

Experto Universitario en Ethical Hacking

Módulo 5:

Ethical Hacking

Unidad 3:

Ingeniería Social



Presentación

En esta tercera Unidad del módulo, conocerán una de las técnicas más utilizadas en donde pone en manifiesto la poca información que los usuarios tienen con respecto a qué medidas de seguridad tomar.

Aprenderán las contramedidas, así como también conocer sobre las distintas maneras de como utilizan esta técnica.



Objetivos

Que los participantes logren...

- Aprender sobre los conceptos expuestos en el mundo del Hacking.
- Conocer las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades y test de penetración (Pentesting), con una filosofía enfocada en la ética profesional.
- Comprender la importancia de usar cifrado seguro en aplicaciones, abordar vulnerabilidades y potenciales ataques y amenazas, así como la correcta concientización en los usuarios.



Bloques temáticos

1. Introducción
2. Fases de un ataque
3. Contramedidas
4. Ejercicios

Introducción



Si quisiéramos convencer a una persona que nuestro obelisco fue traído de Estonia, o que fue creado por los primeros colonizadores, si supiera algo de nuestra historia, diría que estamos locos, sin embargo, alguien que no tenga conocimientos y hasta le diéramos pruebas “reales”, es muy probable que nos crea.

El factor que se utiliza en este método, es el convencimiento, reforzado con material creado adrede para ser más creíble, y hasta utilizando la ignorancia de la víctima.

Aprenderemos a través de esta unidad, varias técnicas que tendremos que tener en cuenta para no precipitarse y entregar nuestros datos importantes en bandeja, tanto por querer “ayudar”, “cooperar” y “colaborar”.

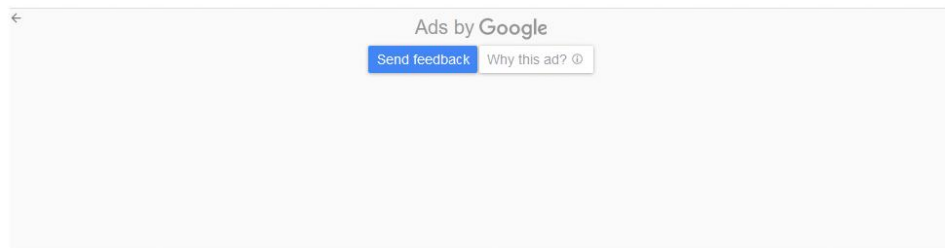
Nadie dice que sea malo, pero una de las mejores contramedidas para no ser víctima de este tipo de técnica, es **ESTAR ATENTOS**.



CREER O NO CREER?

New hacking tool: chocolate

A security group found that London office workers are willing to reveal their network-access passwords for a price--a bar of chocolate.



By Munir Kotadia | April 20, 2004 -- 13:38 GMT (06:38 PDT) | Topic: United Kingdom

A survey of office workers in London found that almost three quarters would reveal their network-access password in exchange for a bar of chocolate.

The survey was conducted by the organizers of Infosecurity Europe 2004, a security exhibition to be held in London next week. They offered 172 commuters at Liverpool Street Station a bar of chocolate if they would reveal their corporate password.

MORE FROM MUNIR KOTADIA



AUSCERT
AUSCERT 2013: PRISM,
soep, and kittens



AUSCERT
AUSCERT 2013: Nigerian
scam victim tells her

Fuente: <https://www.zdnet.com/article/new-hacking-tool-chocolate/>

Infosecurity Europe llevo a cabo una encuesta a trabajadores de oficinas en Londres, donde en un artículo publicado por ZDNet el 20 de abril de 2004, el estudio descubrió que las tres cuartas partes de los trabajadores encuestados están dispuestos a revelar su contraseña de acceso a la red a cambio de una barra de chocolate.

Esto demuestra lo fácil que es acceder a las redes sin tocar una sola pieza.

Al final del día, no importa cuánto de encriptación y tecnología de seguridad se haya puesto en práctica, una red nunca es completamente segura.

Uno nunca puede deshacerse del eslabón más débil, **el factor humano.**

No importa la tecnología utilizada como firewalls, redes privadas virtuales (VPN), o dispositivos de encriptación, si los empleados están dispuestos a dar acceso a los sistemas a cualquier persona que lo solicite.

¿Qué es la ingeniería social?



Es una técnica para disponer y obtener acceso a información vital, privilegiada y confidencial y/o recursos que podrían servir para un ataque diferente.

Su mayor éxito se basa en la parte humana, a través del uso de factores como engaños, persuasión e influencia.

Suelen ser utilizados desde cualquier parte (local, remota), y con cualquier tecnología de uso (teléfono, celular, email, papel, etc).

Puede estar dirigido a:

- **Una organización objetivo**
- **A un determinado empleado/a**
- **A un determinado grupo de personas**
- **A un usuario en general**
- **Todo aquel que se encuentre relacionado con éstos.**

El contacto realizado es hecho supuestamente por:



- ✓ **Prestador/a de servicios.**
- ✓ **Conocido/a, amigo/a o pariente de alguien.**
- ✓ **Autoridad.**
- ✓ **Colega de otro sector o sucursal.**
- ✓ **Anónimo.**
- ✓ **Impersonalizado.**



En tipo de modo:



Casualidad

Directo: consulta inocente y típica, firmar entrega de regalo, encuesta, completar planillas, etcétera.

Indirecto: involucrar a terceros ficticios o reales sin conocimiento.

Trampa directa e indirecta: envío de correo con material en DVD, suplantación de pendrive, etcétera.

Invasivo: acceso a recintos, irrupción dentro de oficina con o sin utilización de lockpicking, instalación de hardware espía (recolector o transmisor de datos, uso de Keylogger)

A través de los medios:



Cara a cara con protagonista: Mediante diálogo.

De carácter secundario: Como empleado de correo o cadetería.

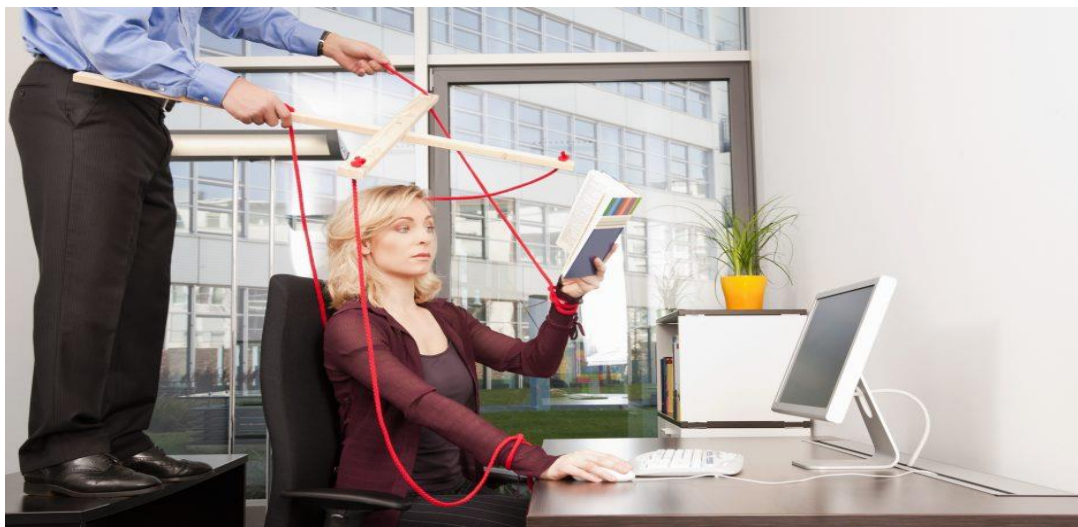
E-mail: Todas las formas imaginables, algunas detalladas más adelante.

Teléfono, impersonal: Diálogo.

Fax: Enviando documentos con requerimientos de modificación de datos o con información sensible.

Medios y agentes combinados: el intruso envía un e-mail de un supuesto superior de una sucursal, avisando a la recepcionista de otra sucursal que en unos momentos va a pasar alguien a recoger un dato o determinada información para que se la tenga preparada.

Fin del acto:



Información: busca pequeñas pistas o datos para planificar el embate.

Acciones: busca generar determinadas acciones.

En una **Prueba de Intrusión (Pentest)** a menudo se pide realizar precisamente esto, emplear tácticas de ingeniería social para descubrir si los empleados están siguiendo las políticas internas y no revelar información sensible.

Un ingeniero social es alguien que utiliza el engaño, la persuasión, y la influencia para obtener información que de otro modo no estará disponible.

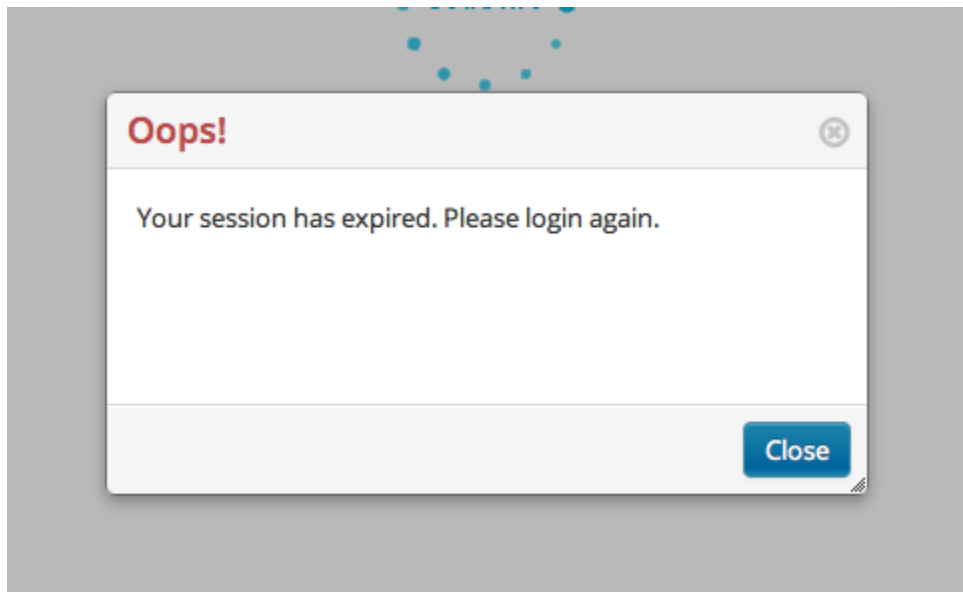


Existen dos tipos de ingeniería social:

- **Basadas en la tecnología**
- **Basadas en Humanos**

La ingeniería social basada en la **tecnología**, utiliza la tecnología para engañar a los usuarios en dar información sensible.

Un ejemplo clásico de una tecnología basada en ataque es tener una ventana emergente en la computadora de un usuario y pedir su contraseña, como se demuestra en el ejemplo.



Aquí el usuario es informado de que su sesión ha finalizado, y se le pedirá que introduzca su nombre de usuario y contraseña nuevamente. Después de que el usuario hace clic en el botón Enviar, el nombre de usuario y contraseña son enviadas al ordenador del intruso.

El intruso puede utilizar esa información más adelante para acceder a la red de la víctima.

En cambio, la ingeniería social basada en **humanos** no emplea la tecnología, sino que se hace en persona, o a través de una llamada telefónica.



Ambas técnicas se basan en el comportamiento previsible del ser humano que quiere ayudar a otro ser humano.

A través de una llamada por teléfono, un intruso podría solicitar directamente un usuario y una clave, previo reconocimiento y de acuerdo al escenario que tenga en el destino, de esa manera habría una posibilidad de que se lo pasen sin ningún inconveniente.



Aquí hacemos un homenaje a una persona grandiosa, que ha dejado una gran huella en las personas que lo escuchamos y nos hizo reír como locos, en mi caso particular lo conocí personalmente, y me enseñó muchas técnicas para hablar por teléfono con las personas.

Un gran saludo al Dr. Tangalanga.

Fases de un ataque



A continuación se exponen diversos tipos de fases para poder llevar a cabo la técnica.

✓ **Identificación del objetivo**

Utilizando técnicas de recolección como:

✓ **Dumpster diving**

✓ **Internet**

✓ **Vigilancia personalizada**

✓ **Se busca establecer una relación con el objetivo, a través de factores la codicia, el miedo, la ignorancia, las ganas de ayudar.**



- ✓ Luego de concretar ese vínculo, se diagrama hasta donde uno quiere llegar, por ejemplo, si el atacante busca una clave, crea el escenario para llegar a ella, que no es lo mismo que crear un escenario para que alguien nos dé una información privilegiada

Una técnica muy utilizada, es el **PHISHING**

De: "no_reply@openbank.es" <no_reply@openbank.es>

Para:

Asunto: Usted debe entrar al sistema de su cuenta en el plazo de 7 dias

BCC: Fri, 4 Jul 2008 12: ... +0300

openbank

Estimado usuario Open Bank

Durante nuestra verificación regular no pudimos verificar sus datos. La razón es que sus datos están incompletos o incorrectos. Para impedir que su cuenta sea minusválida, le rogamos entrar al sistema de su cuenta (login) y asegurarse de que sus datos de cuenta están completos.

Para entrar al sistema de su cuenta por favor haga clic al link siguiente:

<https://bancaonline.openbank.es/servlet/PPProxy?app=DJ&cmd=232132>

Usted debe entrar al sistema de su cuenta en el plazo de 7 días después de recibir esta notificación, en otro caso se limita el acceso a su cuenta.

Gracias por usar Open Bank.

Por favor no conteste a esta carta electrónica. La carta fue enviada a esta dirección automáticamente y no puede ser contestada. Para recibir la ayuda entre al sistema usando sus datos (log in) Open Bank y elige "Ayuda" en la cabeza de cualquier página.

openbank 

Oficina Principal de Openbank
Plaza de Manuel Gómez Moreno, 2 28020 Madrid
902365361 No Client.
901247361 Clientes

Falsificación usada suplantando una identidad para engañar y hacerse pasar por la misma identidad.



From: ADINET WEBMAIL ADMIN <[REDACTED]@hispeed.ch>

Date: 2010/12/20

Subject: Verifique su dirección de correo electrónico Adinet

To:

--

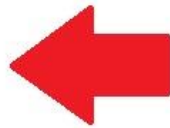
Adinet Estimado WEBMAIL CUENTA DE USUARIO

En estos momentos estamos actualizando nuestra base de datos y todos Cuenta Adinet WEBMAIL necesitan de ser verificada.
Para completar la activación de su cuenta con nosotros, usted está obligado a responder a este mensaje y escriba correctamente la información que se requiere de usted.

Escriba su Nombre de Usuario y Contraseña en el espacio provisto (*****) Usted está obligado a responder a este e-mail dentro de las próximas 48 horas.

Si no se vuelve a nosotros, su cuenta de Adinet WEBMAIL será desactivado de la base de datos.

NOMBRE COMPLETO: *****
FECHA DE NACIMIENTO: *****
Nombre de usuario :*****
Contraseña :*****
Contraseña Re-Type :*****

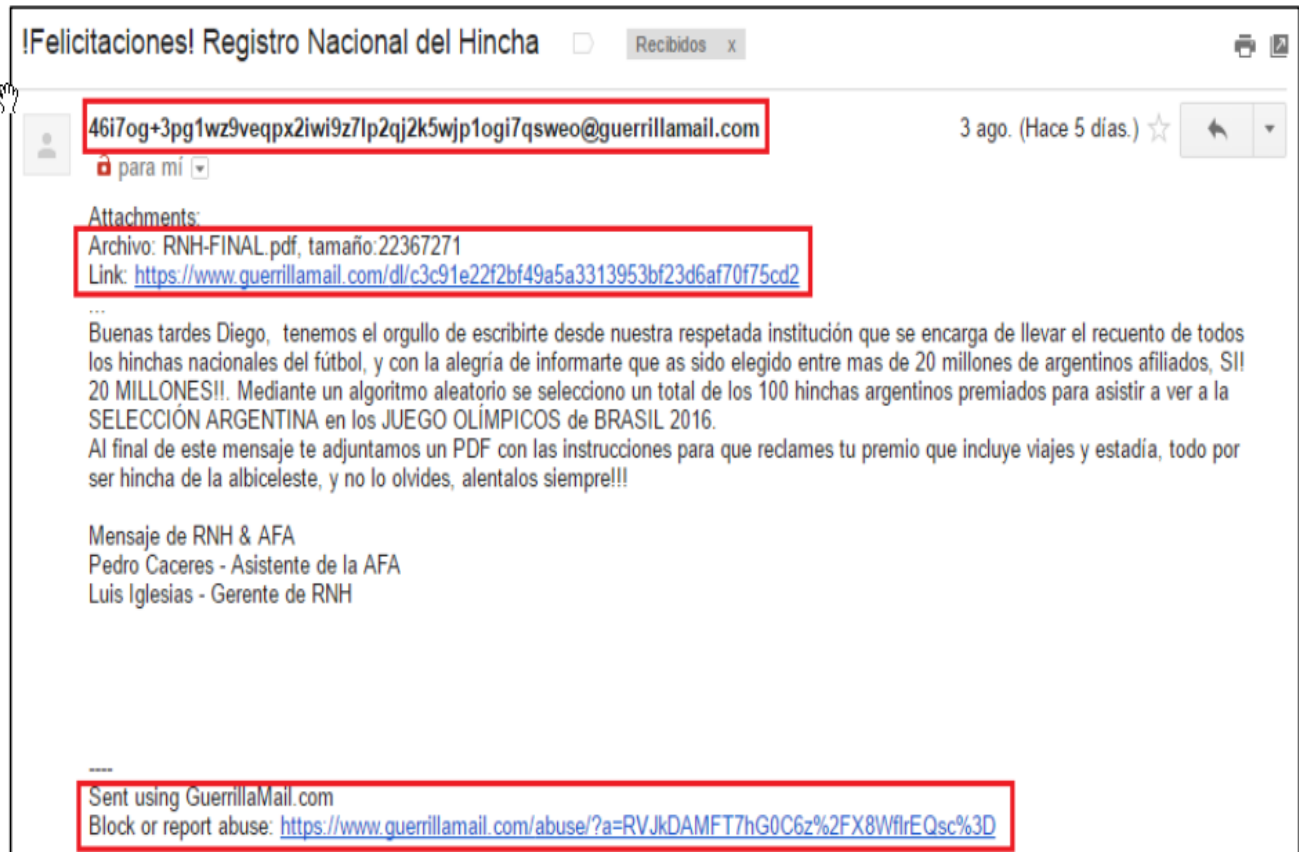


**Nunca hay que
proporcionar esta
información por correo**

También puede confirmar su dirección de correo electrónico, acceda a su cuenta de correo electrónico en
<http://correo.adinet.com.uy/cp/ps/Main/login/Login?d=adinet.com.uy>

Gracias por utilizar Webmail Adinet

El solo hecho de hacer un “CLICK”, sobre el enlace, puede desarrollar un sinfín de tareas y procesos malignos, por ejemplo, un Ransomware que cifre todos los datos o capturar las credenciales cuando se logue.



Que podemos notar de este email, que fue muy utilizado en Argentina, antes del comienzo del mundial de futbol del 2016?

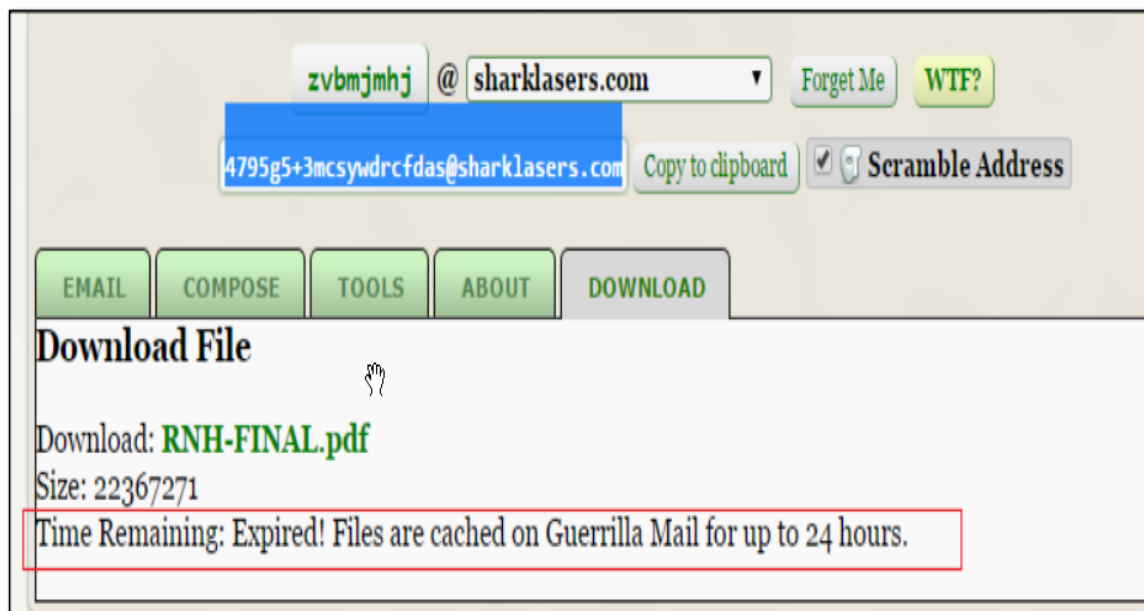
1- Generado desde Guerrilla Mail (sitio para crear mails anónimos y envíos masivos)

Es muy común utilizar sitios que permitan el envío de mails anónimos, los cuales generan en el intruso un “anonimato” temporal y la posibilidad de que la víctima interprete que el mail es real, siempre y cuando el formato del mismo aparente eso.

2- Si contiene errores ortográficos, es porque es un modelo adaptado por idioma, uno de los errores más comunes de los inexpertos en enviar campañas de Phishing.



3- Generalmente los links de descarga duran 24 horas, de esa manera se protegen.

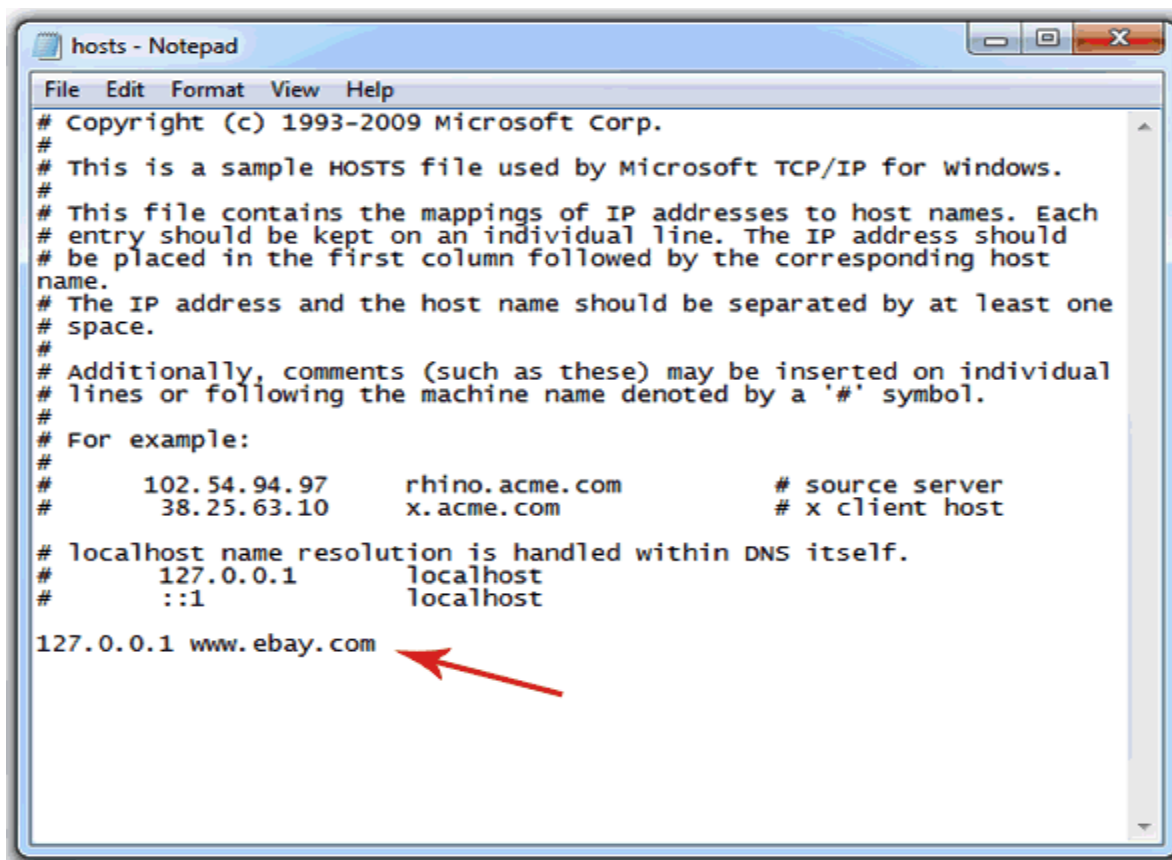


Otros tipos de ataques relacionados con la ingeniería social

Pharming:

Es la explotación de una vulnerabilidad en el software de los servidores **DNS** (Domain Name System) o en el equipo del propio usuario, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta.

De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá a la página web que el atacante haya especificado para ese nombre de dominio.



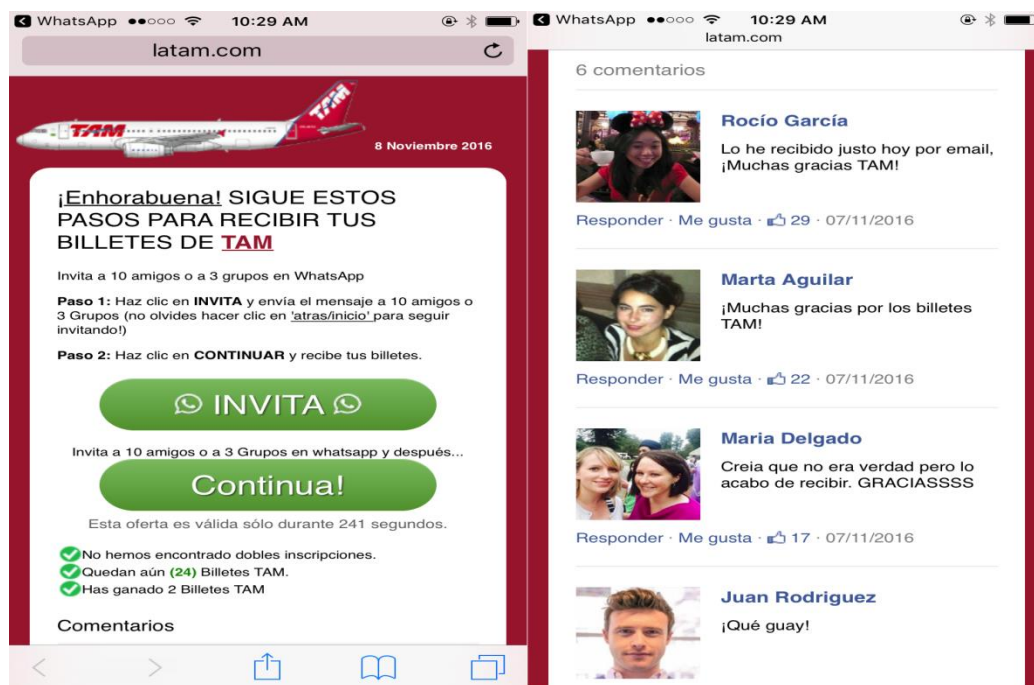
Una técnica muy conocida, que no hace falta utilizar DNS, es a través del archivo HOSTS, el cual al tener la posibilidad de editarlo, uno puede insertar una IP que se haga pasar por el dominio que quiera, de esa manera, cuando en la PC pongan el dominio, apuntará directamente al servidor WEB ilegítimo.



Spam:

Utilizado como medio para hacer llegar al usuario del correo publicidad no deseada, Phishing, código malicioso, etc.

En esta caso depende de que el usuario sea curioso y vea su contenido.



Hoax:

Mensajes de correo electrónico de distribución masiva, que intentan persuadir al usuario a que responda al mensaje o haga algo con el objetivo de recolectar direcciones de correo electrónico o algún otro dato confidencial.

Contrameditadas



Recordar que siempre dependerá del factor humano, por ende, tenemos que disponer de ciertas medidas y políticas recomendadas y que se cumplan (sobre todo).

Concientización institucional acerca de la ingeniería social.

Políticas internas que contemplen la descentralización de datos y el resguardo de la información.

Políticas acerca del buen uso de recursos de comunicación e informáticos, por parte de todos los empleados.

Lucidez mental.

Mínimos privilegios

AntiSPAM, configurado con BlackList (mitiga Phishing)

Como evitar el uso de Ingeniería Social:

Limitar filtración de información sensible:



La información volcada en sitios web, bases de datos públicas, registros de Internet, Registros DNS, etc. debería ser genérica, por ejemplo, si se trata de una empresa, limitarla a los números de teléfono y cargos en lugar de nombres:

Tel. ###-##### - Administrador de Redes en vez de Tel. ###-##### - Juan Perez.

Existen en la red, miles de bases de datos, que se van acumulando y llenando de datos, a través de la recolección automática de los mismos, y no solamente de datos personales, también las hay de claves.

71@gmail.com	milano71
sce@gmail.com	camposja
slu@gmail.com	v10838033
s@gmail.com	zaq12wsx
y@gmail.com	fbobh_c4wu
g@gmail.com	soccer123
da@gmail.com	duc
da@gmail.com	duc@ti62*
es.169@gmail.com	1234juan
radio@gmail.com	calafate74
ola7@gmail.com	alwayshope
ones@gmail.com	july87407
do@gmail.com	071822juan
he.1@gmail.com	piquin69
ca@gmail.com	Holahola1
fva@gmail.com	cano2009
396@gmail.com	jci01298
981@gmail.com	jmc1981
4@gmail.com	mexican12
juan.cano@gmail.com	jimena07

[+] 2001 emails found.
 [-] Create file with data.
 [+] The file 200620-112939.json was created.

Formular una política interna para los procedimientos de soporte técnico:

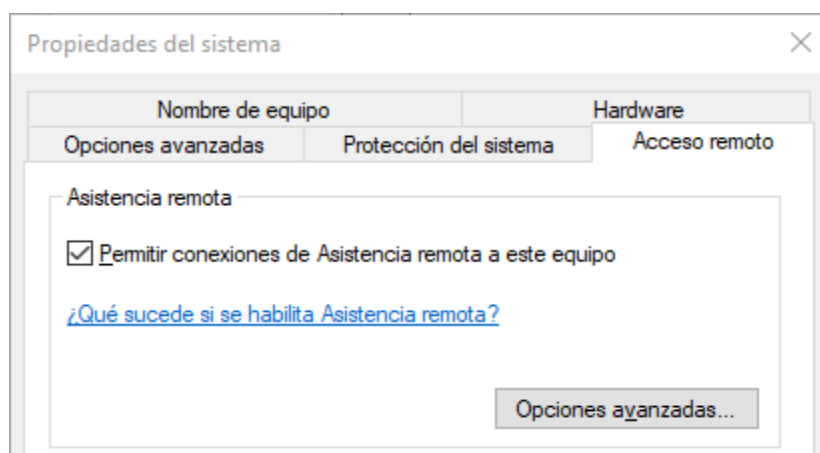


Por ejemplo, solicitar un número de legajo (o alguna otra forma de identificación) a un supuesto empleado que solicita soporte técnico.

Establecer claramente los casos en que se brinda soporte.

Instruir al personal de soporte para que nunca brinde información acerca de las tecnologías, políticas, etc. utilizada por la empresa.

Poner especial cuidado en el acceso remoto:



Si bien es una gran herramienta de productividad, es también una potencial puerta de ingreso para los hackers.

Si duda de la veracidad del correo electrónico, jamás hacer clic en un link incluido en el mismo.

Nunca abrir un enlace recibido por correo electrónico. Escribir la dirección en la barra de su navegador.

Si se recibe un email de tipo de phishing, hoax, u otro, ignorarlo y jamás responderlo.



Comprobar que la página web en la que se ha entrado es una dirección segura que ha de empezar con **https://** y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.

Cerciorarse siempre escribir correctamente la dirección del sitio web que se desea visitar ya que existen cientos de intentos de engaños de las páginas más populares con solo una o dos letras de diferencia.

Esta técnica se llama TypoSquatting, donde aprovecha los posibles errores de gramática en escribir una URL.

Examples of TypoSquatting

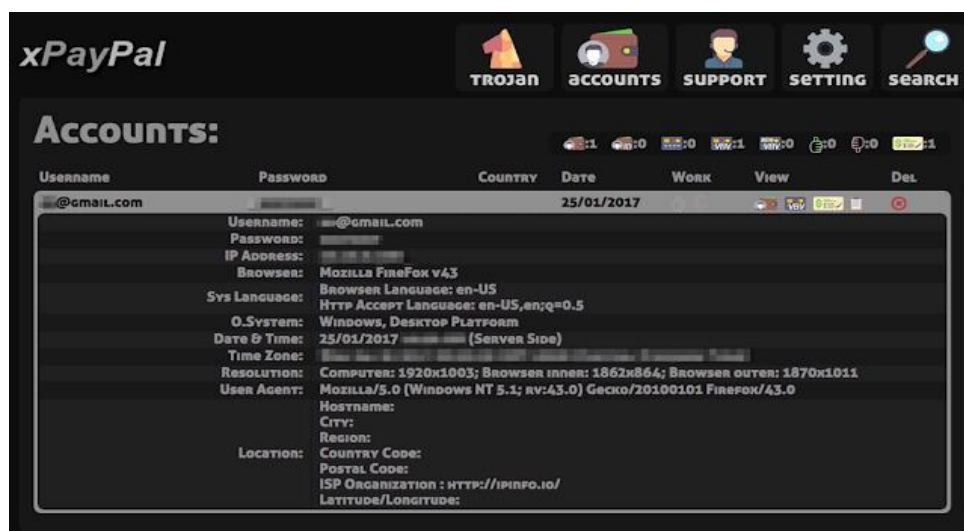
Real Domain Targeted	Typosquat Domain Example
www.github.com	www.gIthub.com
www.google.com	www.gougle.com
www.amazon.com	www.amozon.com
www.victoriaSsecret.com	www.victoriasecret.com
www.homedepot.com	www.homdepot.com

Si sospechamos que fue víctima del Phishing, cambiar inmediatamente todas las contraseñas y ponerse en contacto con el Área de Sistemas de la empresa para informarles.

Conocimiento de las directivas de seguridad de la empresa:

Si no existe, deberá desarrollarse, y difundir la misma a todos los empleados de la organización que trabajen con computadoras. Concientizar a cada uno sobre su responsabilidad en cuanto a la seguridad de la información que maneja.

Hay que entender que los mensajes pueden ser muy convincentes, de hecho, hay kits preparados para realizarlos y enviarlos de forma automática a la espera de la captura de credenciales.

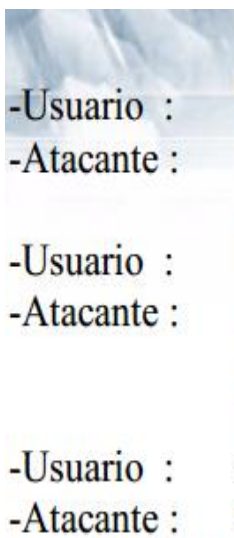


En esta imagen, se ve como el programa va detectando todos los datos que la víctima va insertando.

Otro Ejemplo

Les paso este dialogo, muy entretenido, pero que los dejara pensando, hasta donde se podría llegar.

- Usuario : Hola?
- Atacante : *(Denotando prisa y fastidio) Si, buenos días habla Marcelo de acá de sistemas...*
- Usuario : Marcelo?... de sistemas?
- Atacante : *Si(con voz segura), tenes algún problema con tu usuario*

- 
- de red? porque acá figura que hay algún problema!*
 - Usuario : Mira que yo sepa no.
 - Atacante : *Bueno puede ser un error nuestro, a ver... decime tu... nombre de usuario... o tu dirección de mail...*
 - Usuario : Si.. ehh.. es.. "agonzalez"...
 - Atacante : *mmm, seguro... a ver... agonzalez... agonzalez... aha si acá estas ok, ahora dame tu actual contraseña así la cambiamos por una nueva para no tener mas problemas.*
 - Usuario : Si... es "marina".
 - Atacante : *Ok, gracias hasta luego...*
- [Fin del Dialogo]

Ejercicio 1 Unidad 3



La idea sería la siguiente:

Para participar hay que ponerse en uno de los dos roles (el IS o el especialista de seguridad).

Los que sean especialistas, deberán crear un mail personal cada uno, en cualquier servidor de correo, y se los publican a los que hagan de IS (habrá un foro especial para eso).

Los que sean IS, deberán crear un ejemplo de phishing y enviárselos a los que serían los especialistas de SI.

OBJETIVOS DE CADA UNO:

Los especialistas de SI, el objetivo deberá ser analizar el phishing y ofrecer recomendaciones de cómo evitar caer al mismo.

El objetivo del Intruso, es realizar un phishing y enviárselo, **nada más.**

Obviamente en caso de necesitar ayuda para realizar el ataque, el instructor también ayudara, pero en este caso en forma de guía (**no se olviden que no se enseña a atacar en esta cursada!!!!**)

No es obligatorio realizar este ejercicio, pero se los recomiendo.

Dudas y consultas sobre el mismo, al instructor.

Todo quedará publicado en el foro, pero antes de postear tanto el tipo de IS como la forma de solucionarlo, tienen que informar al instructor, si alguien postea sin autorización, el post será borrado sin previo aviso.

No es una competencia, es una manera divertida e interactiva de aprender, sobre todo en lo que sabemos que es una técnica muy utilizada y debemos saber todo para mitigarla, por lo que el instructor ayudará a los que les toque ser especialistas.

Recomendación del instructor

Por una cuestión ética y legal, no podemos enseñar cómo hacer un Phishing, pero podemos nombrar que una de las mejores herramientas para poder realizarlo se llama SET.

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 5.4.1 [---]
[---] Codename: 'Walkers' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

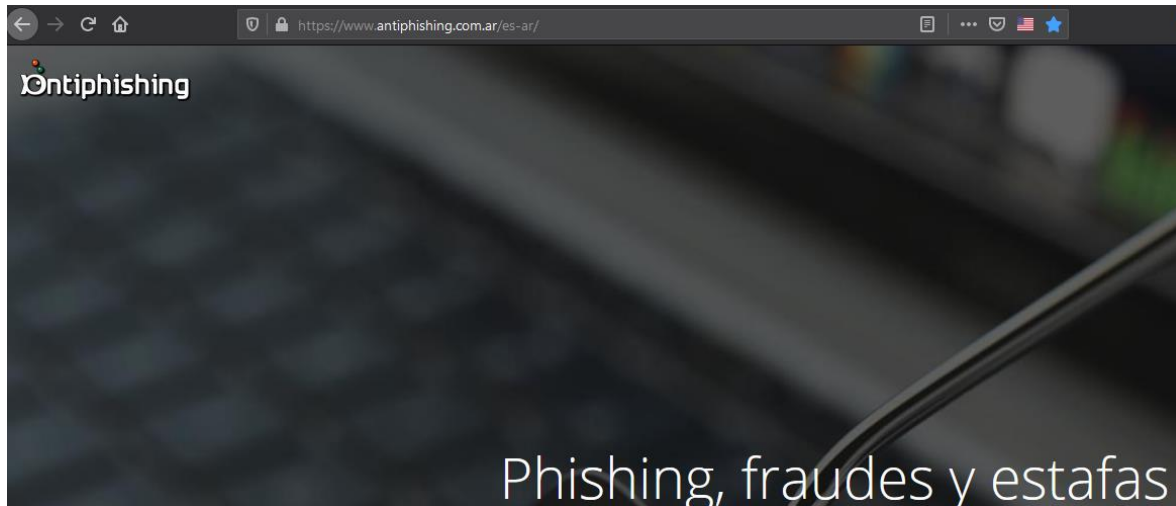
Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

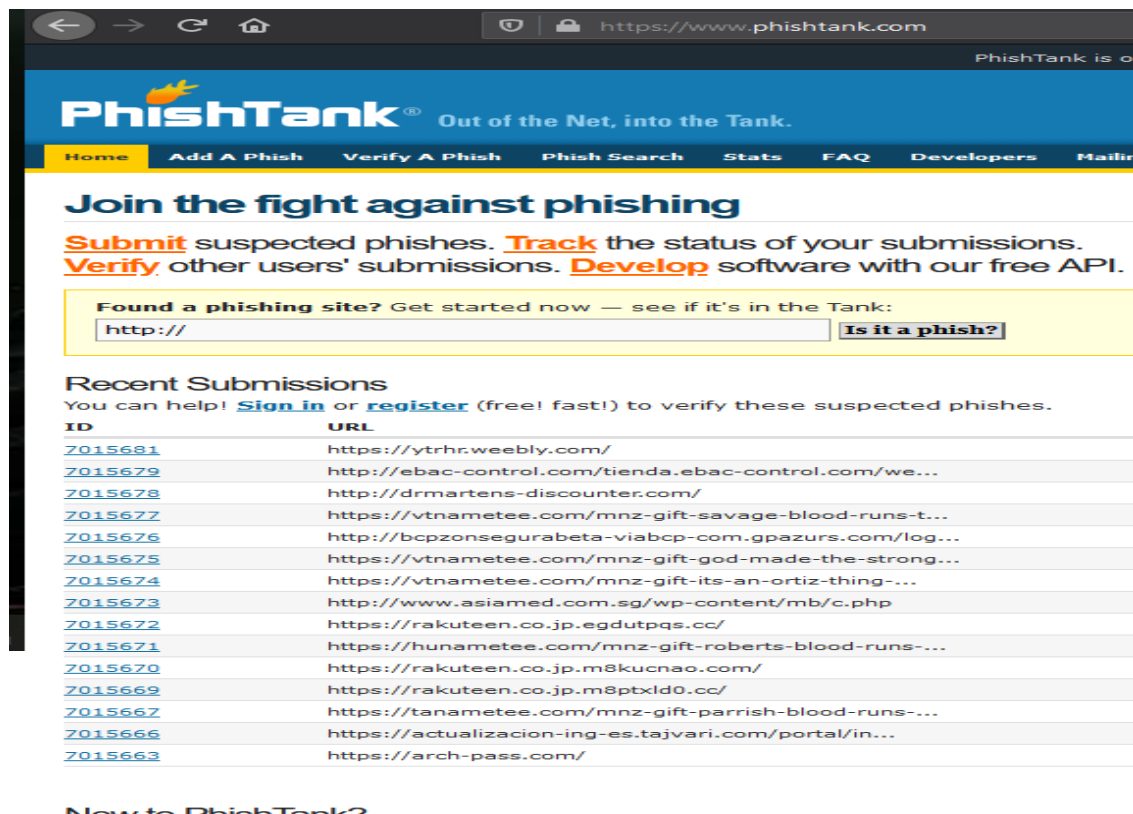
99) Exit the Social-Engineer Toolkit
```

Es RESPONSABILIDAD del alumno, el uso de la misma, ni la universidad ni el instructor son responsables de los actos del alumno/a.

Así como hablamos de ataques, también podemos hablar de defensa, a continuación les recomiendo uno de los mejores sitios para poder denunciar PHISHING y colaborar con la comunidad.



A nivel internacional disponen de:



Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy **IMPORTANTE** que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.



Bibliografía utilizada y sugerida

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU.

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México.

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España.

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU.

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU.

Link complementarios:

<https://mejorshackerfamosos.blogspot.com.ar/2015/07/biografia-del-hacker-kevin-mitnick-vida.html>

<http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/>

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado)