



Curso de

Introducción a la Ingeniería Social: Técnicas, Ataques y Pretexting

Dra. Aury Curbelo

Introducción a la ingeniería social

Disclaimer Renuncia de responsabilidad

Disclaimer

Todo lo que se enseña en este curso es solo para propósitos educativos.

La Dra. Aury Curbelo no se hace responsable de los usos no educativos que puedan surgir durante o luego del curso.

¿Quién soy yo?

- Certified Social Media Examiner (CSME)
- Certified Dark Web Investigator (CDWI)
- Certified Data Privacy Solution Engineer (CDPSE)
- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator Certification (CHFI)



¿Quién soy yo?

- ISO 27001 Lead Auditor
- Security +
- ITIL V3
- CNSS/NSA 4011
Information Systems
Security Professional
- CNSS/NSA 4012 Senior
Systems Manager



Social Engineering Test



All rights reserved to Social-Engineer, Inc., 2014
No part of this publication, including its design, may be reproduced, transferred or otherwise
transferred to its copyright owner, including photocopying and other copying, any transfer or transmission
using any network or other means of communication, any broadcast for distant learning, in any form or by
any means such as any information storage and retrieval system, without prior written
permissions from the author.

Page 1 of 22



Agenda

Introducción

- Bienvenida al curso.
- Presentación de la profesora.
- Antecedentes de la ingeniería social:
definirla.
- ¿Por qué funciona la ingeniería social?
- Perfil del ingeniero social.

Agenda

Los principios de la ingeniería social

- Metas de la IngeSoc.
- Principios.
- Persuasión.
- Aspectos legales y éticos de la IngeSoc.

Agenda

Tipos de ingeniería social

- Basada en humanos.
- Basada en computadora/tecnología.

Tipos de ataques de ingeniería social

- Taxonomía de los ataques.

Agenda

Elicitación

- Por qué es exitosa.
- Técnicas de elicitation.

Agenda

Pretexting

- ¿Qué es el pretexting?
- Ejemplos de pretexting.
- ¿El pretexting es ilegal?
- Proceso de planificación de pretexting.

Agenda

Deepfake

- ¿Qué es el Deepfake?
- Tipos de Deepfake.
- Aplicaciones disponibles para crear Deepfake.
- Relación del DeepFake y la IngeSoc.

Agenda

Deepfake

- Cómo detectar el uso de Deepfake y detener la proliferación de noticias falsas.
- Retos de los procesos de investigación forense en Deepfake.
- Herramientas de detección de Deepfake.

Agenda

Construyendo el muro humano - contramedidas

- Medidas de prevención y protección en contra de la IngeSoc 1/2.
- Medidas de prevención y protección en contra de la IngeSoc 2/2.
- Creando una cultura de seguridad.

Antecedentes de la ingeniería social

Confianza / Desconfianza

THE FIRST BOOK OF MOSES, CAP GENESIS

CHAPTER 1

In the beginning God created the heaven and the earth.

2 And the earth was without form, and void; and darkness was upon the face of the deep.

*And the spirit of God moved upon the face of the deep.

3 *And God said, "Let there be light: and there was light.

4 And God saw the light, that it was good: and God divided light from the darkness.

5 God called the light day, and the darkness he called night.

6 In itself, a

7 saw that

8 13 An

9 mornin

10 14 Q

11 be lig

12 heav

13 the

14 sig

15 d

16 3 Ps. 33:9

17 4 Heb. be-

18 tween the

19 light and

20 darkness

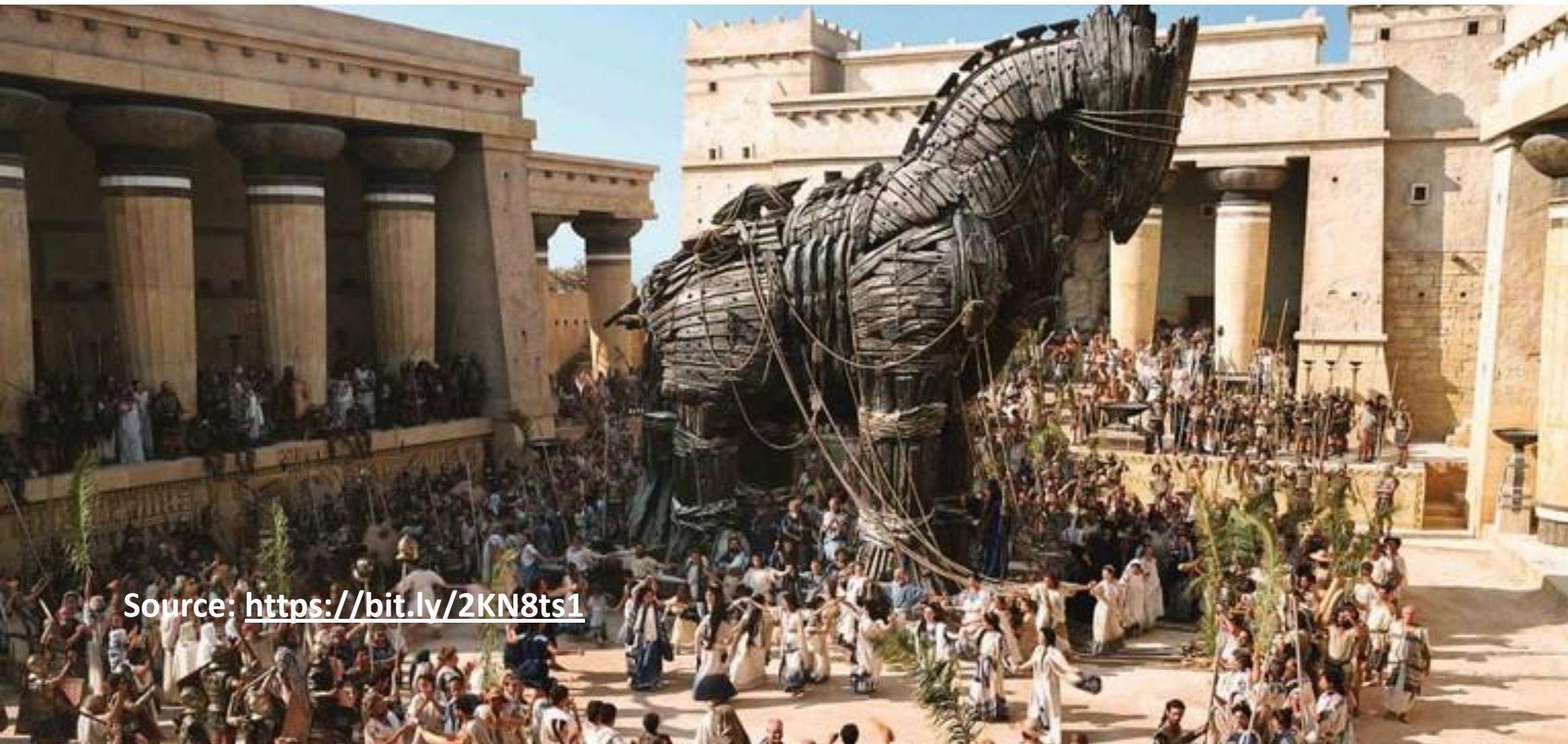
21 5 Ps. 74:1

22 5 Heb. A

23 the eve

24 was, o

Baiting/Carnada



Source: <https://bit.ly/2KN8ts1>

Pretexting - 1960

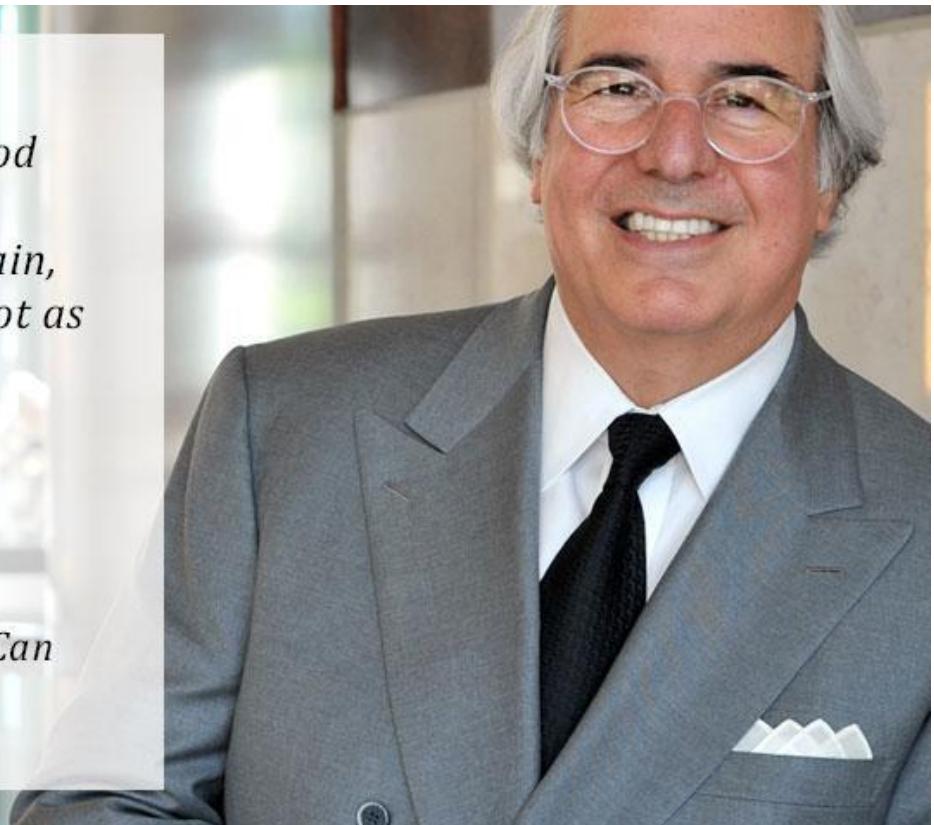
"The vast majority of fraudsters, and criminals get caught not because of good police work, but because they continue doing the same thing over and over again, until someone notices. Criminals are not as bright as people think, and their greed motivates them totally."

- Frank Abagnale

World Expert on Fraud & Cybersecurity

The Inspiration behind Catch Me If You Can

Interviewed by Vikas Shah MBE, @MrVikas
<https://thoughteconomics.com>



Legion of Doom- 1983



Source: <http://phrack.org/issues/31/5.html>

“More on trashing”

September 1984

2600



September, 1984

2600 is published by 2600 ENTERPRISES, INC., an electronicsary organization. Subscription rates: \$10 - 1 year, \$5 - 6 months, \$1 per back issue.
overseas \$13.50 1 year. Write to 2600, Box 752, Middle Island, NY 11953-0752; MCI Mail: 26HUNDRED; TELX: 6501994928

VOLUME ONE, NUMBER NINE

HISTORY OF BRITISH PHREAKING

by Lex Luthor and The Legion of Doom

In Britain, phreaking goes back to the early fifties, when the technique of "Toll A drop back" was discovered. Toll A was an exchange near St. Pauls which routed calls between London and the nearby non-London exchanges. The trick was to dial an unallocated number, and then depress the receiver—rest for $\frac{1}{2}$ second. This flashing initiated the "clear forward" signal, leaving the caller with an open line into the Toll A exchange. He could then dial 018, which forwarded him to the trunk exchange—at that time, the first long distance exchange in Britain—and follow it with the code for the distant exchange to which he would be connected at no extra charge.

The signals needed to control the UK network were published in the *Institution of Post Office Engineers Journal* and reprinted in the *Sunday Times* 15 Oct. 1972. (NOTE: The British Post Office is the U.K. equivalent of Ma Bell.)

The system is called Signalling System No. 3 and it uses pairs of frequencies selected from 6 tones separated by 120Hz. With that info, the phreaks made "Bleepers" or as they are called here in the U.S., blue boxes. The British, though, utilize different MF tones than the U.S., thus your U.S. blue box that you smuggled into the U.K. will not work, unless you change the frequencies. (In the early seventies, a simpler system based on different numbers of pulses with the same frequency (2280Hz) was used. For more info on that, try to get ahold of Atkinson's "Telephony and Systems Technology".

Boxing in Foreign Lands

The following are timing and the frequencies for boxing in the U.K. and other foreign countries. Special thanks to Peter McIvers for the following info:

British "bleeper" boxes have the very same layout as U.S. blue boxes. The frequencies are different, though. They use two sets of frequencies: forward and backward. Forward signals are sent out by the beeper box. The backward signals may be ignored (it's sort of like using full duplex). The frequencies are as follows:

U.S.	700	900	1100	1300	1500	1700 Hz
Fwd	1380	1500	1620	1740	1860	1980 Hz
Blkwrd	1140	1020	900	780	660	540 Hz

For example, change the 900Hz potentiometers in your box to 1500Hz. All numbers 1-0 (10) are in the same order as in an American box. The ones after this are their codes for operator 11, operator 12, space 13, space 14, and 15. One of these is KP, one (probably 15) is Star; it won't be too hard to figure out. The signals should carry -11 dBm +/- 1dB onto the line; the frequencies should be within +/- 4Hz (as is the British equipment). Also, the IVF system is still in operation in parts of the U.K. This would encode all signals 1 to 16 as binary numbers; for instance, a five is 0101. There are six intervals per digit, each .90ms long or a total of 300ms. First is a start pulse of 2280, 50ms. Then, using the example of five (0101), there is a 50ms pause, a 50ms pulse of 2280, a 50ms pause, and a 50ms pulse of 2280. Finally, there is a 50ms pause that signals the end of the digit. The frequency tolerance on the 2280Hz is +/- 0.3%; it is sent at -6 +/- 1dBm. An idle line is signalled by the presence of a 3825Hz tone for more than 650ms. This must be within 4Hz.

Recorder Conner: er: 1800Hz, beeps every 15 seconds.

Multiparty Line Ring: same frequency and modulation as ring, but 1 sec on, 2 sec off (twice as fast).

Titan the Scanner

In the early days of British phreaking, the Cambridge University Titan computer was used to record and circulate numbers found by the exhaustive dialing of local networks. These numbers were used to create a chain of links from local exchange to local exchange across the country, bypassing the trunk circuits. Because the internal routing codes in the U.K. network are not the same as those dialed by the caller, the phreaks had to discover them by "probe and listen" techniques, more commonly known in the U.S. as scanning. What they did was put in likely signals and listen to find out if they succeeded. The results of scanning were circulated to other phreaks. Discovering each other took time at first, but eventually the phreaks became organized. The "TAP" of Britain was called "Undercurrents" which enable British phreaks to share the info on new numbers, equipment, etc.

To understand what the British phreaks did, think of the phone network in three layers of lines: local, trunk, and international. In the U.K., Subscriber Trunk Dialing (STD), is the mechanism which takes a call from the local lines and (legitimately) elevates it to a trunk or international level. The U.K. phreaks figured that a call at trunk level can be routed through any number of exchanges, provided that the right routing codes were found and used correctly. They also had to discover how to get from local to trunk level either without being charged (which they did with a beeper box) or without using (STD). Chaining has already been mentioned but it requires long strings of digits and speech gets more and more faint as the chain grows, just like it does when you stack trunks back and forth across the U.S. The way the security reps snagged the phreaks was to put a simple "printmeter" or pen register, as we call it, on the suspect's line, which shows every digit dialed from the subscriber's line.

The British prefer to get onto the trunks rather than chaining. One way was to discover where local calls use the trunks between neighboring exchanges, start a call, and stay on the trunk instead of returning to the local level on reaching the distant switch. This again required exhaustive dialing and made more work for Titan; it also revealed "fiddles", which were inserted by Post Office Engineers. What fiddling means is that the engineers rewired the exchanges for their own benefit. The equipment is modified to give access to a trunk without being charged, an operation which is pretty easy. In Step by Step (SxS) electromechanical exchanges, which were installed in Britain even in the 1970's,

A famous British "fiddler" revealed in the early 1970's worked by dialing 173. The caller then added the trunk code of 1 and the subscriber's local number. At that time, most engineering test services began with 17X, so the engineers could hide their fiddles in the nest of service wires. When security reps started searching, the fiddles were concealed by tones signalling "number unobtainable" or "equipment engaged" which switched off after a delay. The necessary relays are small and easily hidden.

¿Qué es la ingeniería social?

¿Qué es la ingeniería social?

Visentini (2006):

Es una disciplina que consiste en sacar datos corporativos a otra persona, sin que ésta se dé cuenta de que está revelando "información sensible", y que normalmente no lo haría.

¿Qué es la ingeniería social?



Borghello (2009):

La ingeniería social puede definirse como una acción o conducta social, destinada a conseguir información de las personas cercanas a un sistema.

¿Qué es la ingeniería social?

Se centra en lograr la confianza de las personas para luego engañarlas y manipularlas para el beneficio propio de quien la implementa.



- Reunir información de la víctima.
- Determinar las debilidades de la víctima.
- Elegir un vector de ciberataque adecuado



- Finalizar interacción con la víctima.
- Eliminar todo rastro de malware.
- Cubrir pistas y evidencias.

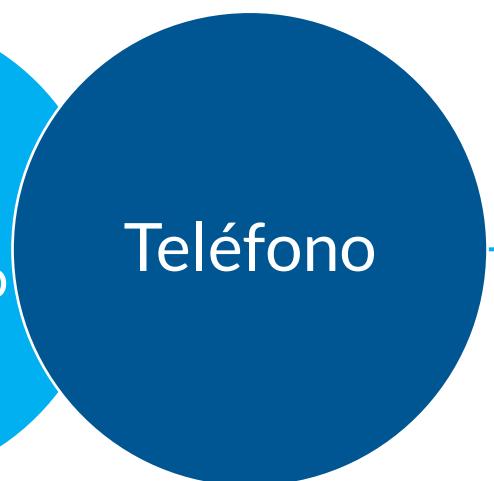
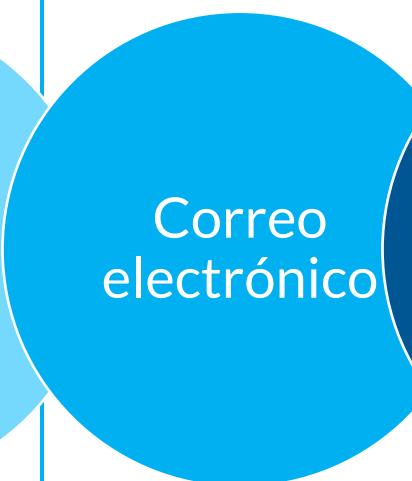
- Atrapar la atención de la víctima.
 - Vender falsas promesas.
 - Retener y manipular a la víctima.
-
- Mantener la historia.
 - Extraer información de la víctima.
 - Ejecutar el ciberataque para hacer uso de los datos obtenidos.

¿Qué puedo hacer con un poco de información?

- Nombre y apellido
- Dirección
- Número de teléfono
- Correo electrónico
- Recibos de luz/agua



- Crear una identidad falsa.
- Hackear su correo electrónico.



- Crear un perfil falso en Facebook.

- Tomar \$\$\$ prestado.
- Abusar del crédito.

- Exponerte a situaciones embarazosas.

¿Cómo y dónde puedo encontrar esa información?

- Nombre y apellido
- Dirección
- Número de teléfono
- Correo electrónico
- Recibos de luz/agua



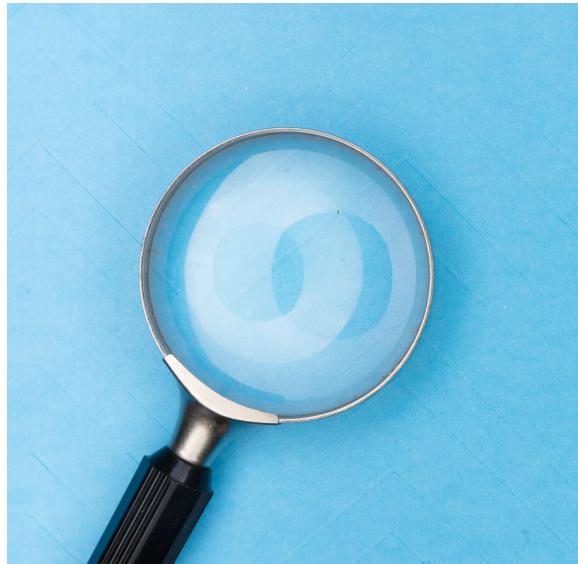
Reglas del compromiso (rules of engagement)

¿Cuándo podemos usar la ingeniería social?

FIN: No es malicioso, está diseñado para **NO** hacer daño.



Pruebas de
penetración de
red/autorizadas.



Investigación.



Comunicaciones
públicas.

Aspectos legales y éticos

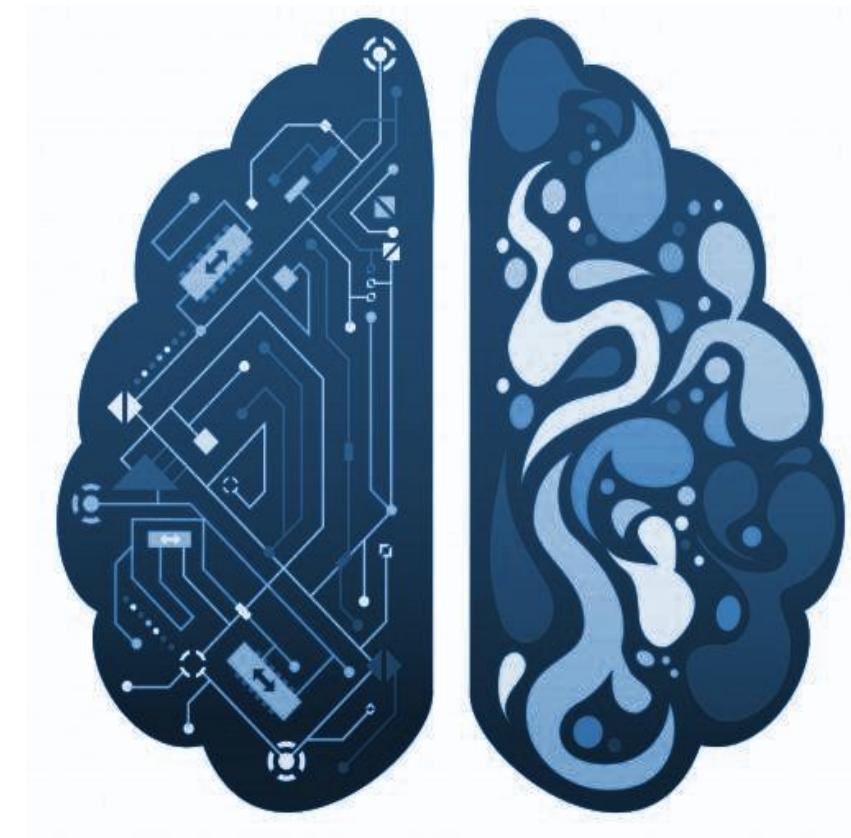
1. ¿Es legal llevar a cabo pruebas de ingeniería social?
2. Discusión de aspectos éticos de la ingeniería social.

¿Por qué funciona la
ingeniería social?

Elementos de la ingeniería social

Ciencias de
cómputo

Psicología
social



¿Por qué la ingeniería social es tan efectiva?

- El campo de la seguridad de la información está enfocado principalmente en seguridad técnica.
- Casi no se presta atención a la interacción máquina-persona.
- Las personas son el eslabón más débil.

¿Por qué la ingeniería social es tan efectiva?

- ¿Por qué gastar tanto tiempo atacando la tecnología si una persona te puede dar acceso?
- Extremadamente difícil de detectar.
- No existe IDS para “falta de sentido común” o ignorancia.

Importancia

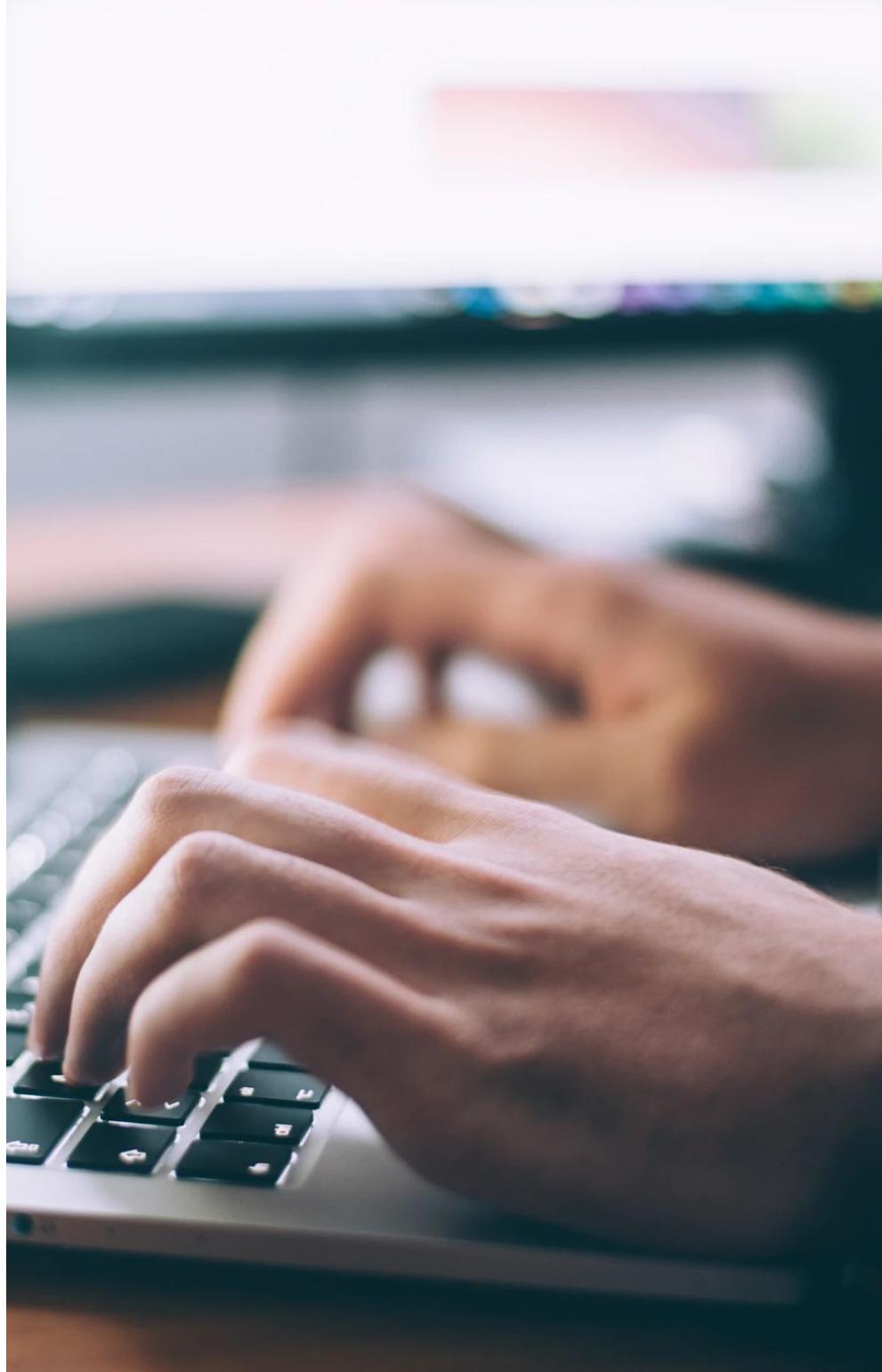
La gente por no querer quedar mal o crear un escándalo, brinda a cualquiera que le solicita, “información sensible”, ahí es donde juega un papel importante la educación, y el enseñarle a los empleados a decir no.

Datos de la ingeniería social

Datos duros

El 80% de los ataques informáticos se deben a errores relacionados con el factor humano y no a temas específicos de tecnología.

Source: <https://bit.ly/3baff5w>



Datos duros

Los incidentes de seguridad de la información son a menudo causados por fallas humanas (Chan, Woon y Kankanhalli, 2005), en lugar de fallas técnicas (Schneier, 2000).

Source: <https://bit.ly/3baff5w>



Datos duros

“La ingeniería social es la técnica más eficaz para hacerse con secretos celosamente protegidos, ya que no requiere de una sólida formación técnica, ni de grandes conocimientos sobre protocolos y sistemas operativos”.

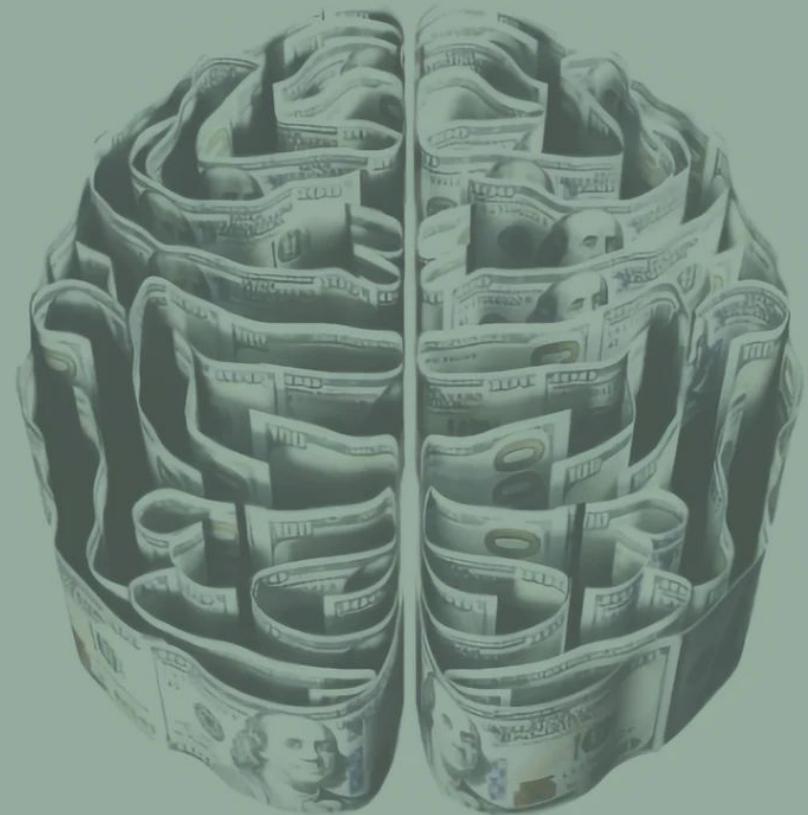
Source: <https://bit.ly/3baff5w>



Datos duros

"Quienes practican la ingeniería social requieren solamente de astucia, paciencia y una buena dosis de psicología".

Source: <https://bit.ly/3baff5w>



Datos duros

La ingeniería social constituye un **riesgo de seguridad** porque se puede utilizar para eludir los sistemas de detección de intrusos, firewalls y sistemas de control de acceso.

Source: <https://bit.ly/3baff5w>

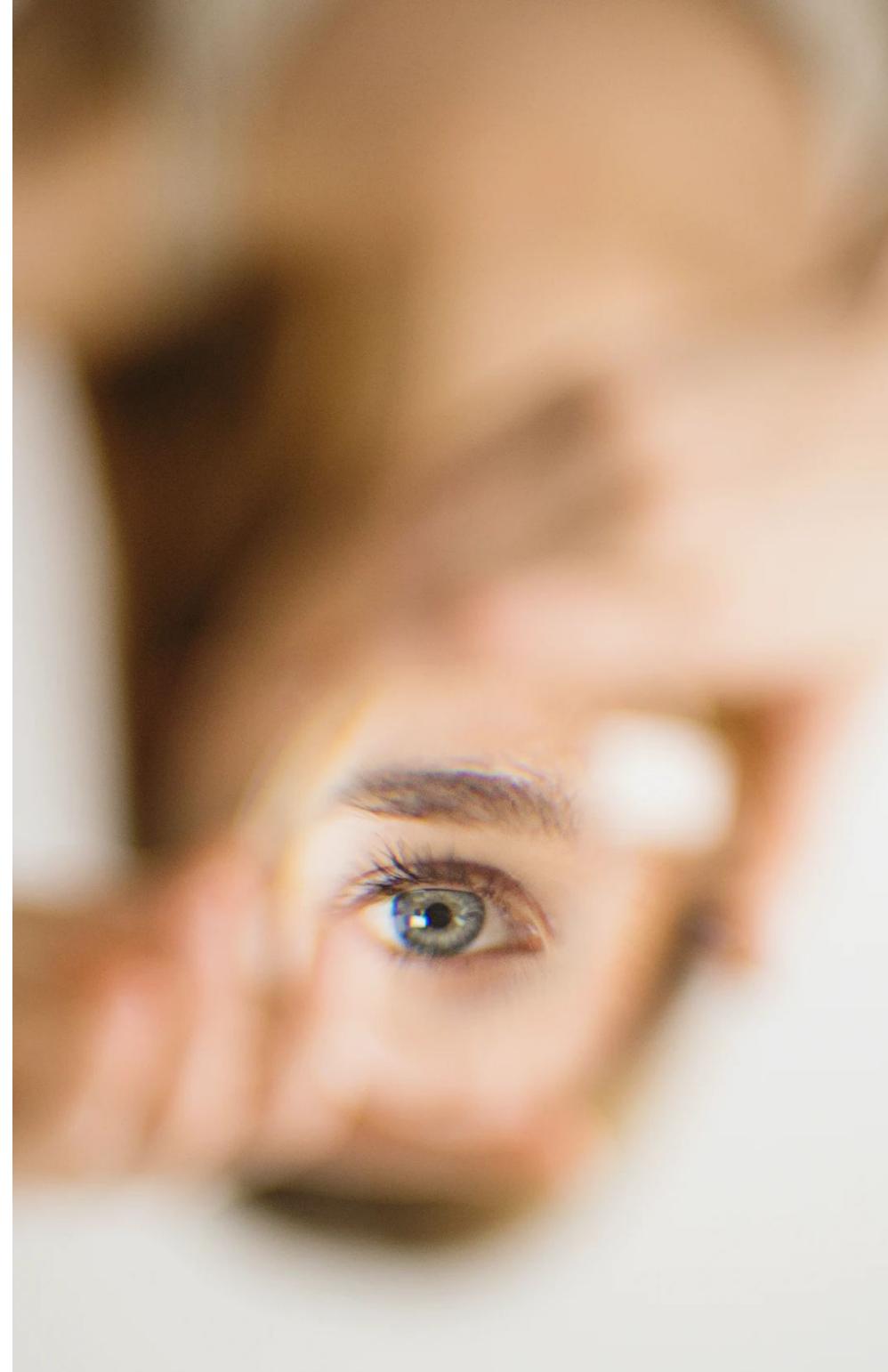


Datos duros

En la mayoría de los casos las personas (objetivos) no se dan cuenta de que están siendo víctimas de ataques de ingeniería social.

(FBI, 2013; Hadnagy y Wilson, 2010).

Source: <https://bit.ly/3baff5w>



Metas de la ingeniería social

Metas de la ingeniería social

Motivos:

- Curiosidad
- Venganza
- Beneficio personal o económico
- Diversión
- Desafío
- Muchos más



Metas de la ingeniería social

Las personas son engañadas para que revelen información confidencial como datos bancarios, contraseñas, etc.

Esta información será usada por los delincuentes para estafar, realizar compras a nombre de otro, enviar spam, etc.

Metas de la ingeniería social

- Acceso a información
- Autorización
- Confianza
- Dinero

Metas de la ingeniería social

- Reputación.
- Cometer fraude.
- Espionaje industrial.
- Robo de identidad.
- Irrumpir en los sistemas/redes.

Personal vulnerable a ataques de ingeniería social en una empresa



Personal administrativo más susceptible a los ataques por ingeniería social

Repcionistas

Vendedores

Personal de nómina

Recursos humanos

Personal de finanzas

Administración de oficinas

Posiciones atractivas para un ingeniero social

- Departamento de recursos humanos.

Información de empleados:

- Estado actual: trabajando, de vacaciones, enfermo, de momento trabajando en un proyecto fuera de la empresa, etc.
- Departamento del empleado.

Posiciones atractivas para un ingeniero social

- Nombre de los colegas.
- Superiores (si el ingeniero social quiere tomar la identidad de uno de ellos en un ataque).
- Condición laboral.
- Información sobre el contrato y el salario de un empleado.

Posiciones atractivas para un ingeniero social

- Gerenciales
- “Newbies”
- “Temporeros”
- “Freelancers”

Posiciones atractivas para un ingeniero social

Help Desk

Responsabilidades:

- Cuentas de usuarios (creación, eliminación, activación, desactivación, reactivación).
- Cambiar contraseñas.
- Instalar software (por razones de seguridad los empleados no deben tener permiso para hacer esto).
- Ofrecer ayuda.

Cómo escoger un buen objetivo

Una persona que:

- Trabaje en áreas donde tenga mucho contacto con el público.
- Sea empleada en una compañía asociada con el objetivo.
- Sea familiar/amigo del objetivo.
- Cuente con amplia presencia en redes sociales.
- Una persona que exhiba la característica de ser muy sociable.

Principios de la ingeniería social

Principios de Kevin Mitnick

Mitnick fundamenta las estrategias de ingeniería social en los siguientes postulados:

- Todos los seres humanos quieren ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir no.
- A todos nos gusta que nos alaben.



Principios de Kevin Mitnick

- La ingeniería social utiliza la **influencia** y la **persuasión** para engañar a la gente.
- El ingeniero social es capaz de aprovecharse de la gente para obtener información con o sin el uso de la tecnología.

Principios de Kevin Mitnick

- Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc.
- Lo único que se necesita es un llamado a un empleado desprevenido. Tienen todo en sus manos.

Principios de persuasión

Robert Cialdini (2009)

Conocido mundialmente como el experto en la ciencia de la persuasión y cómo aplicarla éticamente en los negocios.



Source: <https://bit.ly/38YLgL8>

Principios de persuasión

- Ha pasado toda su carrera realizando investigaciones científicas sobre lo que lleva a las personas a decir "sí" cuando se les solicita algo.
- Toda su investigación se fundamenta en los 6 principios de la persuasión.

Source: <https://bit.ly/38YLgL8>

Los 6 principios de persuasión de Cialdini

- El principio de escasez.
- El principio de prueba social.
- El principio de autoridad.



Los 6 principios de persuasión de Cialdini

- El principio de simpatía.
- El principio de consistencia y compromiso.
- El principio de reciprocidad.

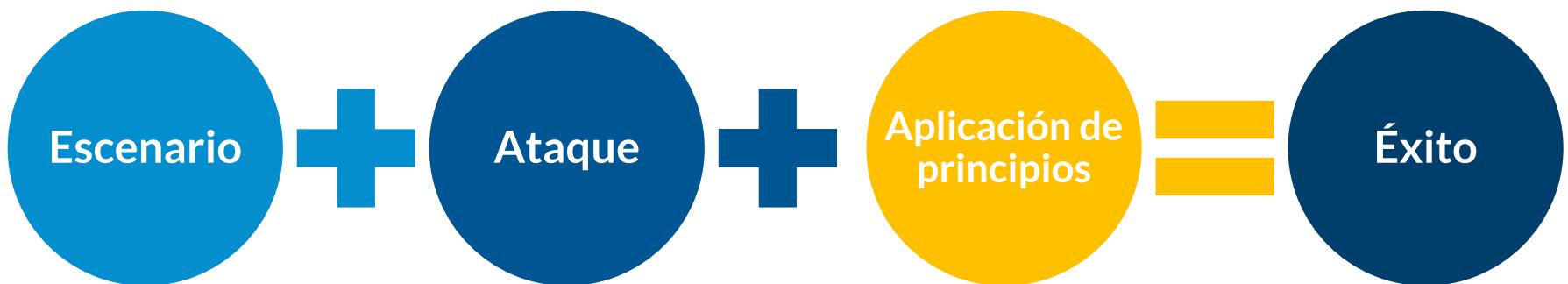


Datos sobre los principios de persuasión de Cialdini

- La persuasión es propiedad del atacante, **NO** de la víctima.
- Para que los principios de persuasión sean efectivos, deben darse en conjunto con un escenario bien planificado y teniendo conocimiento sobre la víctima.

Datos sobre los principios de persuasión de Cialdini

Se debe utilizar una combinación de principios para ser efectivos:



Principios de la ingeniería social a detalle

Reciprocidad

- Cuando una persona nos ofrece algo, tendemos a ofrecerle algo también.
- Por el contrario, si esa persona no nos trata con respeto, estaremos más susceptibles a pagarle con la misma moneda.

La reciprocidad es un «instinto» social fácilmente manipulable.

Urgencia y escasez

- Un clásico entre los clásicos.
- La mayoría de los ataques de ingeniería social consiguen que las personas caigan a través de la urgencia.



Urgencia y escasez

Ejemplos:

- "¡Alguien ha accedido a tu cuenta bancaria, entra en el siguiente enlace para solucionarlo y proteger tu dinero!".
- "¡Esta oferta sólo durará durante los próximos cinco minutos!".
- "Tu ordenador ha sido infectado, haz clic aquí para borrar el virus ahora".

Escasez

- Principio: todo aquello que es escaso tiene más valor.
- Es **irracional**. Solo hace falta ver cómo reacciona la gente durante las rebajas o ante las ofertas limitadas.



Source: <https://bit.ly/386CHig>

Consistencia

Si, en algún momento, hemos dado nuestra palabra, tendemos más a cumplir con ello que a no hacerlo.

Ejemplo: Cuando un trabajador de una empresa pide a la víctima que realice determinadas tareas habituales.

Source: <https://bit.ly/3mhZWd1>

Consistencia

- Empezando por **pequeñas acciones** y continuando por otras más delicadas.
- A pesar de que una de esas tareas pueda parecer **rara**, al haberse **comprometido**, **la llevará a cabo junto al resto**.
- De esta manera, el ingeniero social consigue manipular por **consistencia**.

Simpatía

Nuestra **desconfianza se reduce** cuando el interlocutor con el que hablamos nos cae bien o está alineado con nuestros intereses o valores.

Source: <https://bit.ly/3mjP66e>



Simpatía

Nos señala algo que a primera vista puede parecer simple:

Estamos más predispuestos a dejarnos influir por personas que nos agradan, y menos por personas que nos producen rechazo.

Autoridad

- Cuando una persona en prácticas de una empresa pide las credenciales de acceso de un servicio, lo más probable es que sea vista con desconfianza.
- No obstante, si las mismas credenciales son pedidas por un Director/a, la situación cambia.

Autoridad

- **El uso de la autoridad juega un papel clave en la usurpación de identidad, ya sea de forma real (robo del perfil digital del Director/a) o ficticia (clonado de perfiles o phishing).**

Validación social

Si recibimos un correo electrónico en el que se nos pide hacer una determinada acción, la cual es extraña, lo más seguro es que pensemos si llevarla a cabo o no.

Source: <https://bit.ly/3afXcuB>



Validación social

Sin embargo, si en una misma conversación hay varios conocidos como, por ejemplo, compañeros de la misma empresa, y ninguno de ellos pone objeción alguna, lo más probable es que **NO acatemos las normas**, aun sin saber de dónde ni de quién provienen.

Validación social

Al ser las personas tan gregarias y en búsqueda permanente de la acción social, **el sesgo de grupo** es continuamente utilizado, también conocido como "**presión grupal**", especialmente en el ámbito de la política para conseguir movilizar el voto.

Caso: Robin Sage



"Getting In Bed with Robin Sage."

By Thomas Ryan
Co-Founder & Managing Partner
Provide Security, LLC.



Source: <https://bit.ly/34bynV>

The image shows a Facebook profile page for a user named "Robin Sage". The profile picture is a woman with long dark hair. The bio section contains several negative comments about the user's LinkedIn profile, hometown, and political views. The "Information" sidebar lists basic profile details like relationship status, birthday, and city. The "Recent Activity" section shows various interactions with other users, such as becoming friends or commenting on posts.

Robin Sage

Wall Info Photos

Write something...

Attach: Share

Omachonu Ogali I'm sorry, but you're extremely sketchy.

You create LinkedIn, Blogger, and Twitter profiles with a fake name, all on the same day.

Your LinkedIn profile initially said you were a "Cyber Intelligence Operator", which is a position that does not exist. You recently changed it to "Cyber Threat Analyst".

You claim your hometown is Moyock, NC, which is Blackwater's US training HQ.

No one in the 2003 class of St. Paul's has any idea who you are.

Worst of all, you randomly add tons of people in the security industry, but no one can vouch for you.

3 minutes ago · Comment · Like · See Wall-to-Wall

RECENT ACTIVITY

Robin and Omachonu Ogali are now friends. · Comment · Like

Robin and Zach Valko are now friends. · Comment · Like

6 more similar stories

Robin became a fan of Blackwater. · Comment · Like · Become a Fan

Robin changed her Religious Views. · Comment · Like

Robin and Gunter Ollmann are now friends. · Comment · Like

Robin and Murdoc D. Net are now friends. · Comment · Like

3 more similar stories

Robin likes Mike Roadancer's status.

Robin commented on Mike Roadancer's status.

Robin and Robert RSnake are now friends. · Comment · Like

Robin and Jeremiah Grossman are now friends. · Comment · Like

Perfil de un ingeniero(a) social

Cualidades

- Capacidad de socializar con facilidad.
- Habilidad en el hablar.
- Habilidad en el arte de persuasión.
- Sonar convincente.

Source: <https://bit.ly/3aaVSsU>



Cualidades

- Aparentar ser inofensivo.
- Mantener un perfil bajo.
- Sonreír siempre.
- Tono de voz cómodo.

Source: <https://bit.ly/3aaVSsU>



¿Cómo identificarlo?

¿Cómo identificarlo?

Identificar un ingeniero social puede ser bastante difícil.

Sin embargo, hay personas que, al lado de Hackers y Crackers, tienen un buen potencial para desarrollar un ataque de ingeniería social por su experiencia de trabajo.

¿Quién puede atacar?

- Ex-empleados molestos
- Infiltrados
- Empleados descontentos
- Visitantes



¿Cómo identificarlo?

Los siguientes puntos facilitan la identificación de un ingeniero social:

- Intentan presionar a sus víctimas mediante:
 - ❑ “Name-dropping”.
 - ❑ Uso de autoridad o amenazas.
- Presionan creando un sentido de gratitud en las víctimas (**reciprocidad**), siendo amable y cordial.

¿Cómo identificarlo?

Una víctima debe estar **muy atenta** a todo lo que se pregunta, independiente de lo que se dijo antes o después, sin tener miedo por preguntar por su derecho a saber una información delicada.

¿Cómo identificarlo?

- Favorecen la sensación de comodidad de la víctima.
- Provocan que **la víctima contravenga derechos y políticas de seguridad**, obteniendo la información deseada.
- **Aparentan ser confiables a otros:**
Incluyen información que han conseguido antes, mientras atacan a otra persona.

Tipos de ingeniería social

Basada en humanos

Ingeniería social



Basada en humanos

Consiste en recolectar información sensible mediante la interacción entre humanos.

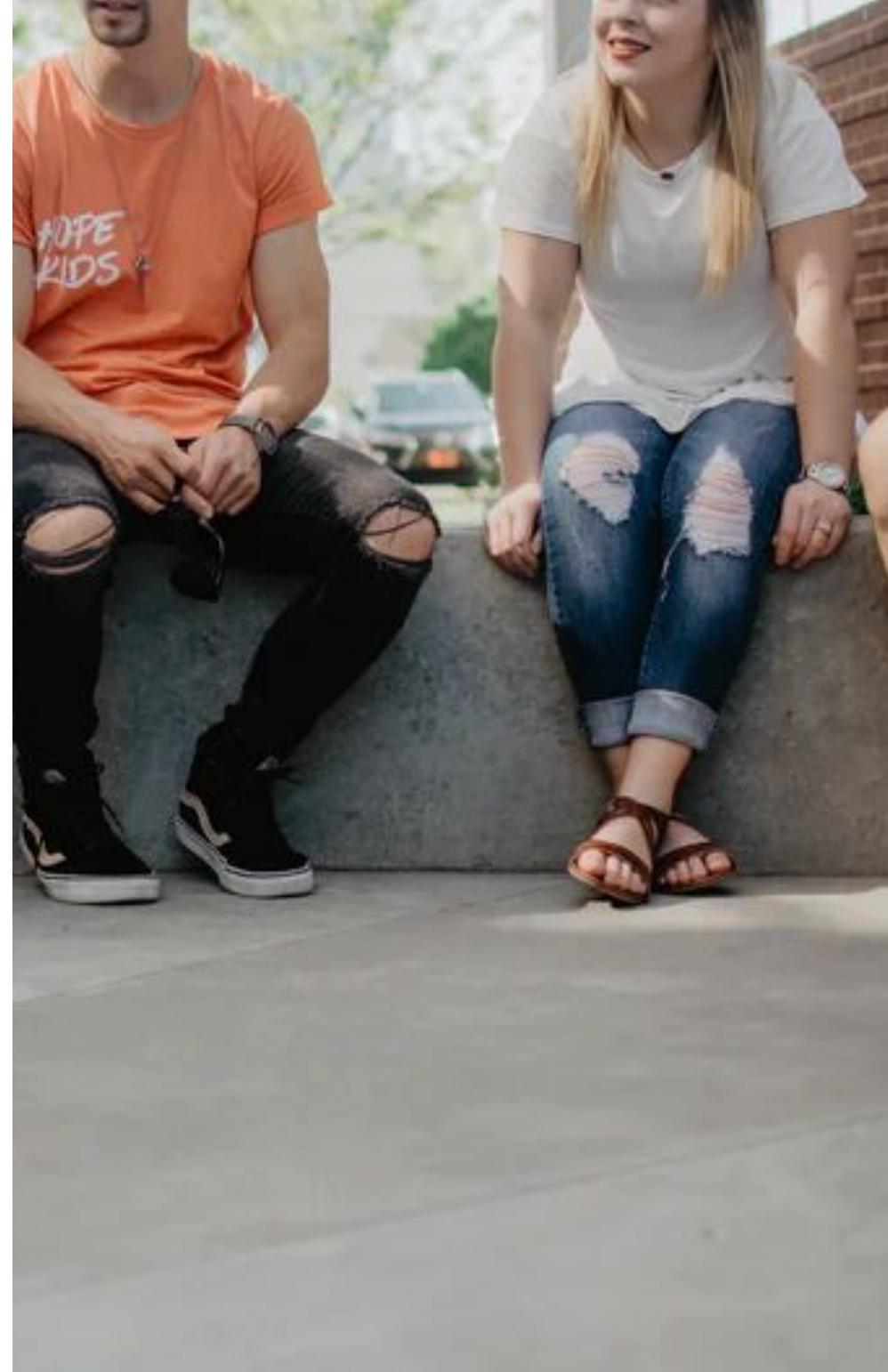


Basada en tecnología

Se lleva a cabo con la ayuda de las computadoras.

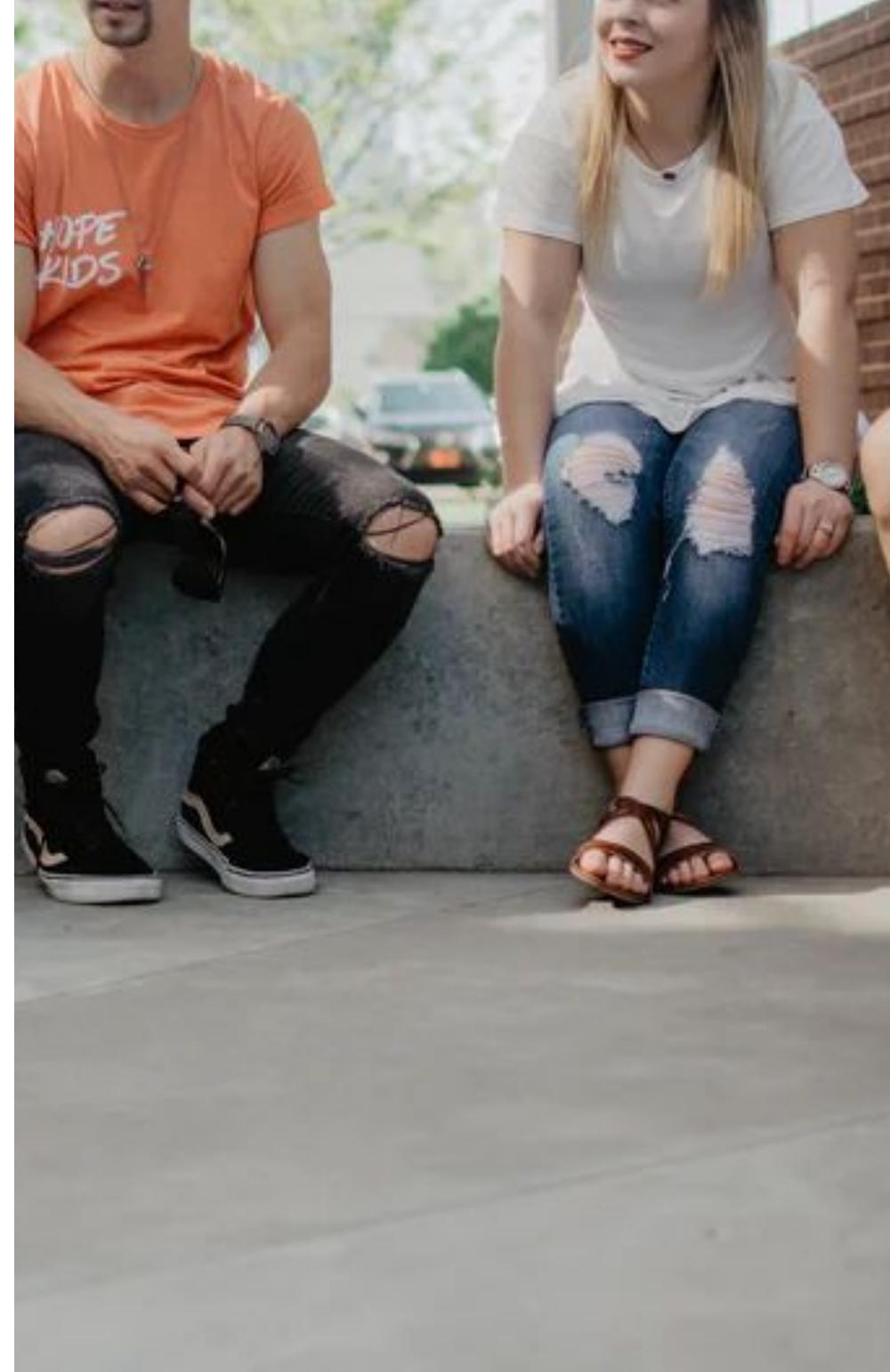
Estrategia basada en humanos

- Imitando ser un usuario legítimo.
- Imitando ser una persona importante (alto rango).
- Imitando ser personal técnico.



Estrategias basadas en humanos

- Espiar por encima de su hombro (shoulder surfing).
- “Dumpster diving”- Buscando en los zafacones.
- En persona.
- Organización Privada.



Dumpster Diving

Buscando en los contenedores de basura.

- Recibos de facturas, luz, agua, teléfono, cable u otros servicios.
- Información financiera.



Dumpster Diving

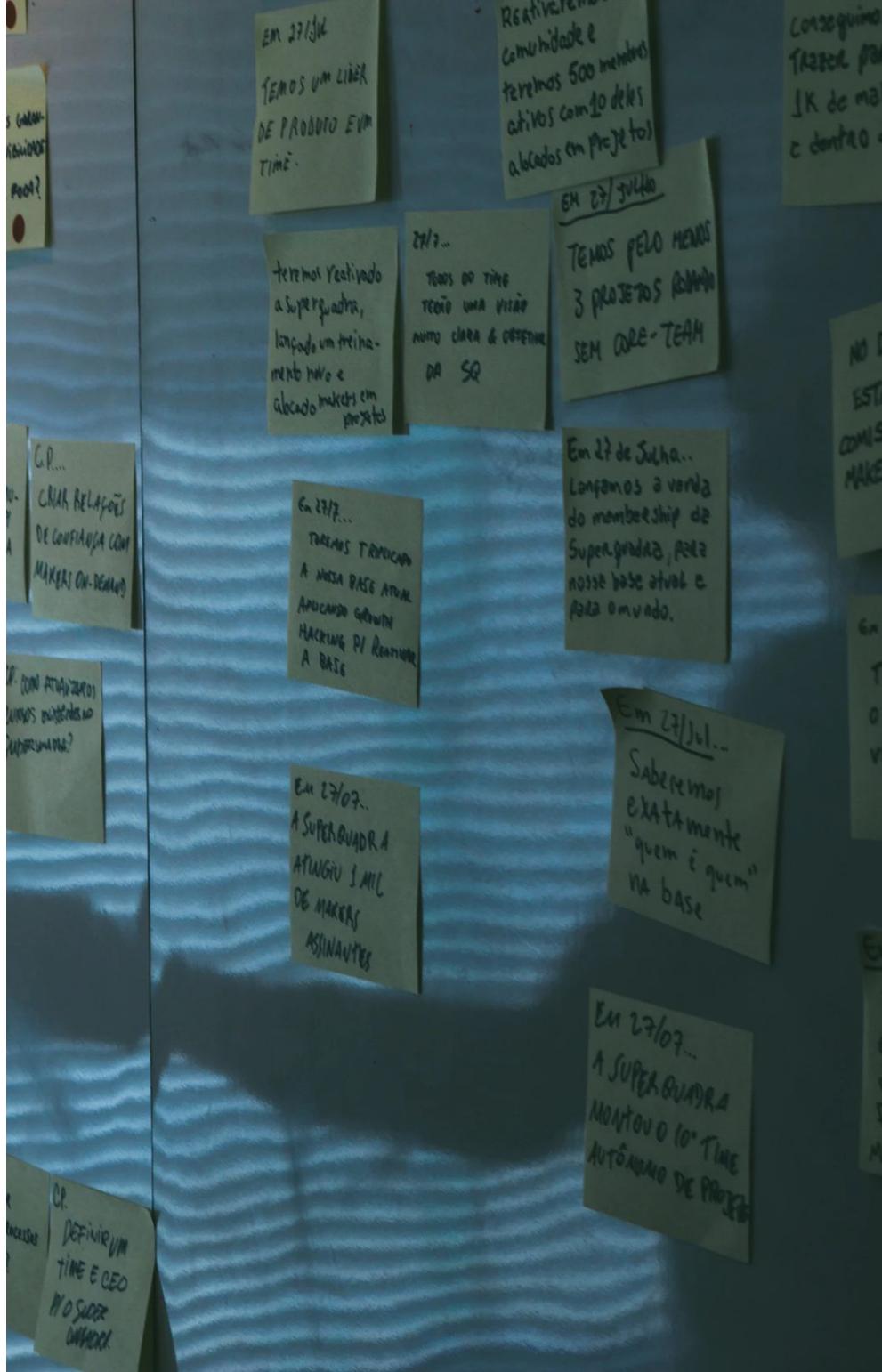
Buscando en los contenedores de basura.

- “Post-it”.
- Números de teléfono.
- Matrículas.
- Otros.



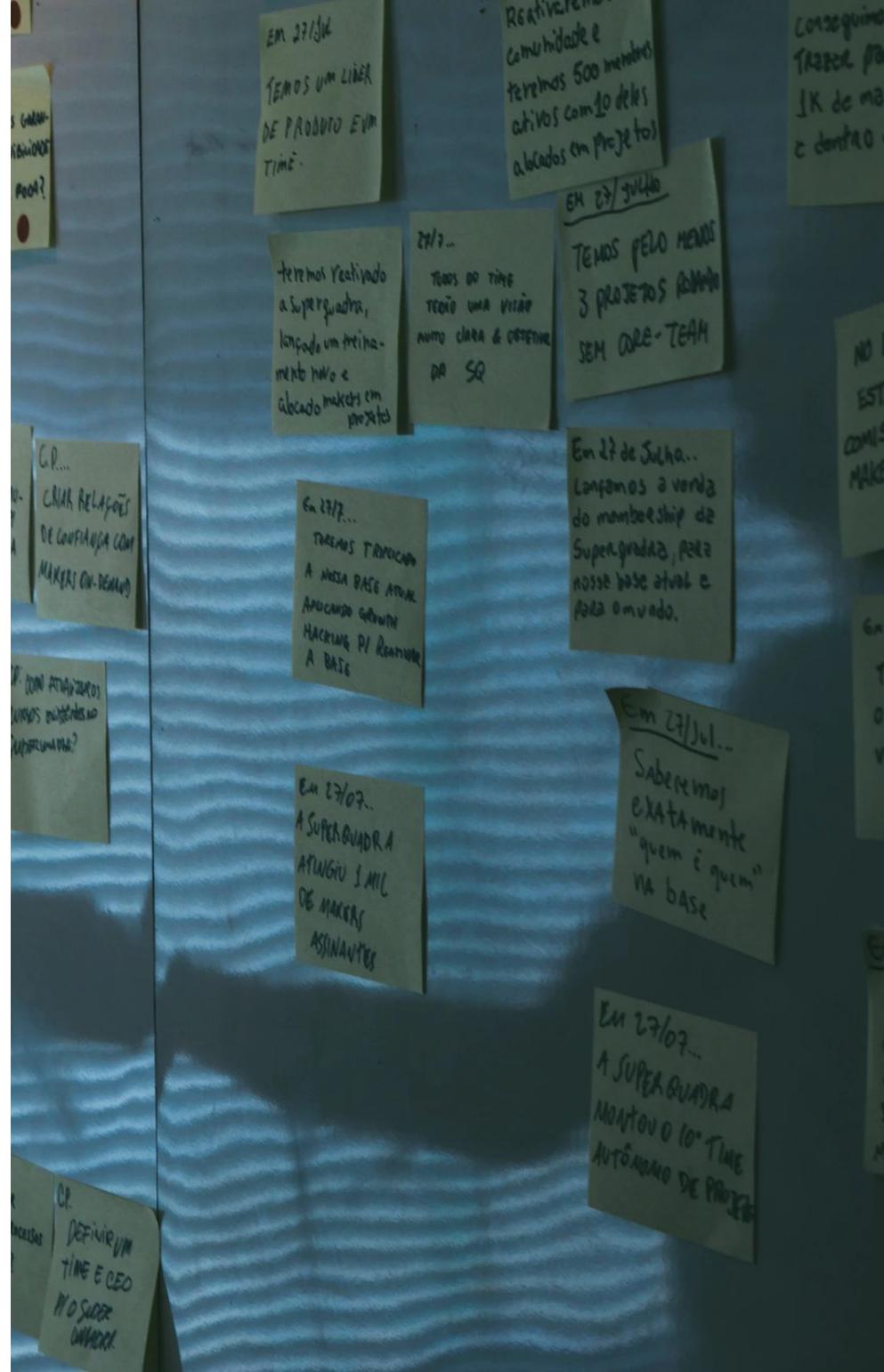
Revisión de desperdicios o basura

- Libretas telefónicas.
 - “Memos” y apuntes.
 - Organigramas.
 - Manuales de procedimientos.
 - Calendarios (de reuniones, eventos y vacaciones).



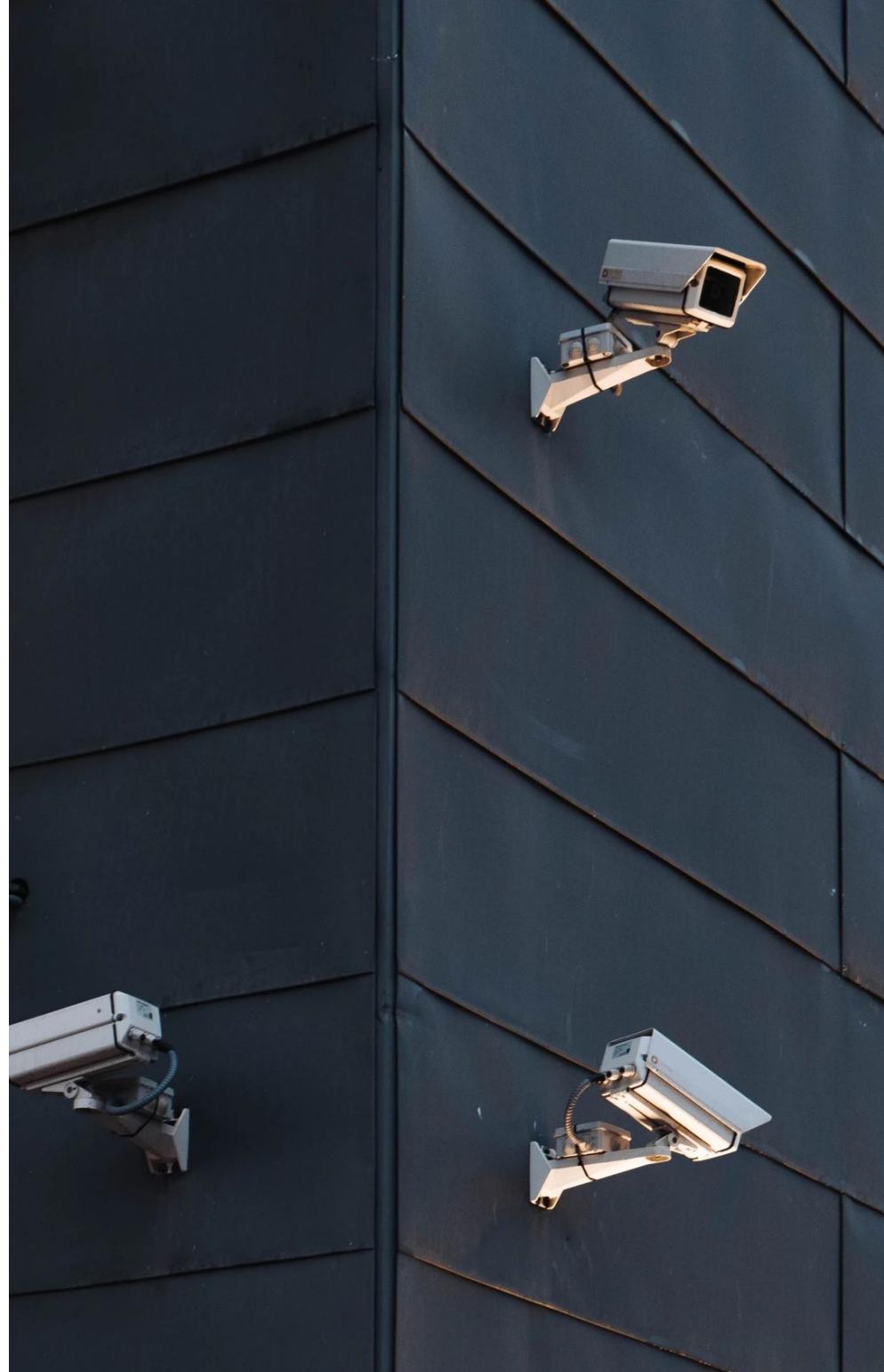
Revisión de desperdicios o basura

- Manuales de operación de sistemas.
- Reportes con información.
- Cuentas de usuarios y sus contraseñas.
- Formatos con membretes.
- Papel con sellos.



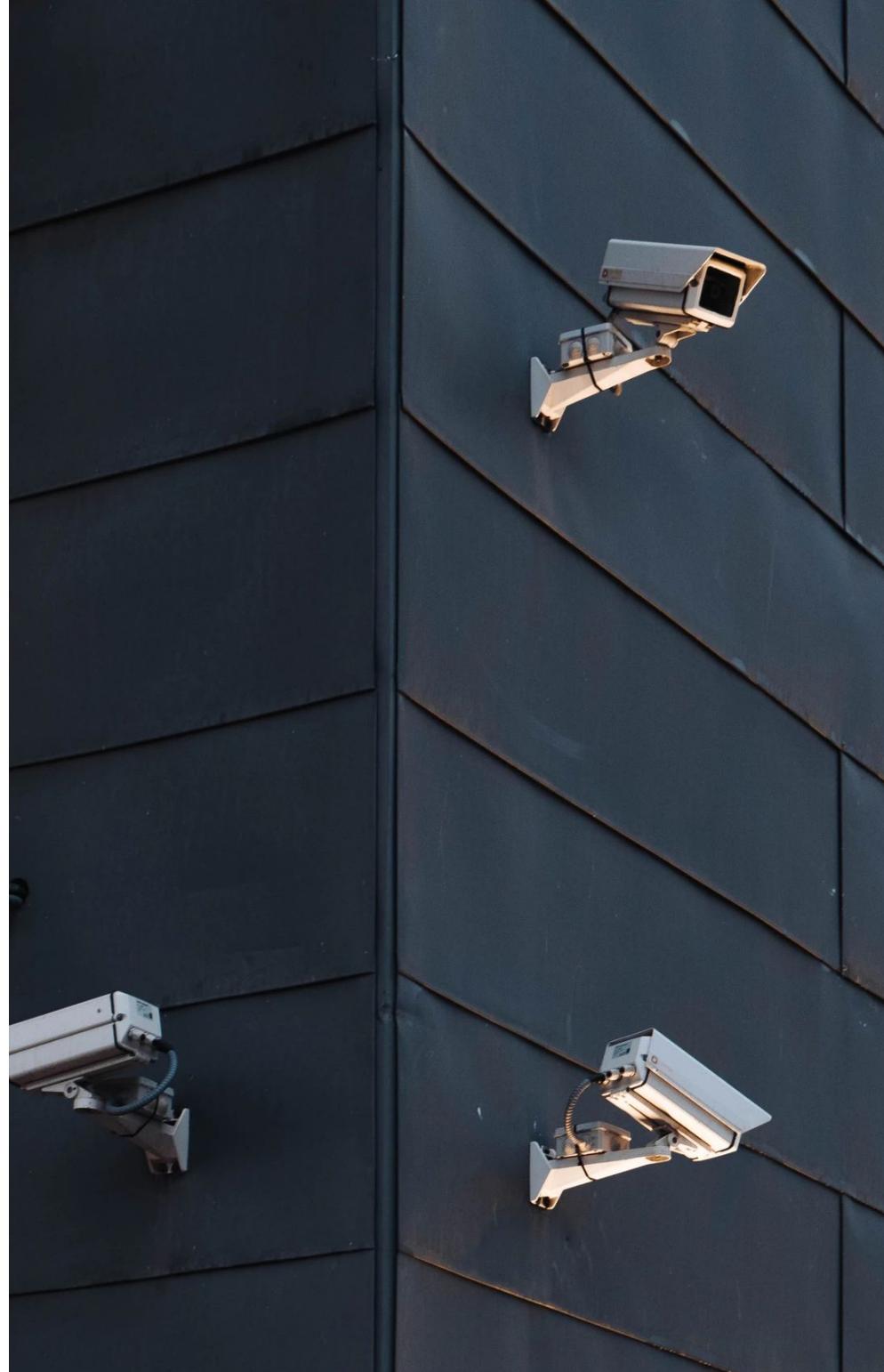
Contramedidas para el Dumpster Diving

- Candado a los contenedores.
- Colocando portones.
- Colocando letreros de “No pase”.
- Luces.
- Utilizando Cámaras de seguridad.



Contramedidas para el Dumpster Diving

- Implementando una política de triturar documentos.
- Utilizando trituradoras en las oficinas.
- Utilizando servicios de recolección.



Discusión

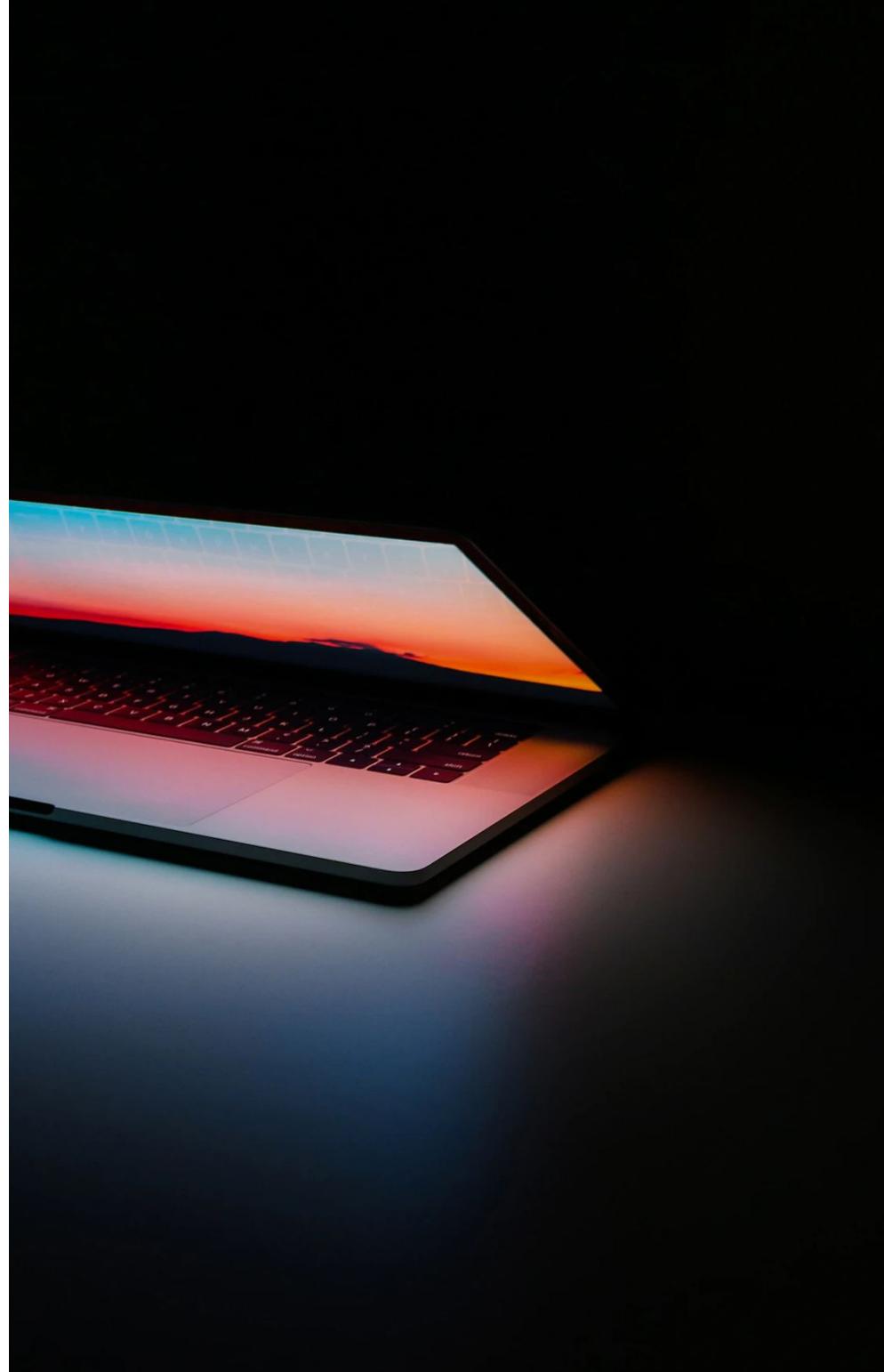
- ¿La empresa para que trabajas tiene una política oficial para disponer de los documentos?
- ¿Cuál es esa política? ¿Cómo se podría mejorar la misma? ¿Quién es el responsable de implementarla?
- ¿Haces algo de esto en tu hogar?

Tipos de ingeniería social

Basada en computadoras

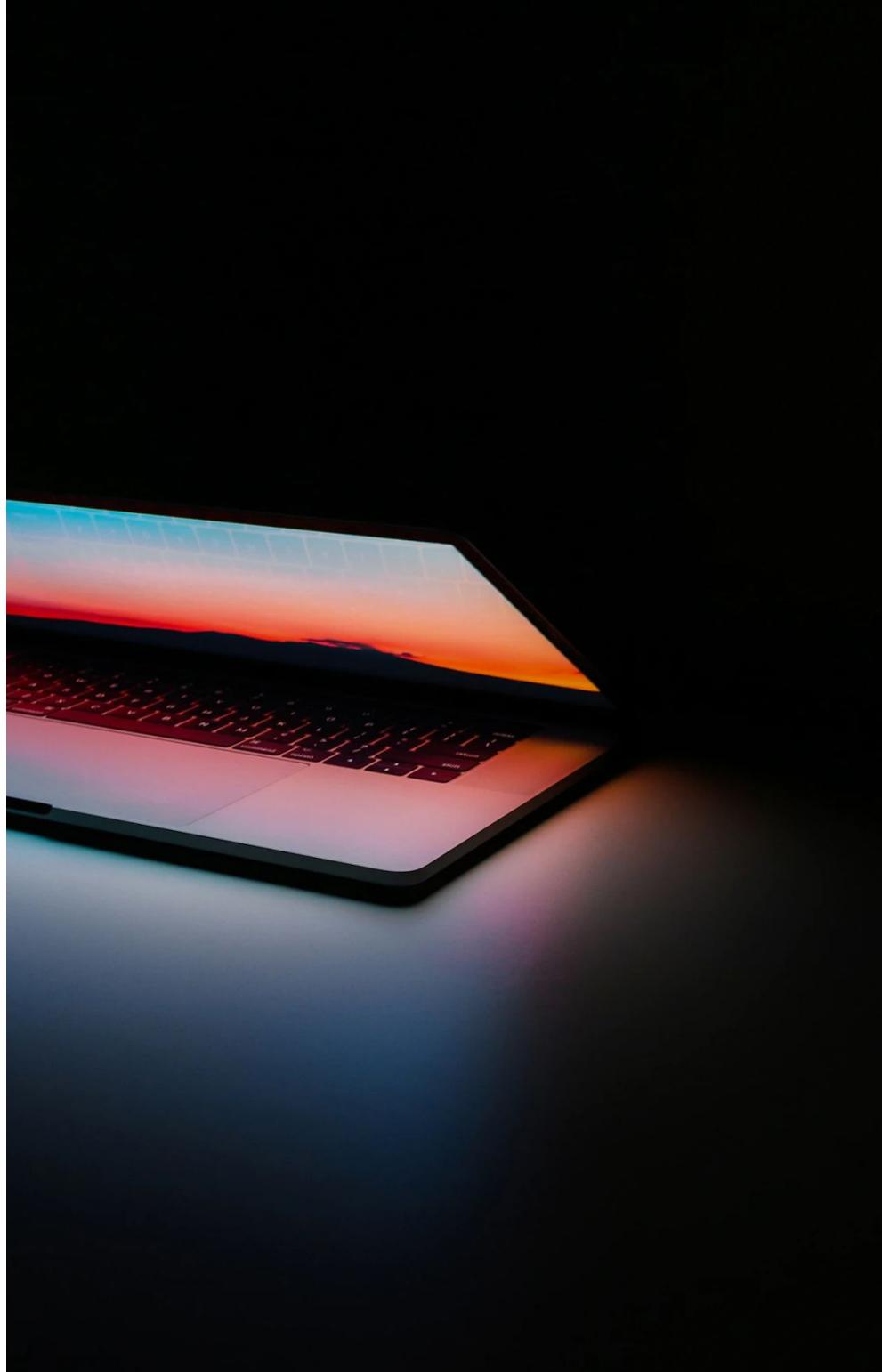
Estrategias basadas en tecnología

- Email con malware.
- Spam (correo no deseado).
- Cadena de cartas (chain letters).



Estrategias basadas en tecnología

- Emails de engaño (hoaxes).
- “Phishing”.
- Instalando un keylogger.



Tipos de ataques de la ingeniería social

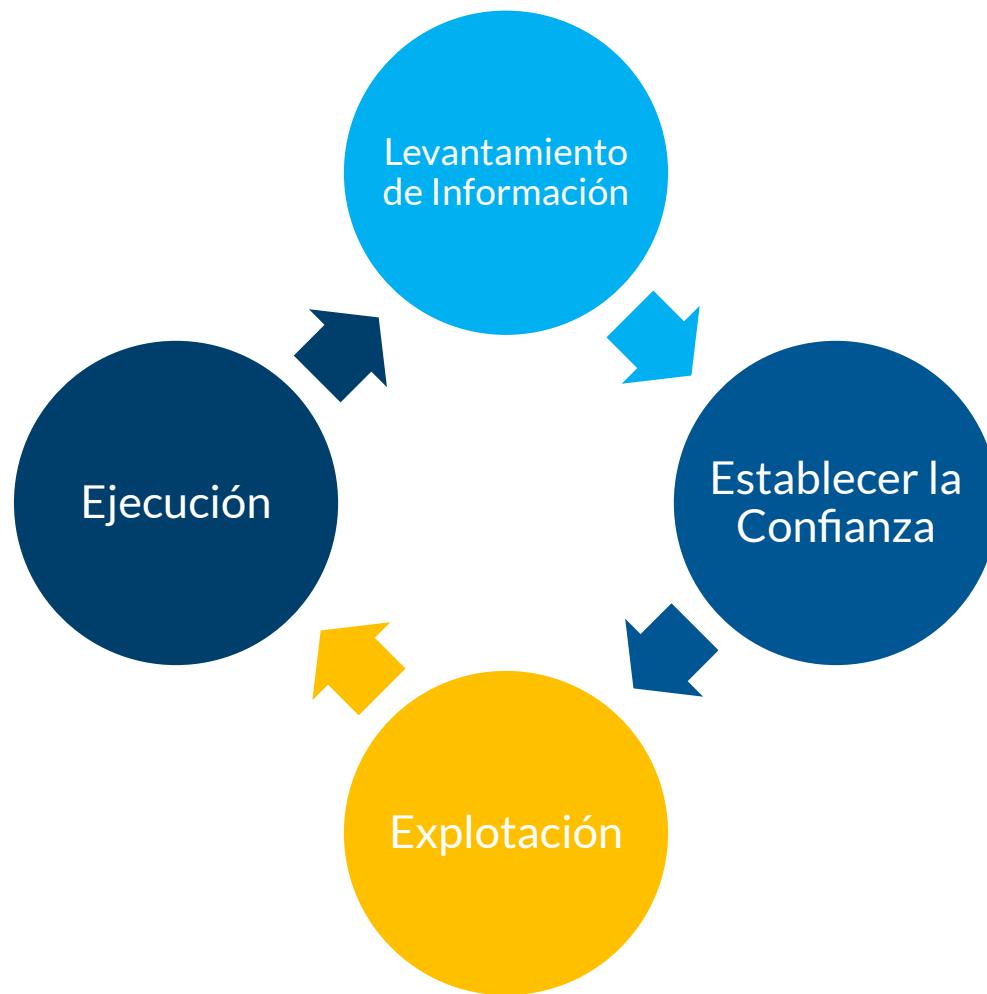
Taxonomía de los ataques

Marco de ataque de Ingeniería Social

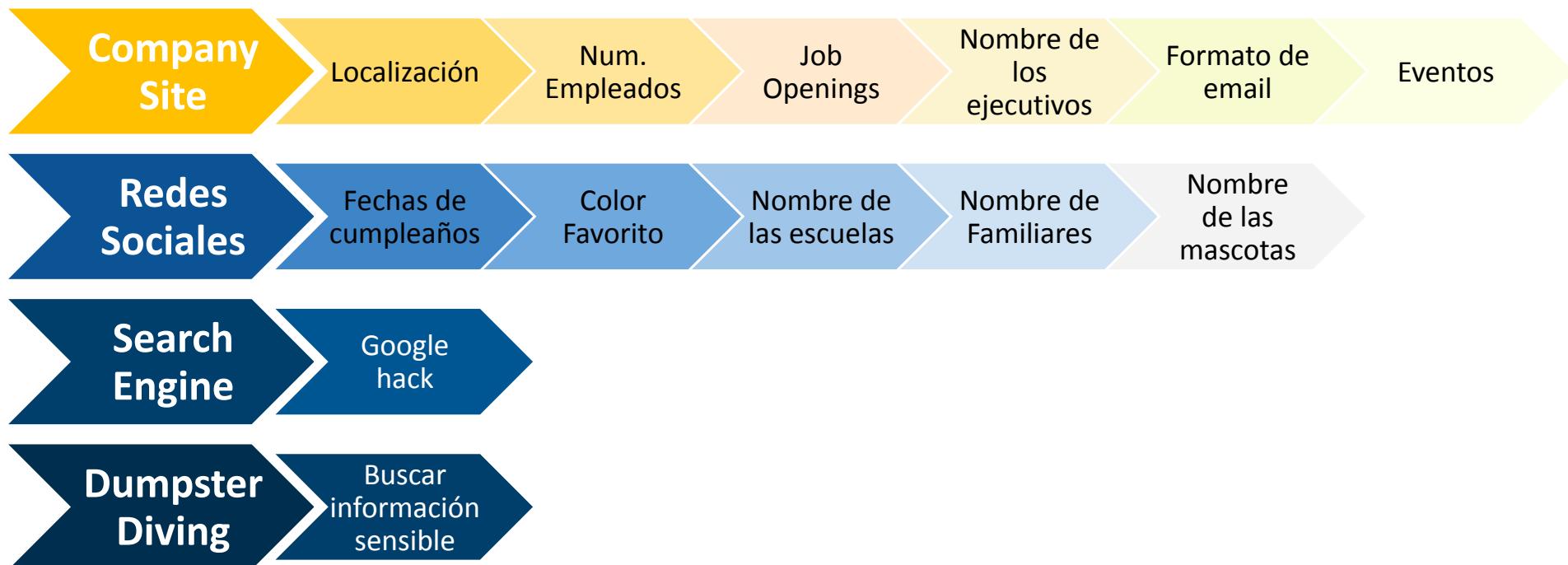


Source: <https://bit.ly/3o8fLF6>

Etapas de los ataques de ingeniería social



Levantamiento de información



Fase 1: selección de la víctima

Se busca por debilidades en el personal de la organización:

- Help Desk
- Soporte técnico
- Recepción
- Soporte administrativo
- Etc.

Fase 2: recopilación de inteligencia

- Fuentes de información primaria:
 - Basurero
 - Páginas web
 - Ex-empleados
 - Contratistas
 - Vendedores
 - Socios estratégicos

La base para la siguiente fase.

Fase 3: el ataque

- Basado en rutas de persuasión:
 - Autoridad
 - Similitud
 - Reciprocidad
 - Compromiso y consistencia

Usa la emoción como una forma de distracción.

Fase 4: obtener la información

- El atacante obtiene la información necesaria de los sistemas de la empresa.
- Diseña el plan de ataque informático.
- Ejecuta el plan.
- Borra las huellas.
- Prepara el informe.

Categorías generales de los ataques de ingeniería social

Categorías generales de ataques

- Ataques técnicos
- Ataques al ego
- Ataques de simpatía
- Ataques de intimidación



Categorías generales de ataques

- No hay contacto directo personal con las víctimas.
- El atacante envía mensajes al correo electrónico, diseña websites falsos, popups o algún otro medio.
- Pretende ser soporte autorizado o un administrador de sistemas.

Categorías generales de ataques

- Trata de obtener información sensible de los usuarios (claves, nombres de usuario, números de tarjeta de crédito, claves de cajero, etc).
- Muy exitoso.



Social Engineering. (2020). [Illustration].
Pinterest.
<https://br.pinterest.com/pin/691372980270225351/>

Ataque al ego (Reciprocidad/Simpatía)

- El atacante apela a la vanidad o ego de la víctima.
- Usualmente atacan a alguien que parezca frustrado con su situación laboral.
- La víctima trata de probar cuán inteligente o conocedor es y provee información o incluso acceso a sistemas o datos.

Ataque al ego (Reciprocidad/Simpatía)

- El atacante puede pretender ser una autoridad de la ley, la víctima se siente honrado de ayudar.
- La víctima usualmente nunca se da cuenta.

Ataque de simpatía (Simpatía/Compromiso)

- El atacante pretende ser un nuevo empleado, contratista o vendedor.
- Existe alguna urgencia de completar una tarea u obtener alguna información.
- Necesita asistencia o perderá su trabajo o estará en problemas.

Ataque de simpatía (Simpatía/Compromiso)

- Juega con la empatía/simpatía de la víctima.
- El atacante pide ayuda hasta que encuentra alguien que pueda ayudarlo.
- Ataque muy exitoso.

Ataque de intimidación (autoridad)

- El atacante pretende ser alguien con influencias (una figura de autoridad, oficial de la ley).
- Trata de utilizar su autoridad para forzar a la víctima a cooperar.

Ataque de intimidación (autoridad)

- Si hay resistencia utiliza la intimidación y amenazas (pérdida del empleo, cargos criminales).
- Si pretende ser un oficial de la ley dirá que la investigación es encubierta y no debe ser divulgada.

Ejemplos de ataques de ingeniería social

Common Social Engineering Techniques

PHISHING



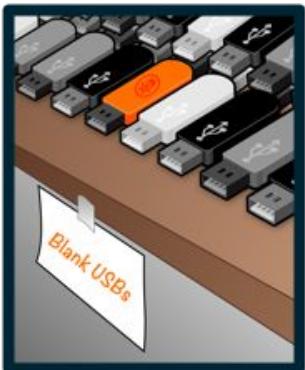
SPEAR PHISHING



QUID PRO QUO



BAITING



PRETEXTING



VISHING



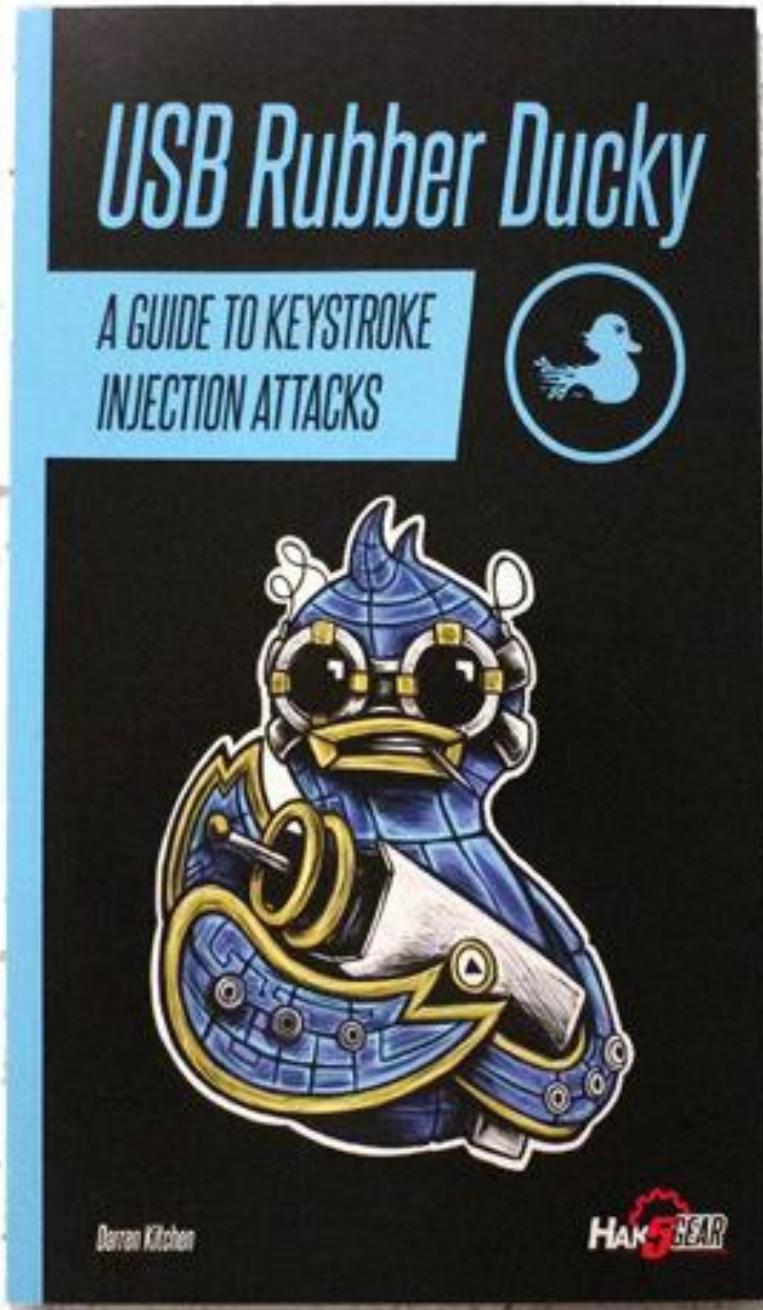
TAILGATING



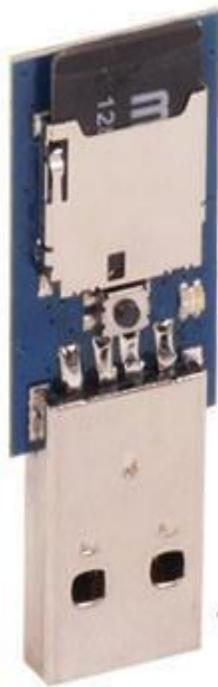
Spanning. (2019, November 20).
social-engineering-techniques
[Illustration].
Social-Engineering-Techniques.
<https://spanning.com/blog/social-engineering-insider-threat-to-cybersecurity/social-engineering-techniques/>

Carnada/Baiting

- El cibercriminal puede dejar un dispositivo, como una memoria USB, infectado con software malicioso a la vista en un espacio público.
- Alguien recogerá ese dispositivo y lo conectará a su equipo para ver qué contiene.
- En ese momento, el software malicioso se introducirá en el equipo.



USB Rubber Ducky + Book. (2020). [Photograph]. Hackmod.
<https://www.hackmod.de/USB-Rubber-Ducky-Book-1/en>



Micro SD Storage

Replay Button

LED Indicator

Type A Plug



60 MHz 32-Bit CPU

Covert Case

Optional Decal

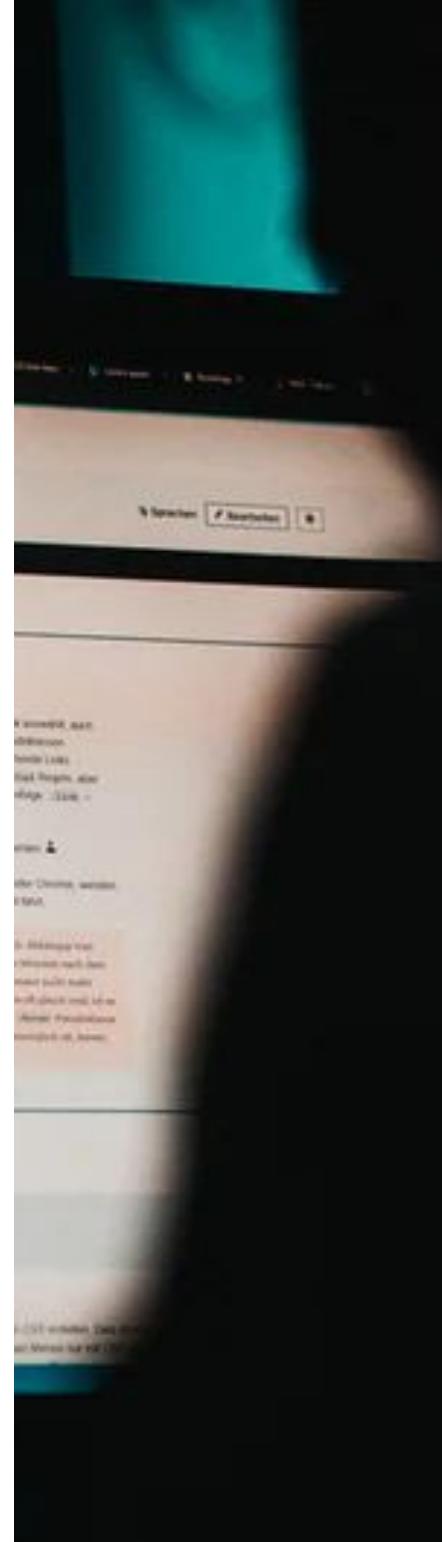


Phishing

El *phishing* es un método que los ciberdelincuentes utilizan para engañar y conseguir que se revele información personal, como contraseñas, datos de tarjetas de crédito o de la seguridad social y números de cuentas bancarias, entre otros.

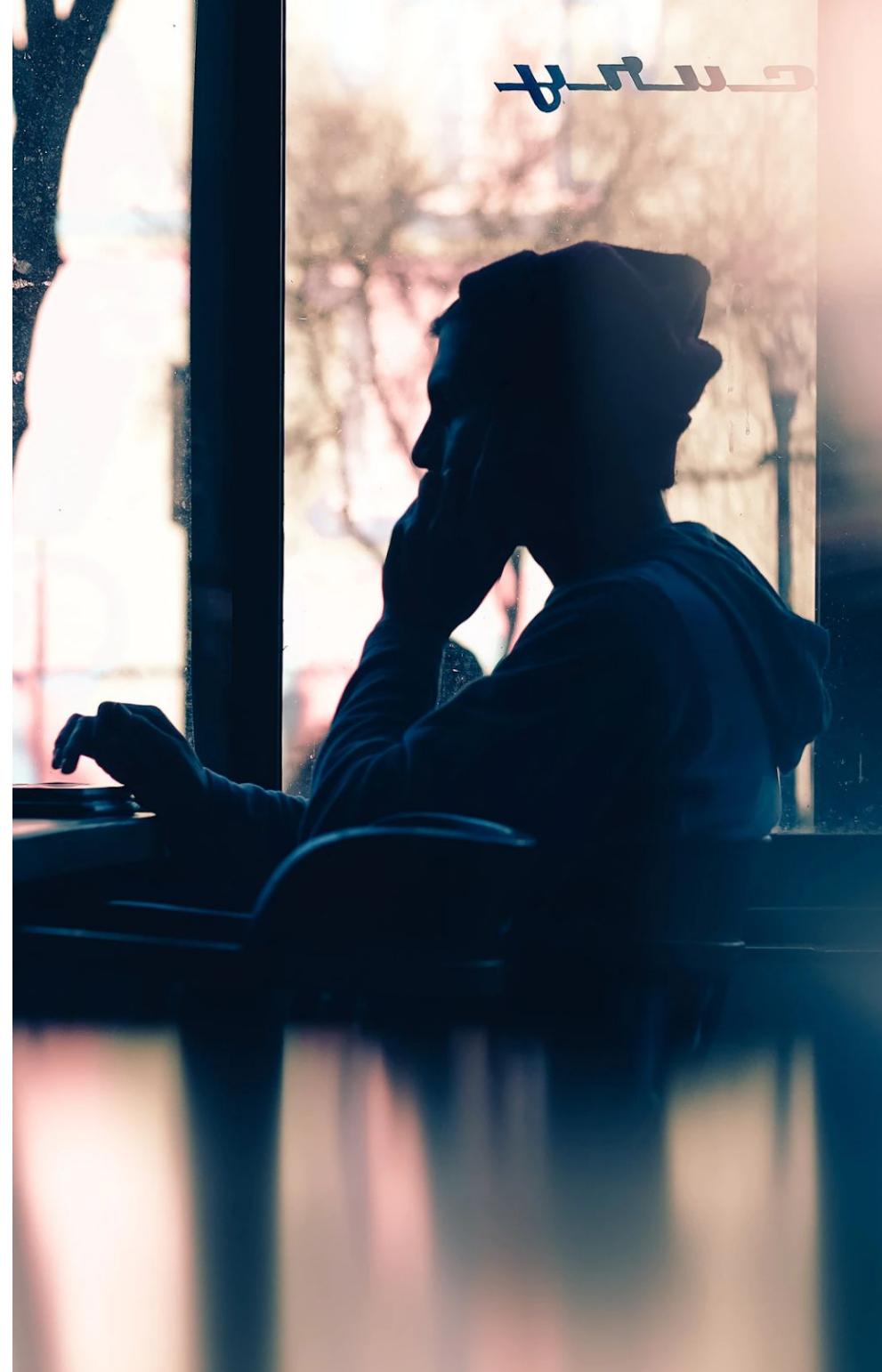
Phishing

Obtienen esta información mediante el envío de correos electrónicos fraudulentos o dirigiendo a la persona a un sitio web falso.



Pretexo Pretexting

El atacante simula situaciones ficticias para obtener información personal, sensible o privilegiada y utilizarla con fines delictivos.



Pretexo Prestexting

El Pretexting a menudo implica investigar el objetivo antes del ataque.

El objetivo principal del actor de la amenaza es ganar la confianza del objetivo y explotarlo a través de una llamada telefónica o en persona.

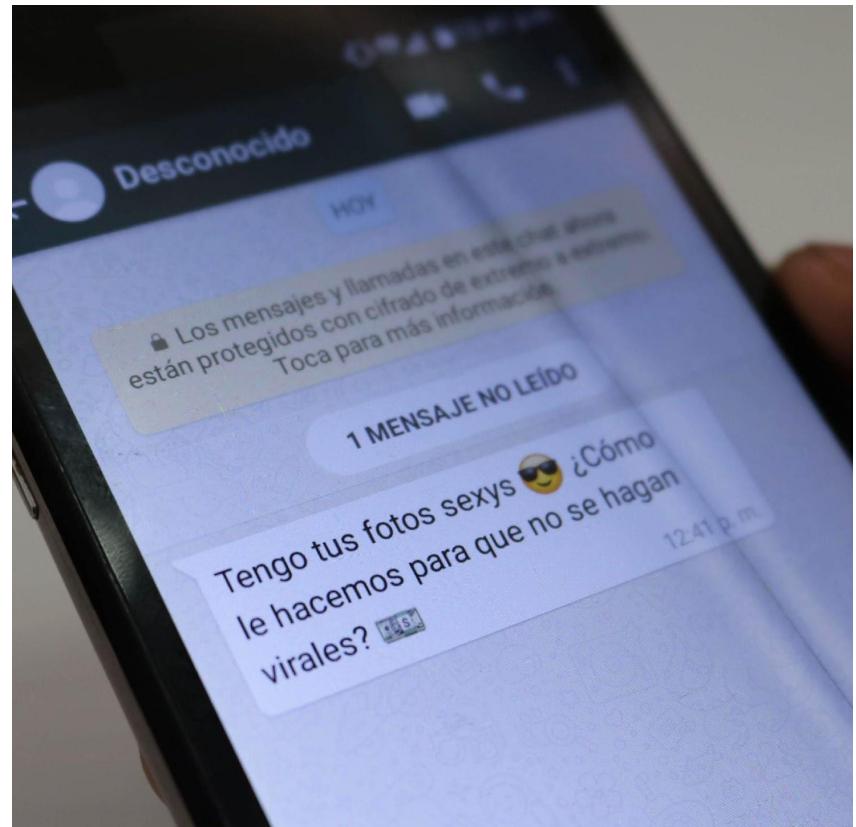
Pretexo Pretexting

El objetivo principal del actor de la amenaza es ganar la confianza del objetivo y explotarlo a través de una llamada telefónica o en persona.



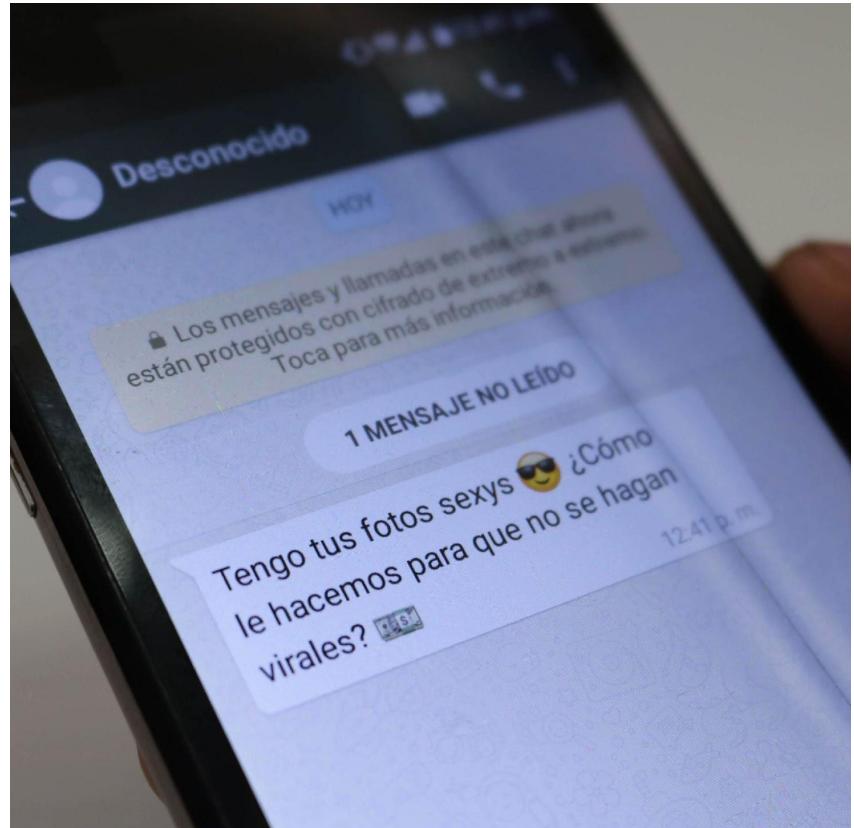
Sextorsión

Este ataque de Ingeniería Social consiste en chantajear a la víctima para que envíe dinero al ingeniero social a cambio de no distribuir por Internet imágenes o videos comprometedores.



Sextorsión

En ocasiones dispone de dicha información comprometida, pero en muchas ocasiones es mentira o es un montaje.



Shoulder surfing

Consiste en espiar físicamente a las víctimas para conseguir información confidencial como las credenciales de acceso a un sistema, equipo, plataforma, etc.

Dumpster Diving

- Este ataque de ingeniería social consiste en **explorar la "basura"** con el objetivo de buscar información valiosa.
- Muchas veces, las personas suelen tirar a la papelera documentos importantes sobre sí mismos o sobre la empresa en la que trabajan.

Quid Pro Quo

“Una cosa por otra”

- En este tipo de estafa se tienta a los usuarios con ganar algo, como premios o descuentos en productos costosos, pero solo una vez que hayan completado un formulario en el cual se solicita una gran cantidad de información personal.
- Todos los datos recopilados se usan para el robo de identidad.

Vishing

- La palabra 'Vishing' es una combinación de 'voz' y 'phishing'.
- La suplantación de identidad consiste en utilizar el engaño para que una determinada persona revele información personal o confidencial propia o de su organización.

Vishing

El vishing es una estafa que pretende suplantar la identidad del afectado a través de VoIP (Voice over IP), recreando una voz automatizada.



Vishing

El modus operandi de **Vishing** más común es el envío de correos electrónicos que solicitan que se llame a un número de teléfono, en el que aparece un contestador automático pidiendo al usuario información confidencial.

Vishing

Otro procedimiento de Vishing es cuando el cibercriminal obtiene la información confidencial mediante un correo electrónico o una web fraudulenta, lo que se denomina ataque phishing pero necesita alguna información que le falta (normalmente un código de SMS) que se exige cuando se tiene activado el **Doble Factor de Autenticación**.

Vishing

En este caso el cibercriminal necesita el código SMS o la clave del token digital para poder validar las operaciones, transferencias o compras online fraudulentas.

Vishing

De manera que los cibercriminales llaman por teléfono al cliente identificándose como personal del banco y tras "darle confianza" y alamarle de algún modo, mediante argumentos de urgencia o de riesgo, le pedirán la clave que necesitan.

Fake News

Pueden buscar este tipo de ganchos para hacerse viral y que lleguen a muchos usuarios.

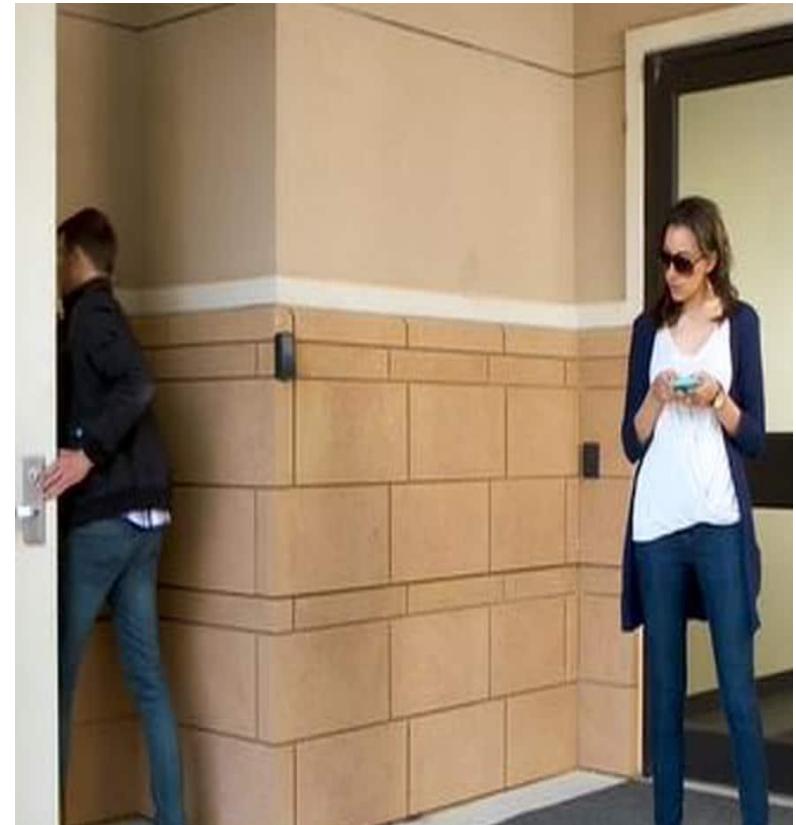


Fake News

Posteriormente esos enlaces, esos artículos falsos, pueden tener contenido malicioso, invitar a descargar software que ha sido modificado por terceros o recopilar datos de alguna manera.

Tailgating

El tailgating se define como la práctica de obtener acceso no autorizado a un área restringida (como oficinas o centros de datos) mediante el engaño o descuido de una persona que si cuenta con la autorización correspondiente.



Tailgating

- Ejemplo una empresa a la que se accede a través de una tarjeta RFID.
 - El atacante espera a que la víctima esté entrando para acercarse rápidamente y decir que se ha olvidado su tarjeta dentro.

La persona que abre la puerta no sabe que lo están siguiendo

Piggybacking

- Es cuando una persona abre la puerta utilizando sus credenciales y te deja pasar sin que TÚ utilices tus credenciales.
- La persona que abre la puerta sabe que los están siguiendo.

Elicitación

¿Qué es elicitación?

“
Elicitación (del latín *elicitus*, "inducido" y *elicere*, "atrapar") es un término asociado a la psicología que se refiere al traspaso de información de forma fluída de un ser humano a otro por medio del lenguaje.

”

Elicitación. Wikipedia, La Enciclopedia Libre.
<https://es.wikipedia.org/wiki/Elicitaci%C3%B3n>

“
En psicología del aprendizaje se trata de un término técnico que designa la acción de provocar una conducta de manera refleja por un evento antecedente, ya sea un reflejo innato (como ocurre con las respuestas incondicionadas) o una conducta aprendida (como en el caso de las respuestas condicionadas).

”

Source: Pellon, Ricardo (Coord.), *Psicología del aprendizaje*. Ed. UNED, Madrid, 2014. Pág 353. ISBN 978 84 362 6727 3

¿Qué es la elicitación?

En las ciencias de la cómputos también se usa, para referirse al traspaso de información de un punto a otro, en forma fluída.

¿Qué es la elicitación?

La información puede fluir desde un software a otro, de un computador a una persona o de persona a persona.

¿Qué es la elicitation?

«Elicitation», es la forma de obtención de información a través de preguntas indirectas como parte de una conversación.



¿Qué es la Elicitación?

Dicha obtención permite recabar información sobre su vida, sus hábitos y problemas, y así, de un modo u otro tener un análisis amplio sobre el objetivo para el posterior «gaining access» del lugar físico o lógico.

El arte de la elicitación

Proviene cuando una persona experta en el campo de la IngeSoc, es capaz de crear cierta «influencia» en la persona, influencia positiva y conseguir una sonrisa, o un pensamiento bueno sobre ella.

¿Por qué es exitosa
la elicitation?

El arte de la elicitación

Para poder desarrollar esta técnica, debe ser natural entender los cimientos básicos de la comunicación verbal y no verbal entre personas, y saber reaccionar rápido y con creatividad ante imprevistos en la comunicación.

El arte de la elicitación

«Ser un gran comunicador», esta es la reseña principal de la «elicitation».



El arte de la elicitation

La magia de la «elicitation» reside en que la víctima no se de cuenta de que está siendo de una forma u otra interrogada, por tanto la comunicación debe ser muy divertida y afable.

Principios para ser exitoso en elicitación

- Ser natural.
- Conocer nuestras posibilidades.
- Ser influyente.
- Lenguaje facial y corporal.
- Uso de preguntas indirectas abiertas.
- Preguntas directas.

Source: <https://bit.ly/2Le61dV>

Principios para ser exitoso en elicitación

- Preguntas asumiendo un hecho que ha «sucedido».
- Si las respuestas dadas en la conversación no da el resultado positivo, no insistir y levantar sospechas con el objetivo.
- Pocas preguntas en la conversación inspira incomodidad.

Source: <https://bit.ly/2Le61dV>

Principios para ser exitoso en elicitación

- Establecer una **metodología secundaria** previamente planeada a tu favor que formará parte de la conversación. Así se evitará sospechas en caso de fallos.
- Necesidad de ayudar y escuchar con atención.
- Sentido del humor.

Principios para ser exitoso en elicitación

- Conversación piramidal.
- Estar de mutuo acuerdo en la conversación.
- Ofrecer información al objetivo. Así de este mismo modo, te la ofrecerá a ti.
- Uso del alcohol para la obtención de la información.*

¿Cómo son los elicidores?

- **Normalmente son personas deseosas de ayudar, incluso a los extraños.**
- Se caracterizan por el deseo de parecer **personas bien informadas** que pueden hablar de cualquier tema y son muy profesionales.

Técnicas de elicitación

Técnicas de elicitation

- Diseñar preguntas con un patrón de uso único para cada objetivo particular.
- Las preguntas diseñadas se pueden clasificar según la respuesta obtenida en:
 - Recolectoras de información .
 - Intrusivas.

Estrategias y respuestas a la elicitación

Cómo evitar las técnicas de elicitación

- Nunca hay que dar información a personas que no están autorizadas a conocerla, incluyendo familia y amigos cercanos.
- Contestar con información que sea pública, como información que aparezca en la prensa.
- Ignorar las preguntas y cambiar de tema.

Cómo evitar las técnicas de elicitación

- **Responder con una pregunta.**
- Responder preguntando ¿por qué me haces esa pregunta?
- Dar una respuesta mediocre.
- Decir que no conoces la respuesta, tú no sabes nada de ese tema.
- Manifestar que **no puedes discutir sobre el tema.**

Pretexting

¿Qué es?

¿Qué es el Pretexting?

- El pretexting es una forma de ingeniería social.
- Es la práctica de presentarse a uno mismo como otra persona con el fin de obtener información privada y privilegiada.

¿Qué es el Pretexting?

- Imitando ser otra persona (impersonation).
- En el pretexto le asigna al atacante el papel de alguien con autoridad que tiene derecho a acceder a la información que se busca, o que puede usar la información para ayudar a la víctima.

“

La parte clave... [es] la creación de un escenario, que es el pretexto utilizado para involucrar a la víctima.

El pretexto establece la escena del ataque, junto con los personajes y la trama. Es la base sobre la cual se realizan muchas otras técnicas para lograr los objetivos generales.

”

Garvin Watson

“

Existen dos elementos principales para un pretexting: un personaje interpretado por el estafador, y una situación plausible en la que ese personaje podría necesitar, o tener derecho a acceder, a la información que busca.

”

Garvin Watson

Ejemplos

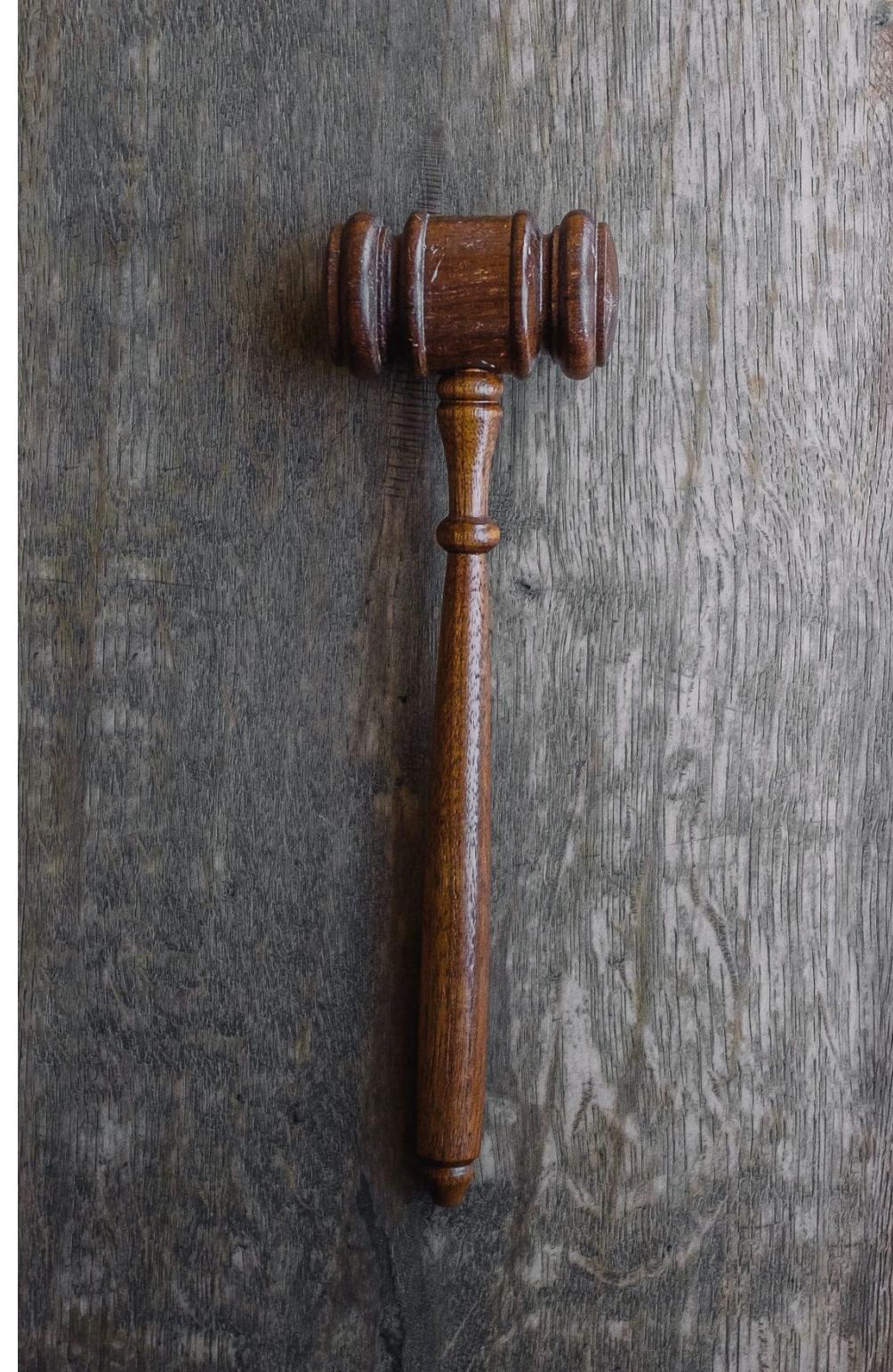


¿Illegal el
pretexting?

¿Es ilegal?

El *pretexting* es, en general, ilegal en los Estados Unidos.

Source: <https://bit.ly/3pXd49Z>



¿Es ilegal?

Para las instituciones financieras cubiertas por la Ley Gramm-Leach-Bliley (GLBA) de 1999 -casi para todas las instituciones financieras-, es ilegal que cualquier persona obtenga, intente obtener, revele o haga revelar al cliente información de una institución financiera por medio de *pretexting* o engaños.

Source: <https://bit.ly/3pXd49Z>

¿Es ilegal?

Las instituciones reguladas por la GLBA también están obligadas a establecer normas para educar a su propio personal, destinadas a identificar los intentos de *pretexting*.

Proceso de planificación de pretexting

Proceso de planificación

- Propósito
- Preparación/Desarrollo
- Práctica
- Ejecución



Propósito

Crear un escenario inventado para persuadir al objetivo a modo que pueda proporcionar cierta información o de realizar alguna acción.

Propósito

Típicamente se realizará una investigación previa para conocer el tipo de lenguaje y la tecnología empleada por la gente que administra los sistemas o que tiene acceso a la información requerida, entre otros.

Preparación Desarrollo

- Escribir un guión-plantilla
- Determinar el método
 - Por teléfono.
 - Si es en persona:
 - Visitar el lugar varios días antes a diferentes horas.
 - Tomar fotos.
 - Determinar el vestuario
 - Higiene. Depende del pretexto.



Nombre del Pretexto:

Nombre del Cliente:

Nombre del Proyecto:

Nombre del Personaje:

Datos demográficos del Personaje:

Antecedentes del Personaje:

Nombre del Objetivo:

Datos demográficos de Objetivo:

Resultados del OSINT:

Script:

Introducción

Contexto

CLOSING

Palabras Claves

Preparación Desarrollo



Nombre del Pretexto:
Nombre del Cliente:
Nombre del Proyecto:

Nombre del Personaje:
Datos demográficos del Personaje:
Antecedentes del Personaje:

Nombre del Objetivo:
Datos demográficos de Objetivo:
Resultados del OSINT:

Script:

Introducción

Contexto

CLOSING

Palabras Claves

Práctica

- La clave del éxito del pretexting está en la práctica continua.
- Frente a un espejo.
- Con tu grupo de trabajo.
- En role play.
- Grabarse en video.

Ejecución



DON'T BE
AFRAID
TO BE
GREAT

Buenos pretextos

- Ser un contratista.
- Entidades sin fines de lucro.
- Encuestador.
- La entrevista.
- Sorpresas.
- Entrega de una orden.
- El nuevo empleado.

Buenos pretextos

- Departamento de sistemas de IT.
- El auditor.
- La mamá/papá preocupados.
- El anciano/a.
- Otro...

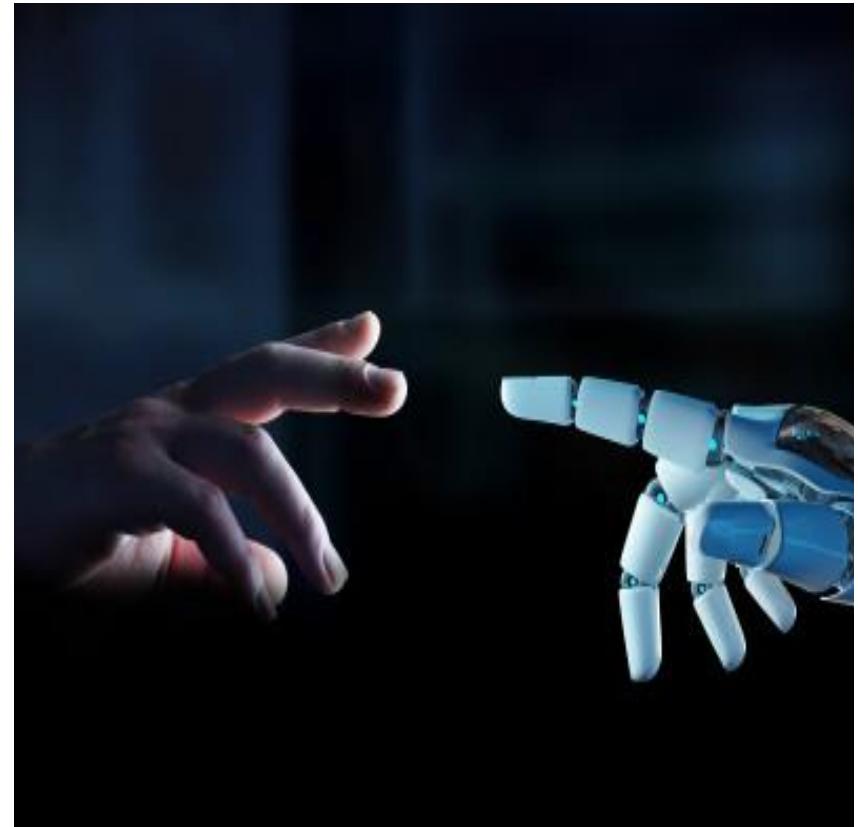
Deepfake

¿Qué es?

Origen

Nace de la unión de dos conceptos:

- El *deep learning*, como se conoce al aprendizaje profundo de sistemas de inteligencia artificial.
- La palabra *fake*, falso.

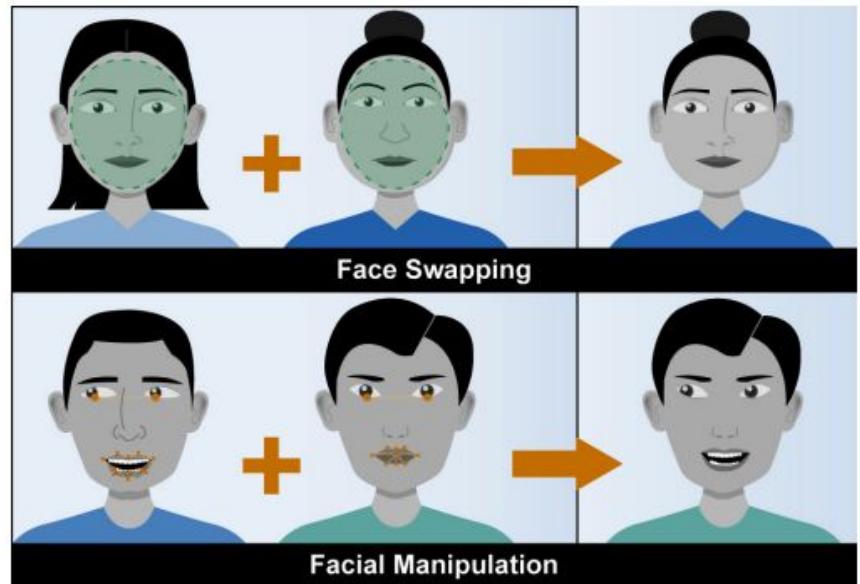


Origen

Se indica que la palabra “Deepfake” se acuñó en un foro de Reddit (2017), cuando se hicieron virales unos videos de alto contenido sexual de algunas celebridades de USA.

¿Qué es?

Un Deepfake es un video, foto, o una grabación en audio que parece real pero que ha sido manipulada con inteligencia artificial.



Source: GAO. | GAO-20-379SP

¿Qué es?

Los Deepfakes son vídeos/audio manipulados para hacer creer a los usuarios que los ven/escuchan a una determinada persona, tanto si es anónima como si es personaje público, realiza declaraciones o acciones que nunca ocurrieron.

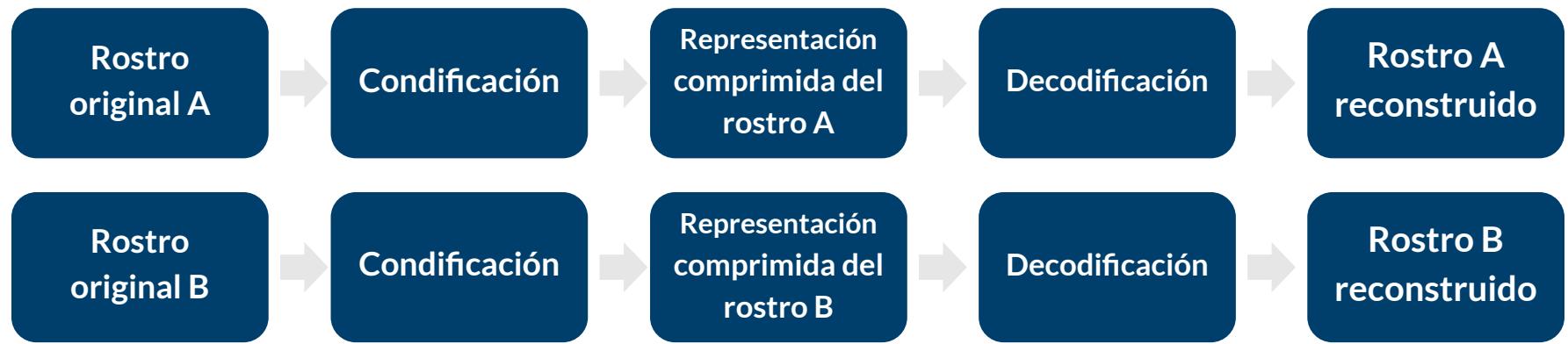
¿Cómo funciona la tecnología de Deepfake?

Existen diferentes algoritmos para crear DeepFakes, pero todos emplean inteligencia artificial, más específicamente, aprendizaje profundo (deep learning), que es un subdisciplina del aprendizaje automático (*machine learning*).

¿Cómo funciona la tecnología de Deepfake?

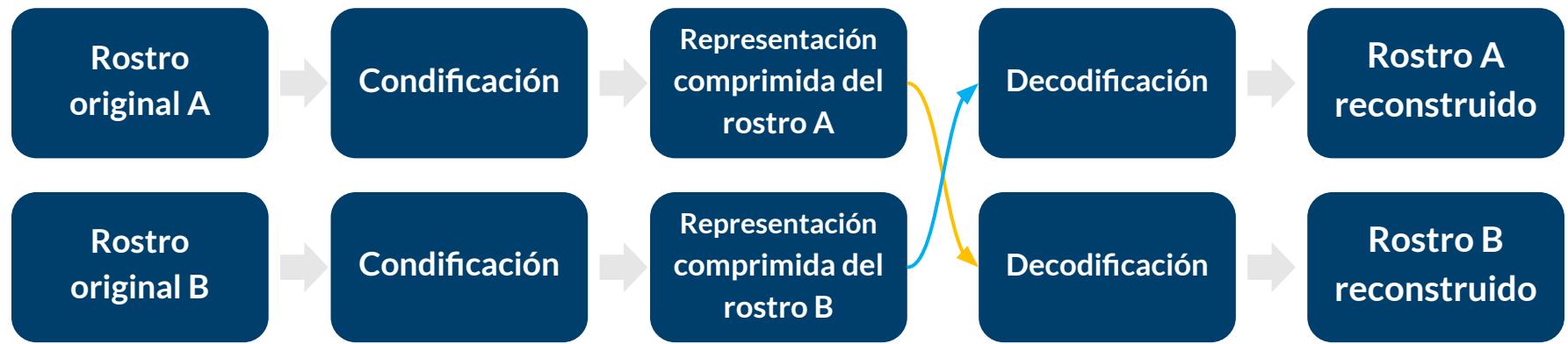
Esto involucra lo que se conoce como redes neuronales artificiales.

¿Cómo funciona la tecnología de Deepfake?



Primer paso para entrenar a los codificador automático.
Cada codificador automático es entrenado para un rostro específico.

¿Cómo funciona la tecnología de Deepfake?



Después de entrenar con éxito los codificadores automáticos, los decodificadores se intercambiado para que el rostro de la primera persona reproduzca el facial expresiones de la segunda persona y viceversa.

Tipos de Deepfake

Modalidades del Deepfake

Deepface: se trata de superponer el rostro de una persona en la de otra y falsificar sus gestos.

En algunos casos, el resultado es tan realista que resulta muy difícil identificar el engaño o fraude.

Modalidades del Deepfake

Deepvoice: en este otro caso se trataría de unir frases y palabras sueltas utilizadas por una persona para crear un discurso. Incluso es capaz de clonar la voz original a partir de estos fragmentos.

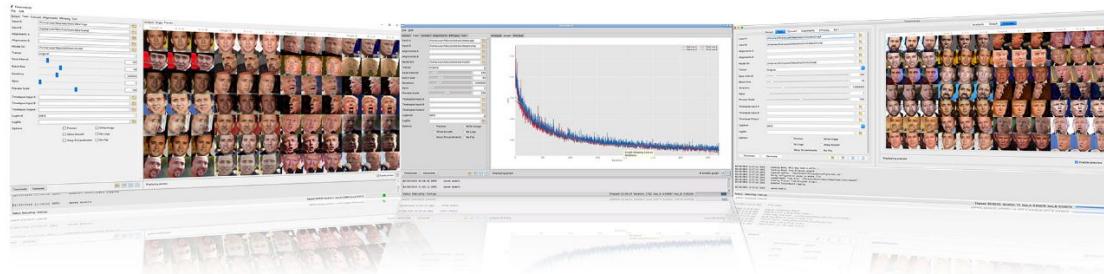
Aplicaciones disponibles para hacer Deepfake

Faceswap



faceswap

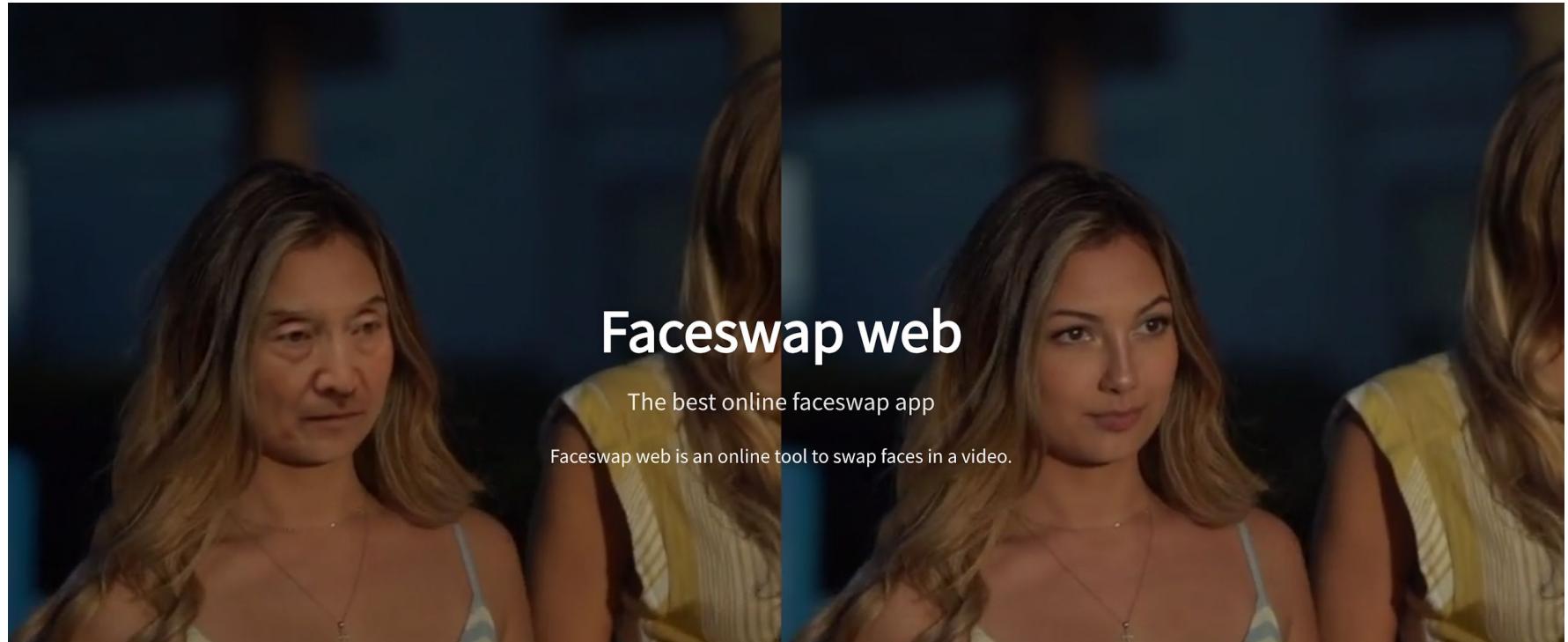
Faceswap is the leading free and Open Source multi-platform Deepfakes software.



Powered by Tensorflow, Keras and Python; Faceswap will run on Windows, macOS and Linux.

<https://faceswap.dev/#content>

Faceswap web



<https://faceswapweb.com>

¿Cómo se hace un Deepfake?

- Descargar software.
- Se recopilan videos de las personas que quieras intercambiar, los cargas en el programa y listo.
- Los programas de Deepfake trabajan cada video como si se tratara de una fotografía y extraen cuadro por cuadro cada imagen que subas.

¿Cómo se hace un Deepfake?

De manera que entre más videos uses, con diferentes iluminaciones –es decir, mientras más información le des a la inteligencia artificial— el resultado parecerá más real.

¿Cómo funciona Deepfake web?



No setup required

Deepfakes Web β is an online app and everything works in the cloud. All you need to do is upload videos.



Private

Only you have access to your learning data, videos and images.



Reuse model

You can reuse your trained model. This allows you to improve the face swapping quality of the results.

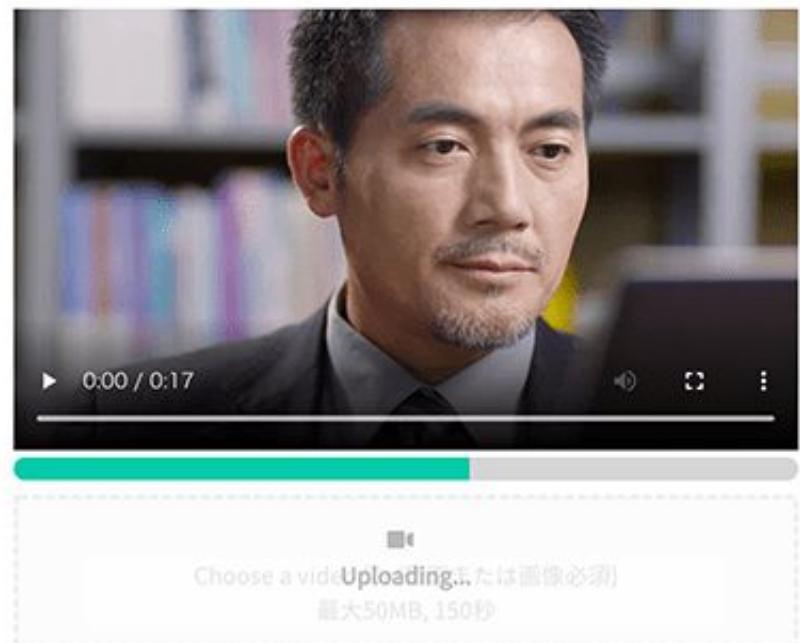
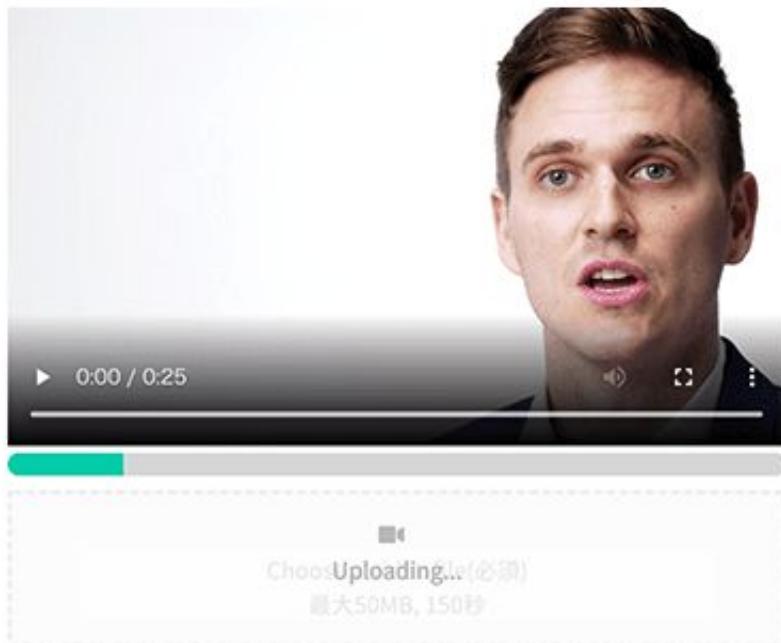
[Create a video](#)

* The quality of the result depends on learning data. It is not guaranteed.

* Spreading malicious fake videos may be punished by law. Please use the site within [Our content policy](#), [the terms of use](#) and the law.

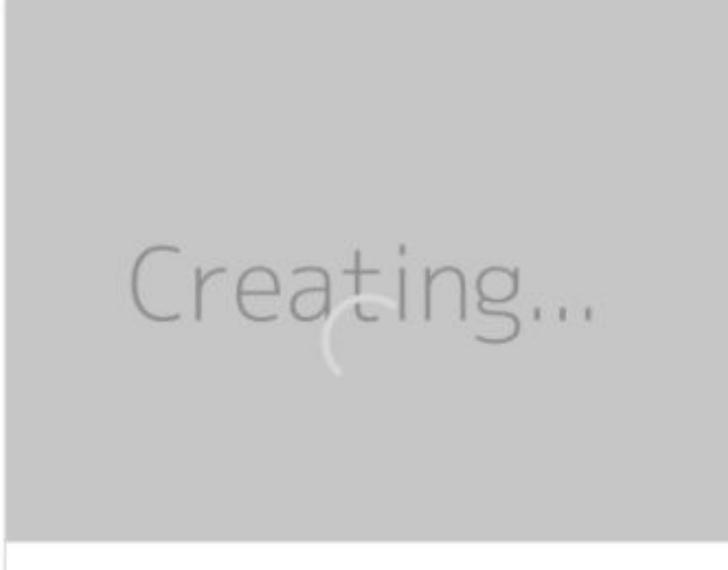
¿Cómo funciona Deepfake web?

1. Upload videos(or images)



¿Cómo funciona Deepfake web?

2. Wait until completion



Creating...

¿Cómo funciona Deepfake web?

3. Done!

You can now watch the video.



¿Cómo funciona Deepfake web?

4. Reuse your model

The lower the loss values are, the higher the quality will be. (They should be less than 0.02)



Learning data of person A

Loss: 0.02658



Learning data of person B

Loss: 0.02798

Voice cloning

Ultra-realistic voice cloning

Overdub lets you create a text to speech model of your voice.

[Download Descript for free →](#)



<https://www.descript.com/overdub>

Voice cloning Reto

Instrucciones

- Descargar la aplicación de clonación de Voz-<https://www.descript.com/overdub>
- Crear DOS audios con DOS (2) temas que te gusten y cuya duración del audio debe ser de 30 segundos cada uno.
- Utilizando la aplicación, combina cada audio para crear un tercer audio producto de la mezcla de los dos primeros.
- Súbelos a la sección de comentarios.

Relación del Deepfake y la ingeniería social

Voice cloning Reto

- Luego escoge un audio de alguno de tus compañeros y mezclalos con el tuyo utilizando la herramienta de edición de la aplicación de Descript.
- Déjanos saber ¿cuál es tu impresión de la aplicación?
- Discute aspectos éticos, facilidad de uso, dificultades y tiempo de aprender a usarla.

¿Por qué debería preocuparnos el Deepfake?

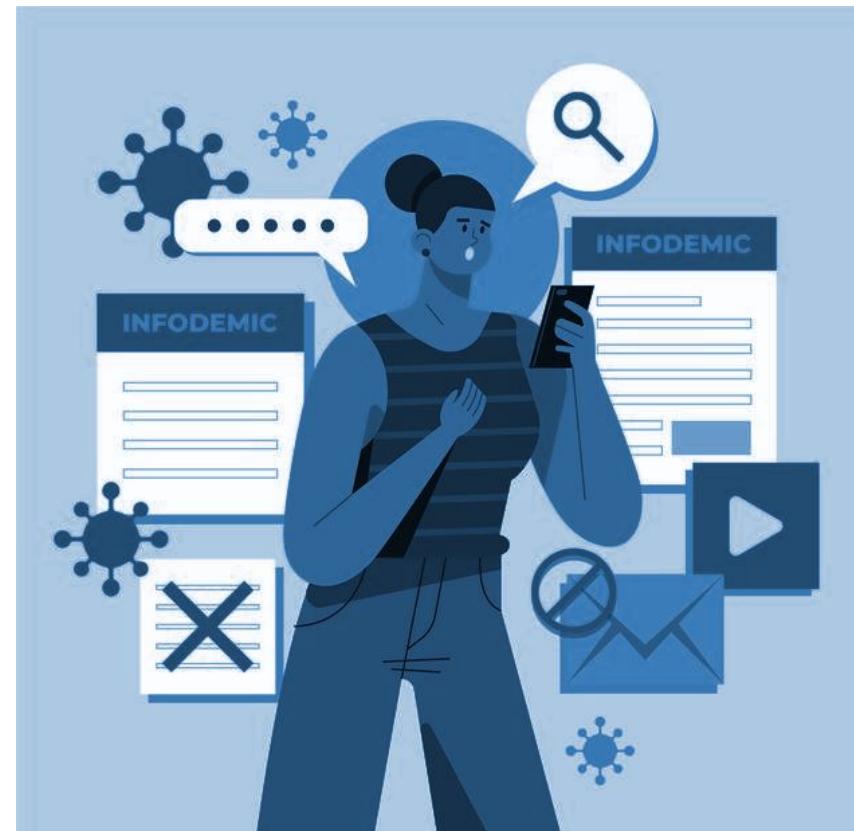
- Las noticias falsas se extienden mucho más rápido que las verdaderas y tienen un 70% más de posibilidades de ser replicadas.
- Sólo el 2% de los jóvenes puede identificar las "fake news".

¿Por qué debería preocuparnos el Deepfake?

Kaspersky y CORPA, dentro de la campaña Iceberg Digital, detalla, quienes son los países que menos logran identificar una fake news el primer lugar lo tienen los peruanos con 79%, seguidos por colombianos (73%) y chilenos (70%).

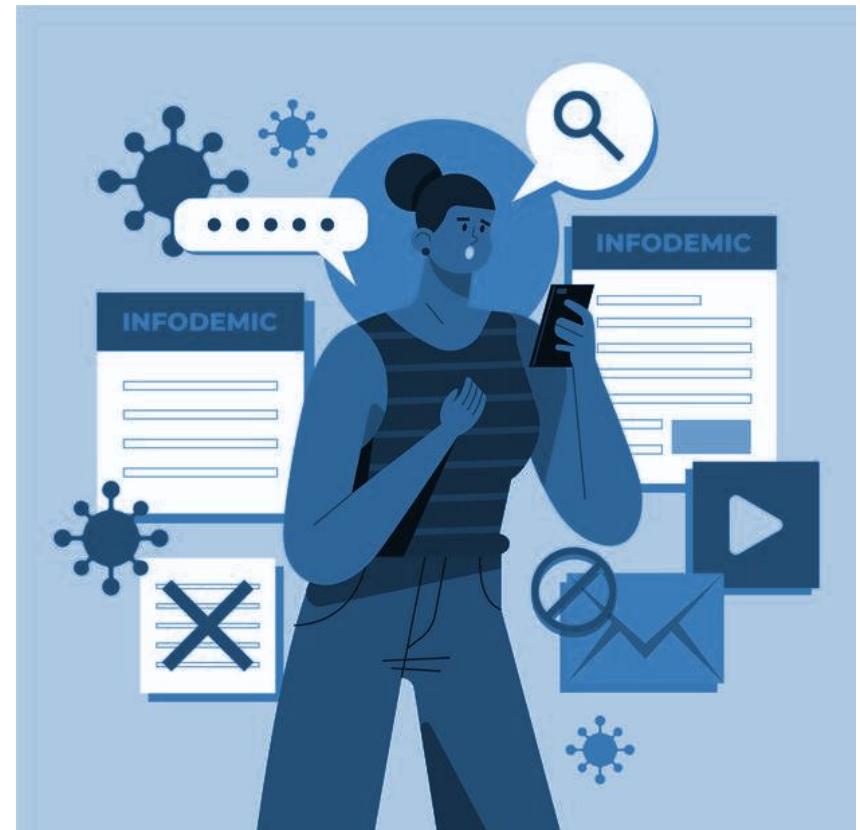
¿Por qué debería preocuparnos el Deepfake?

Detrás se encuentran los argentinos y mexicanos con 66%; y, finalmente brasileños, con 62%.



¿Por qué debería preocuparnos el Deepfake?

Gartner recoge en su informe ‘Predicciones tecnológicas para el 2018’ que en 2022 la mayoría de los países occidentales consumirá más información falsa que noticias reales.



Deepfake: la nueva ingeniería social

¿Modificación en los tipos de ataques de IS utilizando IA?

- Phishing y sus modalidades
 - Spear phishing: tiene como objetivo específico a grupos o individuos.
 - Vishing: voice phishing.*
- Pretexting.

“

El problema central con los “Deepfakes” de audio tiene que ver con capturar no solo el tono de la persona, sino también los gestos específicos del habla.

”

Nisos

¿Modificación en los tipos de ataques de IS utilizando IA?

Los intentos de estafa que usan grabaciones de voz manipuladas, o audio 'Deepfakes', empiezan a ser comunes y por ende más casos de phishing.



Cómo detectar el uso de Deepfake y detenerlo

Claves para identificarlos

- Movimiento NO natural de los ojos.
- Expresiones faciales NO naturales.
- Observar la posición de la nariz.
- Falta de expresión y de emoción.
- Observar la postura del cuerpo.



Claves para identificarlos

- Movimientos del cuerpo no naturales.
- Tono de la piel.
- Observar el cabello y los movimientos.
- Observar los dientes que no lucen naturales.
- Inconsistencia en el audio y sonido del video.
- Imágenes no parecen reales cuando se disminuye la velocidad del audio/video.

Reto

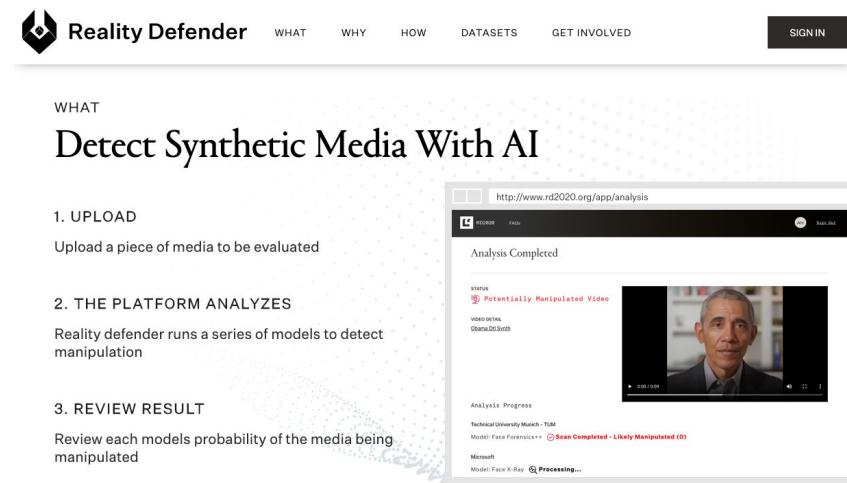
Instrucciones:

- Visitar la página- Detect Fakes de la Universidad de MIT- <https://detectfakes.media.mit.edu/>
- Aparecerán una serie de videos, para que puedas según lo discutido en clases, y puedas identificar cuáles videos son “fake” y cuáles son reales.
- ¡Éxito!

Herramientas de detección de Deepfake

Iniciativas

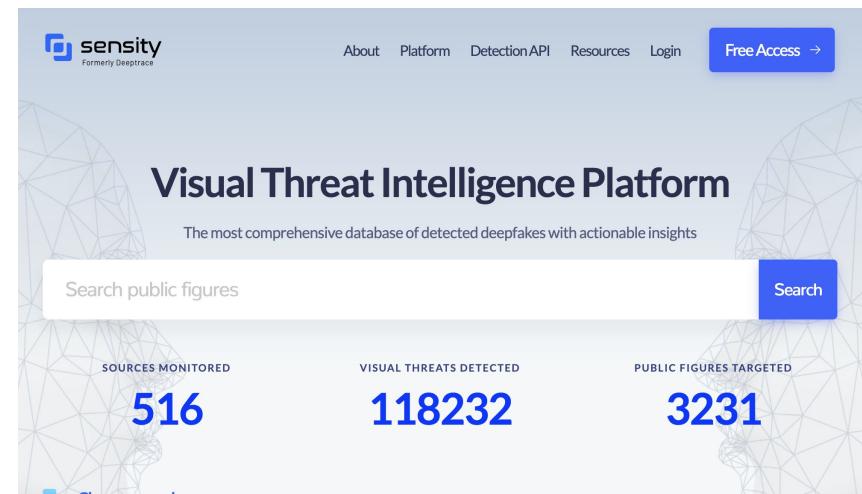
- Facebook y Microsoft lanzaron una iniciativa para detectar el Deepfake.
- Reality Defender
<https://rd2020.org/>



The screenshot shows the Reality Defender website interface. At the top, there is a navigation bar with the logo 'Reality Defender' and links for 'WHAT', 'WHY', 'HOW', 'DATASETS', 'GET INVOLVED', and 'SIGN IN'. Below the navigation, the text 'Detect Synthetic Media With AI' is displayed. The main content area shows a video player with a thumbnail of a manipulated video of former US President Barack Obama. The video player interface includes controls for play, volume, and progress. To the left of the video, there is a list of steps: '1. UPLOAD', '2. THE PLATFORM ANALYZES', and '3. REVIEW RESULT'. The '2. THE PLATFORM ANALYZES' section includes a brief description of how the platform uses models to detect manipulation. The '3. REVIEW RESULT' section includes a note about reviewing model probabilities. At the bottom of the page, there is a footer with links to 'Analysis Progress' and 'Technical University Munich - TUM'.

Iniciativas

- Sensity -
<https://sensity.ai/>
- USA - Legislación para regular los usos - California, Virginia, Texas, Massachusetts y Maryland.
- Mucha educación y capacitación



Reto

Instrucciones:

- Visita los siguientes enlaces y somete los audios que preparaste en los retos anteriores.
 - Sensity: <https://sensity.ai/>
 - Reality Defender: <https://rd2020.org/>
- ¿Cuáles son los resultados? Comparte tu experiencia en los comentarios.

Retos de los procesos de investigación forense en Deepfake

Retos de los procesos

- Estamos ante el abanico de nuevos ciberdelitos debido a la proliferación de los Deepfake.
Ejemplo: pornovenganzas.
- Determinar la autenticidad de la evidencia.
- Limitaciones en los softwares forenses actuales.

Solución: La combinación de técnicas de investigación forense tradicional y tecnología de inteligencia artificial.

Medidas de prevención y protección

Medidas de prevención y protección

Debemos aceptar que:

- La probabilidad de un ataque es alta.
- Individualmente no servirán los controles:
 - Técnicos
 - Administrativos
 - Operacionales
 - De medio ambiente

Medidas de prevención y protección

Aceptar que se necesita una combinación de principios:

- Operacionales
- Administrativos
- Técnicos (lógicos)
- Físicos (ambientales)



Medidas de prevención y protección

Se recomienda lo siguiente:

- Tecnología
- Políticas
- Educación
- Divulgación
- Entrenamiento

Creando una cultura de seguridad

Creando una cultura de seguridad

- No se debe ignorar la interacción persona-máquina.
- Necesitan reconocer los “trucos”.



Creando una cultura de seguridad

- La seguridad de la información es un problema de hardware, software, firmware y peopleware.
- La mejor defensa: educación combinada con tecnología.



Creando una cultura de seguridad

- Todos los clientes/empleados deben tener una actitud hacia la seguridad y cuestionar las cosas.
- Se deben tener procedimientos de respuesta a incidentes y equipos que mitiguen el daño si ocurre un ataque.
- Se debe notificar a los involucrados.

Cómo protegerse y recomendaciones

La mejor manera de estar protegido es el
conocimiento

Recomendaciones

- Educar a las personas, a todas las personas.
- Analizar con antivirus todos los correos que se reciban.
- No informar telefónicamente de las características técnicas de la red, ni nombre de personal a cargo, etc.

Recomendaciones

- Control de acceso físico al lugar en donde se encuentran los documentos importantes de la compañía.
- Políticas de seguridad a nivel de sistema operativo.

Recomendaciones

- Conozca los procesos de ingeniería social, sus principios, sus técnicas, la manipulación y la explotación de los sentimientos y emociones de las personas.
- De esta forma podrá anticiparse a los riesgos de los ataques.

Recomendaciones

- Trabaje en crear la cultura de la cautela, desconfianza y prudencia ante todas las situaciones.
- Los atacantes que usan la ingeniería social prefieren cambiar de víctima cuando se enfrentan a la resistencia educada.

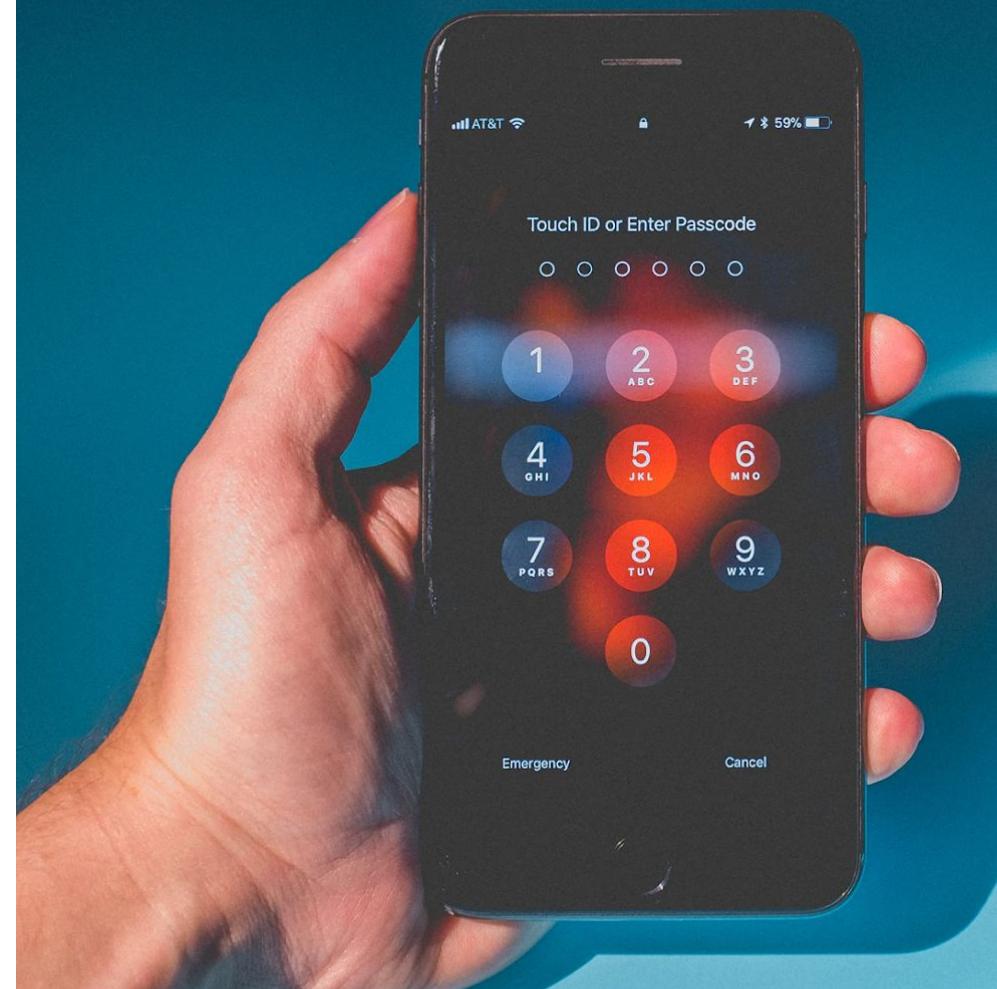
Recomendaciones

Tomar medidas de precaución a la hora de seguir los enlaces que te han enviado a través del correo electrónico, SMS, WhatsApp o redes sociales, aunque sean de contactos conocidos.



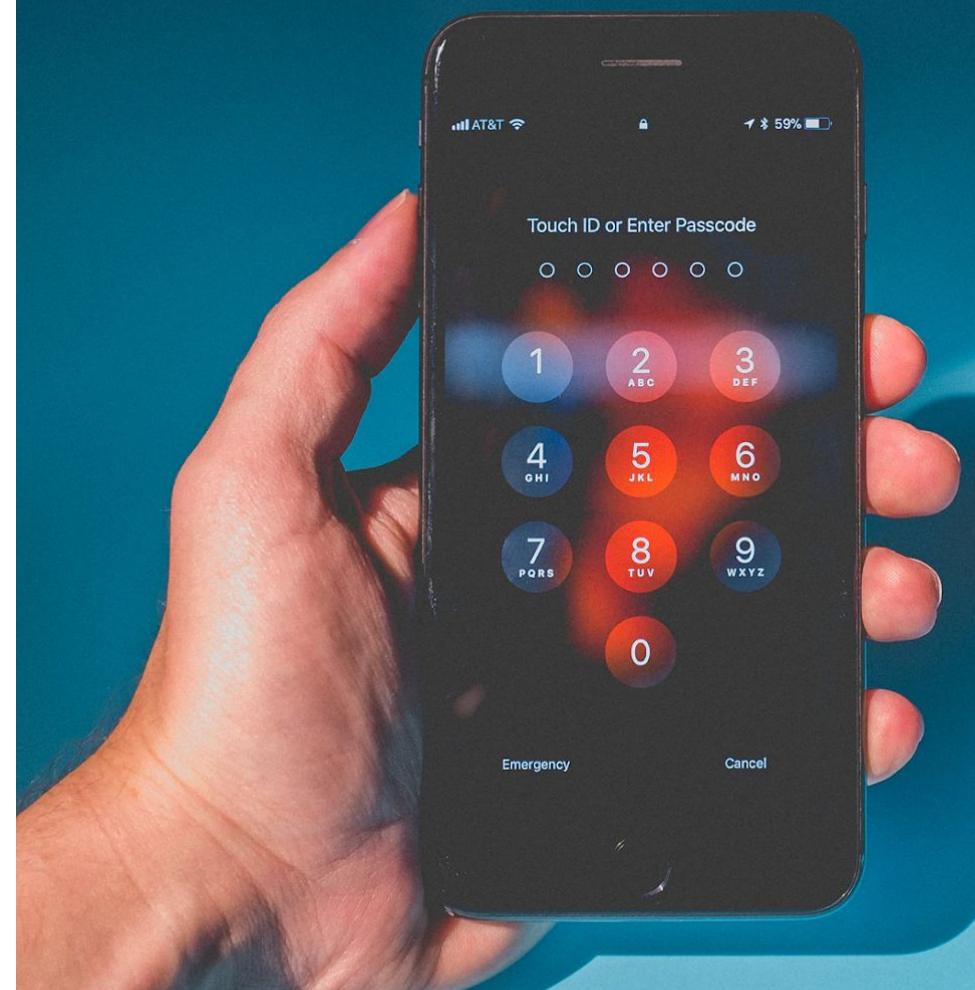
Recomendaciones

Sospecha en caso de que te ofrezcan un premio o trabajo idílico que sea rápido o fácil de conseguir. Como norma general, recuerda que todo en la vida cuesta tiempo y/o dinero.



Recomendaciones

No revelar información personal ni datos confidenciales (credenciales, números de tarjetas de créditos, cuentas bancarias, etc.) por teléfono, email o servicios de mensajería instantánea.



Preguntas

Dra. Aury Curbelo

Especialista en
Ciberseguridad y
Forense Digital

info@Digetech.net



Creando un escenario de pretexting

¡Muchas gracias!

Dra. Aury Curbelo

Especialista en
Ciberseguridad y
Forense Digital.



@acurbelo

