo basta ingresar a https://emailrep.io/ y escribir el correo del cual se desea obtener información. La diferencia radica en la entrega de los resultados, pues mientras en Have I been pwned se mostraban las páginas donde se llevo a cabo la divulgación de los datos, en Emailrep también verifican otros datos como: checar la reputación que un correo electrónico puede llegar a tener, verificar si el correo se usa para hacer spam, los sitios donde se encuentra registrado el correo, entre otros.



Prevención de ataques de ingeniería social.

Prevenir los ataques de ingeniería social es increíblemente importante para todos los usuarios de dispositivos móviles y computadoras, pues más allá de detectar un ataque, también puede ser proactivo con respecto a su privacidad y seguridad.



a) **Nunca hacer clic en enlaces de correos electrónicos o mensajes**. - Como se vio en la lección 1, nunca debe interactuar con ninguna URL que no haya verificado como oficial o legítima.

b) **Usar el factor de doble autenticación**. – Este factor agrega capas adicionales para verificar su identidad al iniciar sesión en la cuenta.

c) **Utilizar contraseñas seguras**. - Cada una de sus contraseñas debe ser única y compleja. Intente utilizar diversos tipos de caracteres, incluidos mayúsculas, números y símbolos. Además, opte por contraseñas largas cuando sea posible.

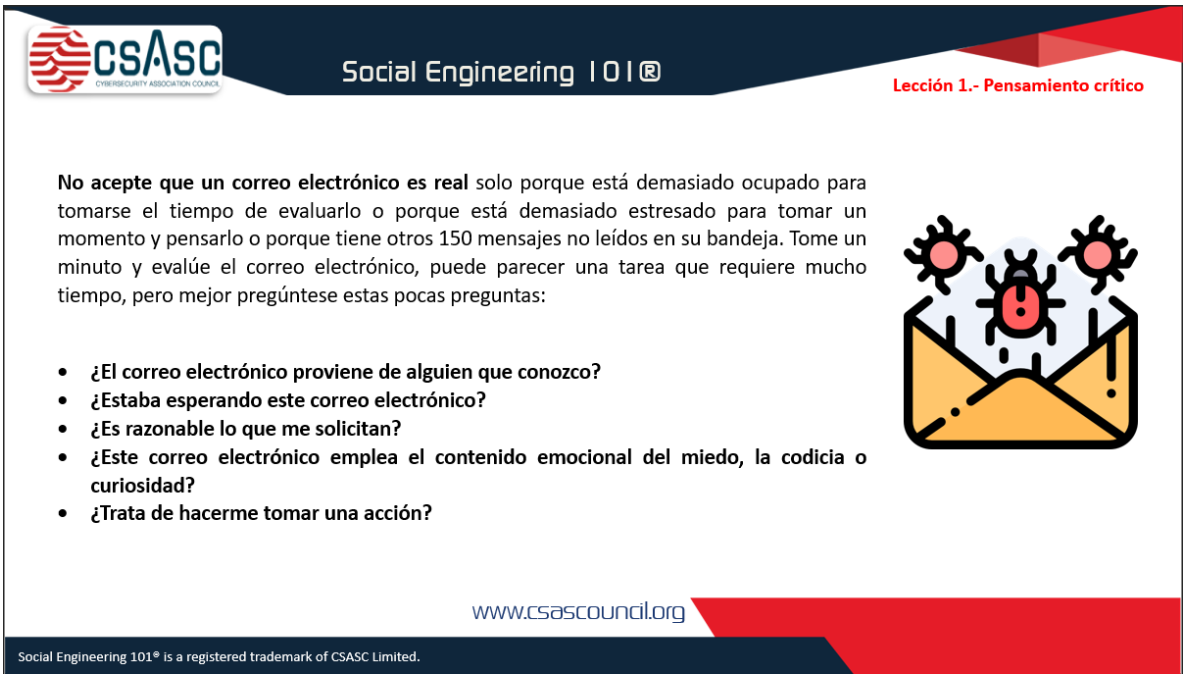
d) **Evitar compartir los nombres de escuelas, mascotas, lugar de nacimiento u otros datos personales**. - Sin saberlo, podría exponer respuestas a sus preguntas de secretas o partes de su contraseña. Si configura sus preguntas de seguridad para que sean memorables pero inexactas, le resultará más difícil a un delincuente acceder a su cuenta.

e) **Nunca dejar los dispositivos sin seguridad en público.** - Siempre bloquee su computadora y dispositivos móviles, especialmente en el trabajo, cuando utilice sus dispositivos en espacios públicos como aeropuertos y cafeterías, téngalos siempre en su poder.

f) **Mantener todo software actualizado tan pronto como sea posible.** - Cuando omite o retrasa las actualizaciones de su sistema operativo o aplicaciones, está dejando agujeros de seguridad conocidos, expuestos para que los ciberdelincuentes los aprovechen.

g) **Mantener seguros todos los dispositivos y servicios conectados a la red**. - Asegúrese de proteger los dispositivos que comúnmente se pasan por alto, como son: sistemas de entretenimiento para automóviles y routers en casas y oficinas. Las filtraciones de datos en estos dispositivos podrían impulsar la personalización de una estafa de ingeniería social.

Lecciones para protección del phishing



Lección 1.- Pensamiento crítico

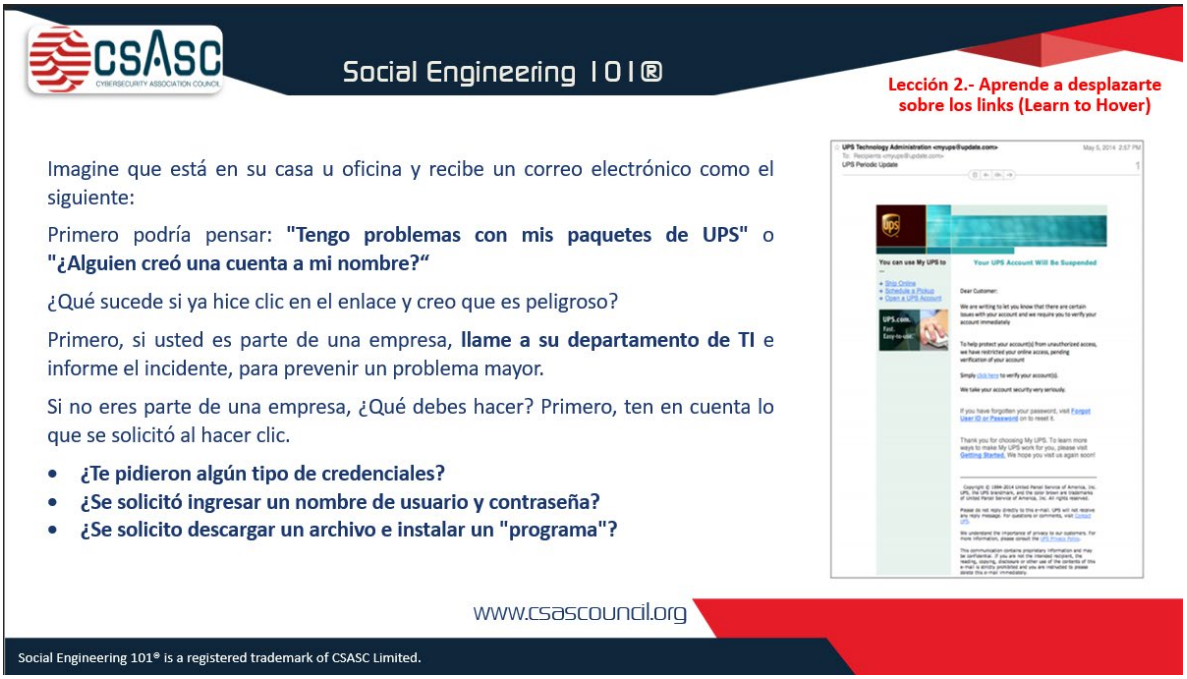
No acepte que un correo electrónico es real solo porque está demasiado ocupado para tomarse el tiempo de evaluarlo o porque está demasiado estresado para tomar un momento y pensarlo o porque tiene otros 150 mensajes no leídos en su bandeja. Tome un minuto y evalúe el correo electrónico, puede parecer una tarea que requiere mucho tiempo, pero mejor pregúntese estas pocas preguntas:

- **¿El correo electrónico proviene de alguien que conozco?**
- **¿Estaba esperando este correo electrónico?**
- **¿Es razonable lo que me solicitan?**
- **¿Este correo electrónico emplea el contenido emocional del miedo, la codicia o curiosidad?**
- **¿Trata de hacerme tomar una acción?**

Solo toma dos o tres segundos cada una de esas preguntas y contestarlas puede hacer que su capacidad de detectar correos electrónicos de phishing sea 100 veces mejor.

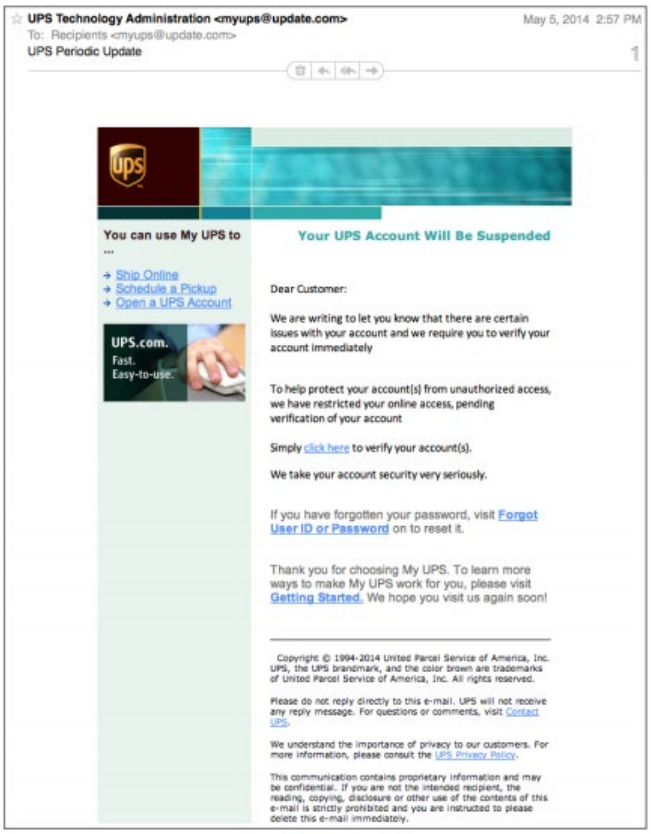
¿Cómo se pueden burlar estas preguntas?

Los atacantes no quieren que pienses críticamente, para eso pueden tratar de utilizar las emociones para apagar su pensamiento crítico (amígdala hijacking) e intentar elevar tus niveles de miedo, tristeza o enojo para lograr que se aplique una acción que no deberías. Cuando estás leyendo un correo electrónico inesperado, de alguien que no conoces y te está causando una respuesta emocional, toma unos segundos antes de ejecutar cualquier medida.



Lección 2.- Aprende a desplazarte sobre los links (Learn to Hover)

Imagine que está en su casa u oficina y recibe un correo electrónico como el siguiente:

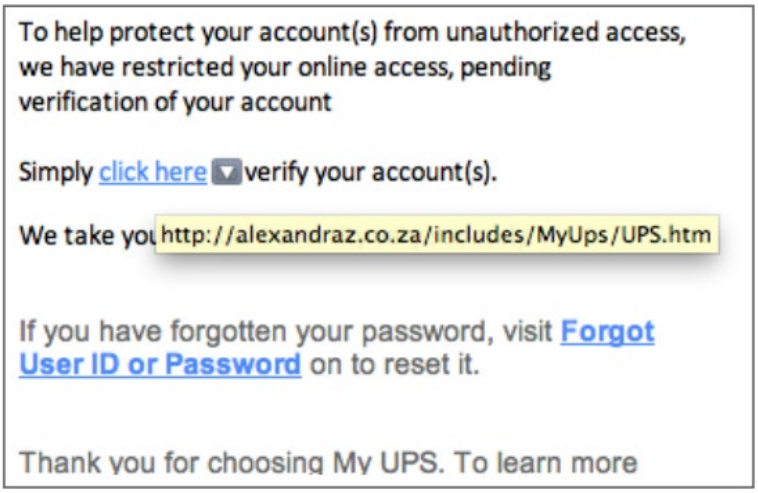


Primero podría pensar: **"Tengo problemas con mis paquetes de UPS"** o **"¿Alguien creó una cuenta a mi nombre?"**

De cualquier forma, **la incertidumbre o la curiosidad** pueden provocar dar clic en el enlace. El correo electrónico parece legítimo e incluso se ve como otros correos electrónicos de UPS que pudo haber recibido en el pasado; todos estos puntos cosas agregan peso a su creencia de que es un correo electrónico real.

¿Qué deberías hacer en estos casos?

Simplemente **mueva el puntero del mouse** sobre el enlace, **¡SIN HACER CLIC!**, deberías ver algo similar a lo siguiente:



Se **reveló el destino de la URL** y ese destino **NO** es UPS, ahora aplica la lección uno y podrá concluir que este correo electrónico puede ser etiquetado como phishing. **La clave es NO hacer clic en este enlace y eliminar el correo electrónico de inmediato.**

¿Qué sucede si ya hice clic en el enlace y creo que es peligroso?

Primero, si usted es parte de una empresa, **llame a su departamento de TI** e informe el incidente, para prevenir un problema mayor.

Si no eres parte de una empresa, ¿Qué debes hacer? Primero, ten en cuenta lo que se solicitó al hacer clic.

- **¿Te pidieron algún tipo de credenciales?**
- **¿Se solicitó ingresar un nombre de usuario y contraseña?**
- **¿Se solicito descargar un archivo e instalar un "programa"?**

Si el sitio solicitó usuario y contraseña y fueron ingresadas, **debe tomar acciones inmediatas**, determine si usa ese mismo usuario y contraseña en cualquier otro lugar y realice el cambio de contraseña lo antes posible.

Si instaló un programa como resultado del correo electrónico, es probable haya instalado un virus, un troyano u otro software malicioso. Necesita limpiar su computadora y cambiar la mayor parte de los nombres de usuario y las contraseñas de su cuenta en otra máquina limpia (o puede hacerlo en su propia máquina justo después de limpiarla).

Monitoree sus cuentas importantes y asegúrese de que no se presenten comportamientos anómalos.

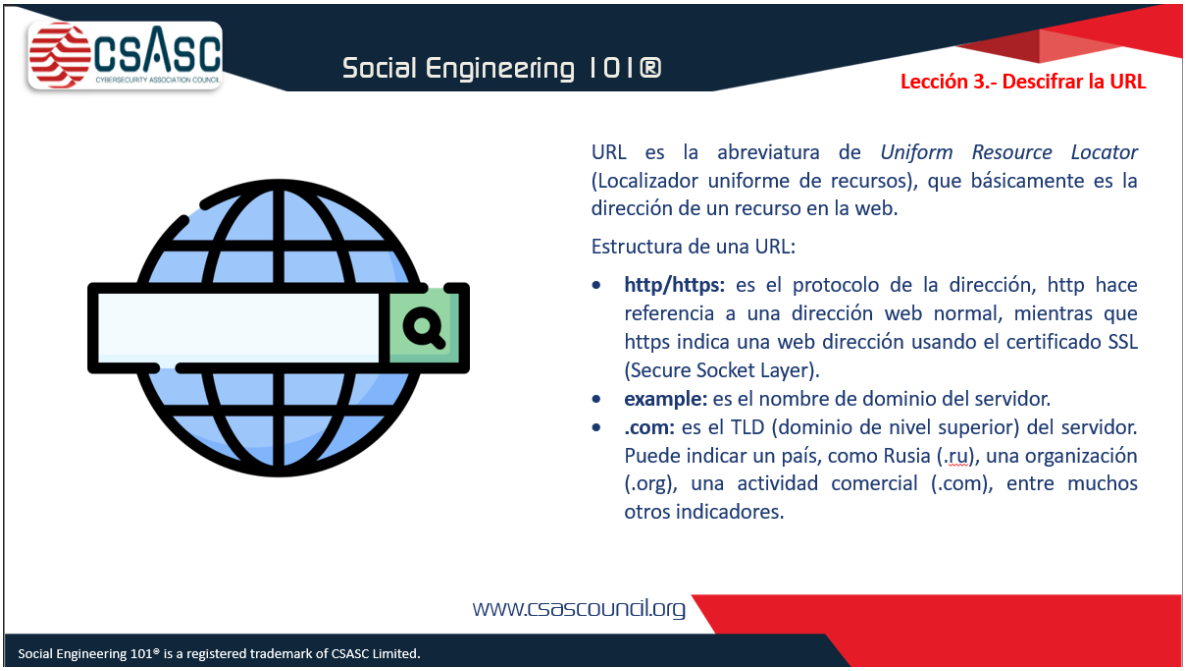
Cuando recomendamos no entrar en pánico, no nos referimos a que no debería tener un sentido de urgencia. Debe hacer estas cosas tan pronto como sea posible, pero enloquecer solo empeora una mala situación. Tome una respiración profunda, forme un plan de acción y fije las cosas que se pueden arreglar inmediatamente para detener cualquier daño adicional que ocurra.

¿Cómo se puede burlar esta lección?

Los ciberdelincuentes pueden comprar dominios que se parecen mucho a dominios legítimos, si un atacante ha comprado y posee el dominio **https://secure-YOURBANK.com**, y pasa el mouse sobre este, vas a tener la impresión de que estás viendo un dominio "correcto", que puede hacer que confíes lo suficiente como para hacer clic.

Otros ataques pueden implicar el registro de certificados para hacer que el sitio parezca legítimo y seguro. Los certificados también pueden tener nombres complicados, y además estar usando “**trusted**”, “**secure**” u otras palabras que están destinadas a hacerte confiar en ellas y sentirte seguro haciendo clic en los enlaces. Por último, pueden enviar correos electrónicos de servidores legítimos que tienen comprometidos.

Se muy cauteloso y siempre debes estar alerta, **analizar los links ayudara a mantenerte seguro.**



Lección 3.- Descifrar la URL

URL es la abreviatura de *Uniform Resource Locator* (Localizador uniforme de recursos), que básicamente es la dirección de un recurso en la web.

https://example.com

Estructura de una URL:

- **http/https:** es el protocolo de la dirección, http hace referencia a una dirección web normal, mientras que https indica una web dirección usando el certificado SSL (Secure Socket Layer).
- **example:** es el nombre de dominio del servidor.
- **.com:** es el TLD (dominio de nivel superior) del servidor. Puede indicar un país, como Rusia (.ru), una organización (.org), una actividad comercial (.com), entre muchos otros indicadores.

Después del TLD puede ver una barra inclinada (/) y lo que viene después puede ser un **directorio** donde el recurso que busca está alojado.

¿Por qué es tan importante entender esto?

Los ciberdelincuentes dependen de su falta de conocimiento para engañarle. Por ejemplo, si necesita descarga de Microsoft un archivo llamado file.txt, ¿puede determinar cuáles de las siguientes URL´s son legítimas a un sitio de Microsoft.com? y cuáles son un peligro potencial.

- ***http://secure-microsoft.com/file.txt***
- ***https://microsof.com/file.txt***
- ***http://microsoft.com/secure/file.txt***
- ***http://rnicrosoft.com/file.txt***
- ***http://microsoft.com/file.txt***

Veamos los resultados.

Con el **primero** tiene que ser cauteloso, secure-microsoft.com podría no ser propiedad de Microsoft. El **"-"** significa que es un dominio completamente diferente que *microsoft.com*.

El segundo pareciera legítimo, pero. si ponemos mucha atención observara que el domino está mal escrito, le hace falta una **t** al final de la palabra Microsof, son muy comunes estas prácticas en los cibercriminales, por ejemplo, I (i mayúscula) y l (L minúscula).

La tercera opción es legítima, solo que se localiza en el directorio secure.

La cuarta opción es complicada, ¿no? Mire cuidadosamente.

No es m-i-c-r-o-so-f-t; es r-n-i-c-r-o-s-o-f-t. Cuando una R y una N minúsculas se colocan lo suficientemente juntos, se ven como una M minúscula.

La quinta opción es legítima a pesar de que usa “http”, se conecta a un sitio real de Microsoft.

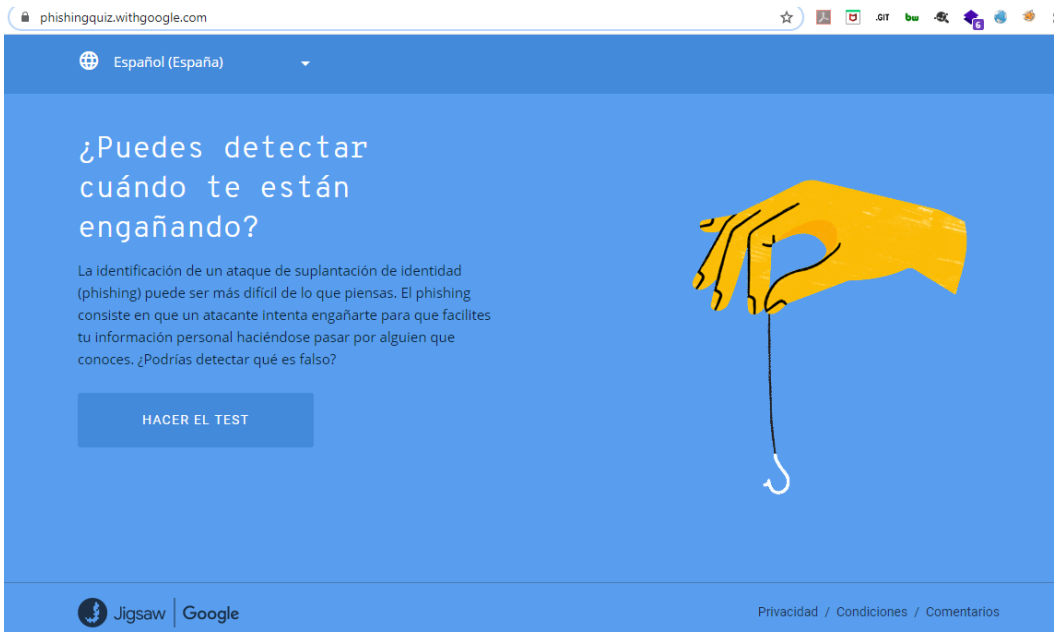
Estas son algunas de las tácticas que utilizan los cibercriminales para engañar a sus víctimas, por esto, la importancia de aprender a descifrar las URL.

¿Cómo se puede burlar esta lección?

Similar a la lección pasada, los atacantes pueden comprar dominios que parecen legítimos, o comprometiendo servidores legítimos en todo el mundo para enviar correos electrónicos de phishing.

Cuestionario de Phishing

Para hacer conciencia acerca del phishing, Google creo un cuestionario gratuito y disponible en línea donde el usuario que lo resuelve debe identificar si el correo mostrado en pantalla es legítimo o es phishing, para acceder al cuestionario basta ingresar a la siguiente liga: https://phishingquiz.withgoogle.com/.

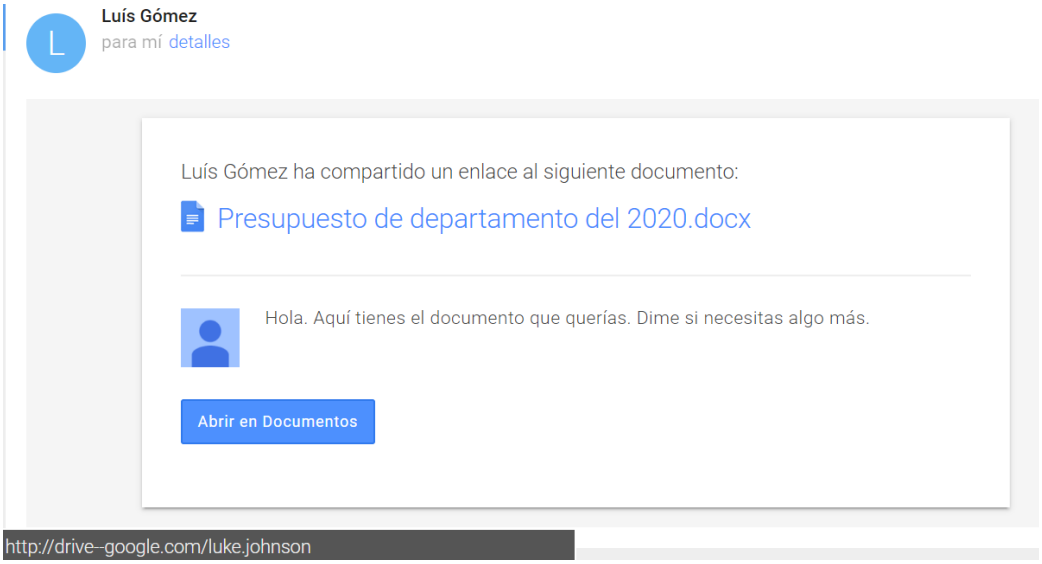


Se le pedirá ingresar nombre y un correo electrónico, puede poner sus datos verdaderos o datos falsos, la finalidad es hacer más realista el cuestionario.

Al dar clic, el cuestionario inicia.

1. Presupuesto del departamento

En este reto se presenta un correo que envía Luis Gómez donde comparte el documento “Presupuesto de departamento del 2020.docx”, el correo de Luis, aunque no tiene el mejor formato, se percibe legítimo, pero qué pasa al desplazar el mouse sobre el archivo que nos compartió.



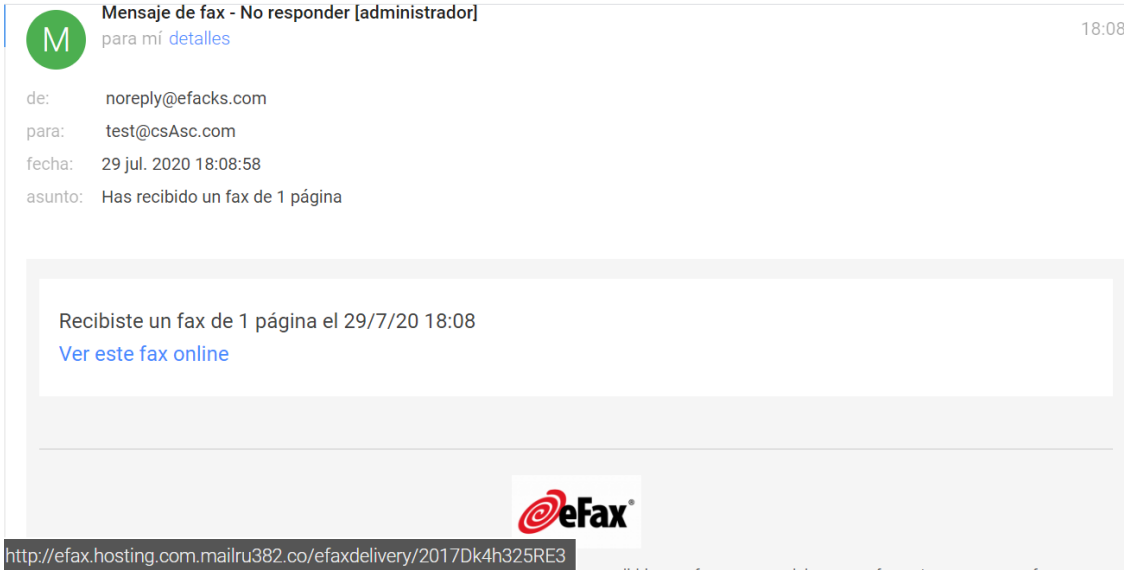
En la esquina inferior izquierda aparece la página *http://drive-google.com/luke.johnson*, que al hacer clic serán redirigidos, ¿qué hay de malo con esta página?, el dominio al que pertenece es **drive-google.com**, que no es un dominio oficial de Google, por otro lado, apunta al directorio **luke.johnson**, que no parece tener relación con la empresa, por lo que este correo se puede catalogar como phishing.

2. Has recibido un Fax

En el segundo reto se presenta el aviso de un fax entrante.

La plantilla del mensaje luce legítima, sin embargo, la dirección de correo del emisor *noreply@efacks.com* no está escrito como el nombre de la empresa que presume mandar el Fax, además, al deslizar el mouse sobre “Ver este fax online”, en la esquina inferior

izquierda se muestra la url a la cual será redirigido el usuario al hacer clic, ¿qué hay de malo con esta url?

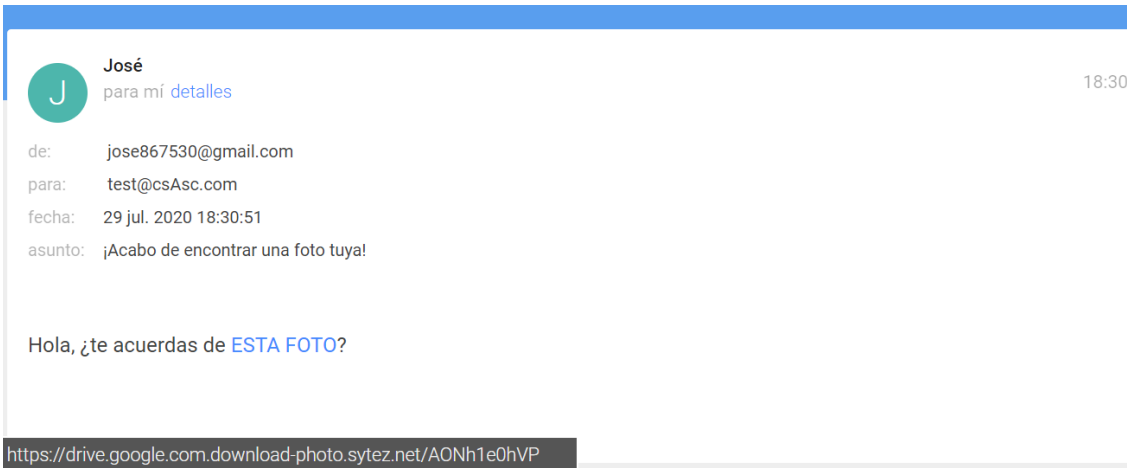


El dominio de la página es **mailru382.com**, el subdominio es **efax.hosting.com** y el directorio es **/efaxdelivery/2017Dk4h325RE3**, por lo que realmente se estaría accediendo a **mailru382.com**, el cual no tiene relación con eFax, por lo cual este correo es catalogado como phishing.

3. El baúl de los recuerdos.

Hoy en día es poco comun recibir fotos a través del correo electrónico.

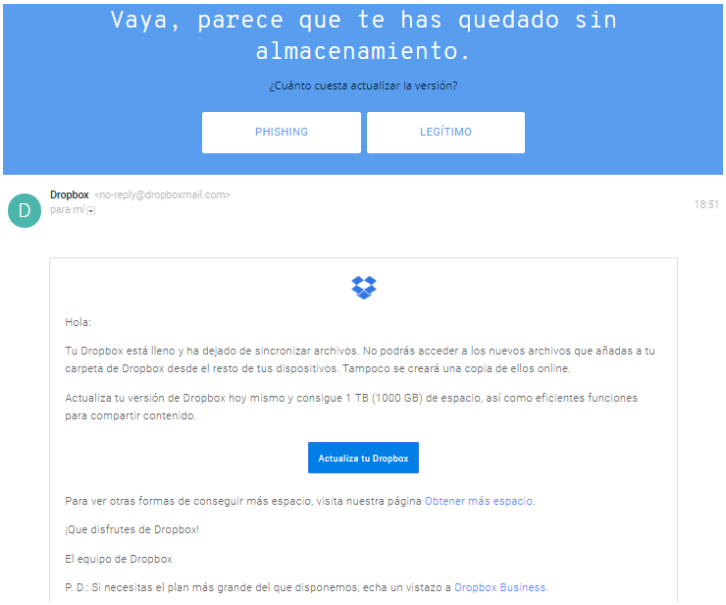
Un individuo llamado José nos comparte una foto, el mensaje es corto y claro, el correo electrónico parece legítimo, pero al desplazarnos sobre "*ESTA FOTO*" muestra el destino al cual será redirigido el usuario al hacer clic, ¿qué pasa con este link?.



El dominio de la url es **sytez.net**, el subdominio es **drive.google.com.download-photo** y el directorio es **/AONh1eOhVP**, por lo que realmente se estaría accediendo a **sytez.net**, por lo cual este correo es catalogado como phishing.

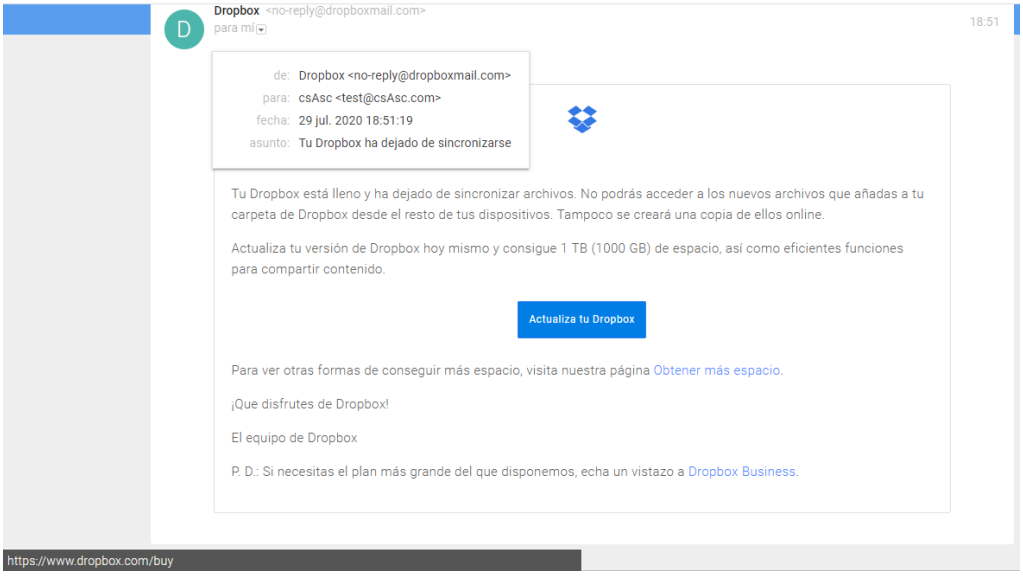
4. Actualizar Dropbox

Siempre es recomendable tener las versiones más recientes de las aplicaciones, en teoría suelen ser más seguras para los usuarios.



Dropbox es una plataforma famosa por haber sido hackeada hace algunos unos años.

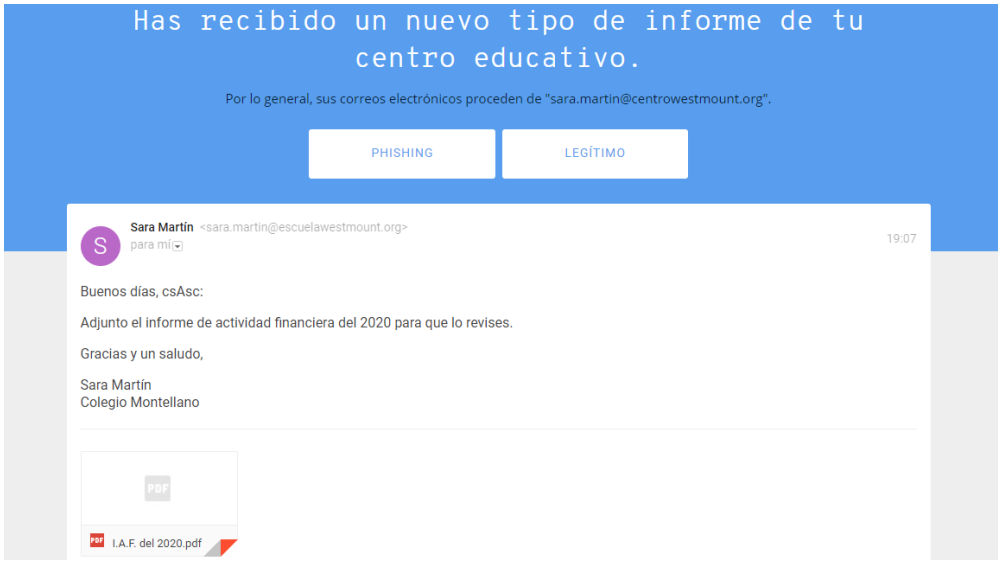
Recibe un correo electrónico mencionando que su cuenta se ha quedado sin almacenamiento, ¿Cómo saber si realmente Dropbox mandó esto?



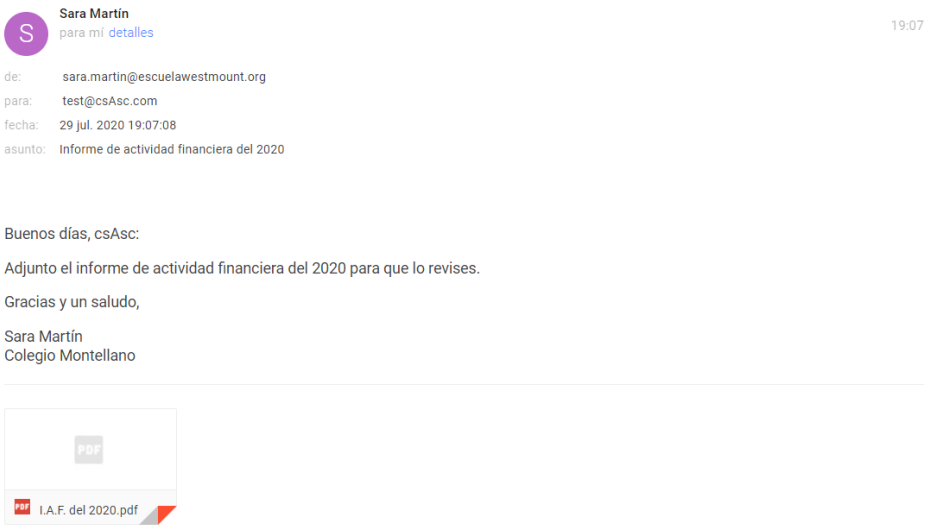
El correo del remitente se percibe legítimo, las url´s a redirigir apuntan a un dominio legítimo, probablemente la plantilla no es la que realmente usa Dropbox, pero ese no es motivo suficiente para catalogar este correo como phishing, por lo que este correo es legítimo.

5. Actividad Financiera 2020

Siempre es buena idea asegurarse de revisar los dominios de los correos entrantes y la institución remitente.



Sara Martín, manda un archivo pdf correspondiente al Informe de la actividad financiera del 2020, el pdf podría contener malware, aunque no es posible saberlo. Lo extraño de este mensaje es el dominio del correo de Sara Martín (Escuela Westmount), y el colegio en el cual dice trabajar (Colegio Montellano).

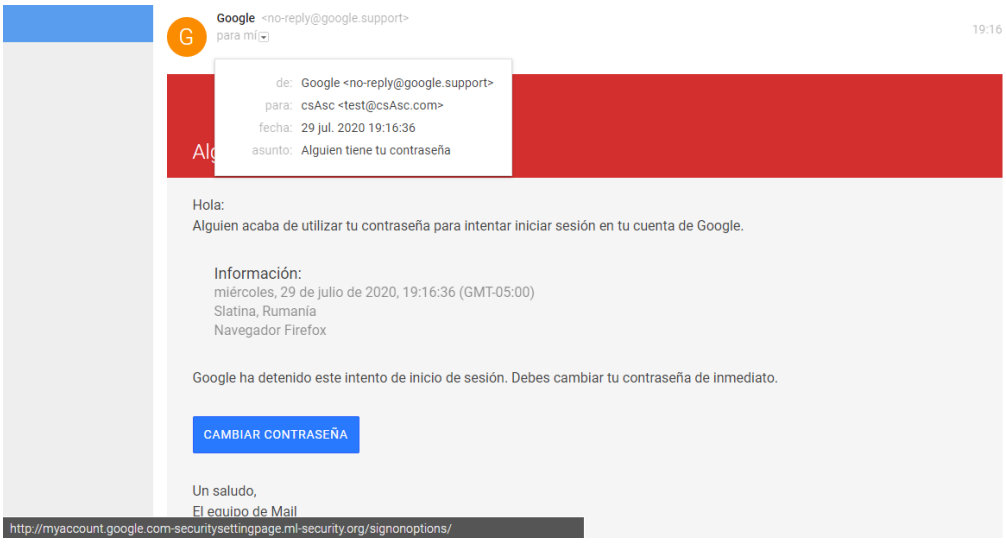


La discrepancia entre el dominio y el nombre del colegio donde labora Sara Martín puede no ser suficiente para catalogar el correo entre legítimo y phishing, sin embargo, es algo que no se puede dejar pasar por alto, por lo tanto, este correo se cataloga como phishing.

6. Cambiar contraseña

Es común recibir correos de este tipo, pero cómo saber cuándo realmente se debe cambiar la contraseña y cuando no es necesario.

El remitente del mensaje es *no-reply@google.support*, este dominio puedo no levantar sospechas, el mensaje es claro y preciso, pero al deslizar el mouse sobre el botón "*Cambiar Contraseña"* la url que aparece en la esquina inferior izquierda es sospechosa.

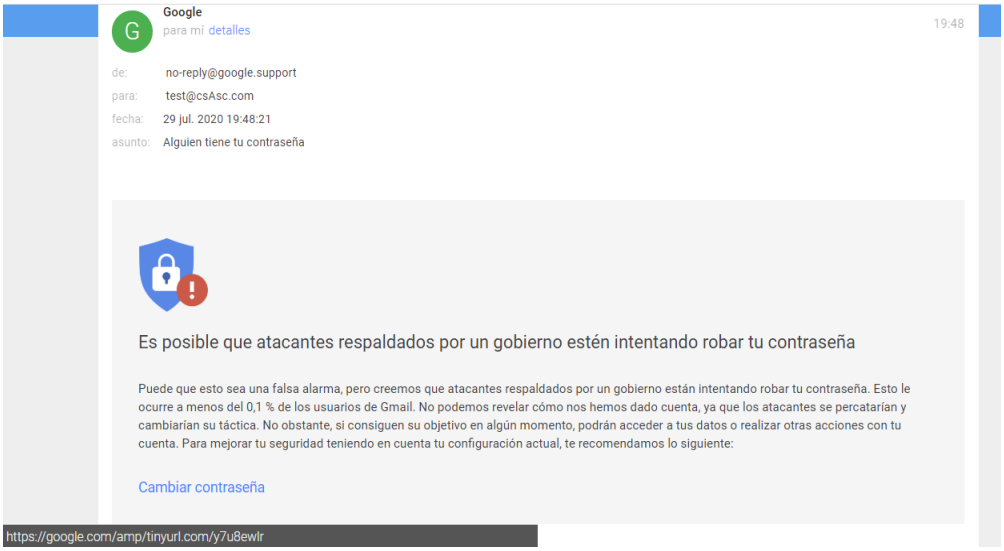


El dominio de la url es **ml-security.org**, el directorio es **/signonoptions** y el subdominio es **myaccount.google.com-securitysettinpage**, por lo que realmente se estaría accediendo a **ml-security.org**, el cual no parece pertenecer a Google, por lo tanto, este correo se cataloga como phishing.

7. El gobierno me hackea

En épocas de elecciones este tipo de correos suele ser bastante frecuente, ¿cómo detectar si es falso o verdadero?.

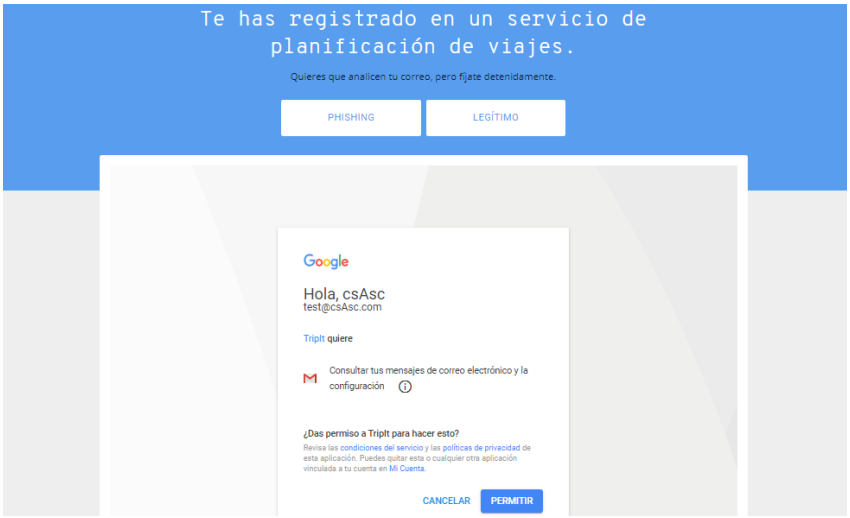
El remitente es *no-reply@google.support*, no levanta sospechas a primera instancia, el mensaje trata de causar emociones en el lector -eso puede ser un indicador de que algo no va bien-. Sin embargo, al desplazar el mouse sobre "*Cambiar contraseña"* la url que se revela en la esquina inferior izquierda es sospechosa.



El dominio de la url es **com/amp/tinyurl.com**, el directorio es /**y7u8ewlr** y el subdominio es **google**, por lo que realmente se estaría accediendo a **com/amp/tinyurl.com**, el cual no parece pertenecer a Google, por lo tanto, este correo se cataloga como phishing.

8. Vámonos de viaje

Es normal que al registrarse en aplicaciones para reservar autos, hoteles y viajes pidan autorización para usar servicios de Google.



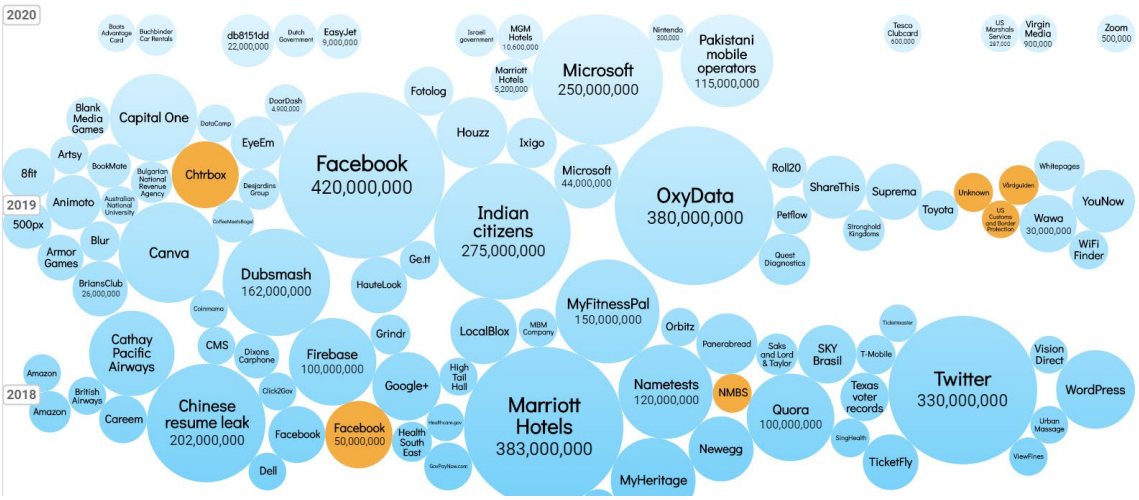
El nombre de la aplicación es legítimo; el permiso que solicita la aplicación *Consultar tus mensajes de correo electrónico y la configuración* es bastante peculiar, sin embargo, no hay motivos para decir que este correo es phishing, por lo que será considerado como legítimo.

Conclusión

Como ya hemos mencionado, en varias ocasiones resulta mas rentable, desde el punto de vista del ataque, aprovecharse del comportamiento de las personas, que explotar vulnerabilidades técnicas asociadas a los sistemas de información.

Podemos concluir que tener entrenado a los colaboradores es clave para ayudar a mantener segura tu organización, sin embargo, se recomienda ampliamente hacer auditorias de seguridad conocidas como análisis de vulnerabilidades y/o pruebas de penetración, para evitar el robo de información, ya que cada **año son millones los datos que se roban.**

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Notas:

Notas: