

# Factor humano

Mikel Egaña Aranguren

[mikel-egana-aranguren.github.io](https://mikel-egana-aranguren.github.io)

[mikel.egana@ehu.eus](mailto:mikel.egana@ehu.eus)



# Factor humano

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



# El factor humano

“

*Al final, un sistema de seguridad es tan efectivo como lo es el más débil de sus eslabones. En el caso de la seguridad online, el eslabón más débil es siempre el factor humano*

**Eugene Kaspersky**

# El factor humano

“

*Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es una llamada a un empleado desprevenido y acceden al sistema sin más.*

**Kevin Mitnick**

# El factor humano

Kevin Mitnick en los 90's fue considerado el Cybercriminal más buscado por el FBI

En uno de sus primeros ataques de ingeniería social explicaba cómo necesitaba un número de solicitante para "pinchar" el Departamento de Vehículos de Motor (DMV)

# El factor humano

Para lograrlo llamó a una comisaría y se hizo pasar por alguien del DMV. "¿Su código de solicitante es el 36472?", a lo cual el agente contestó: "No, es el 62883"

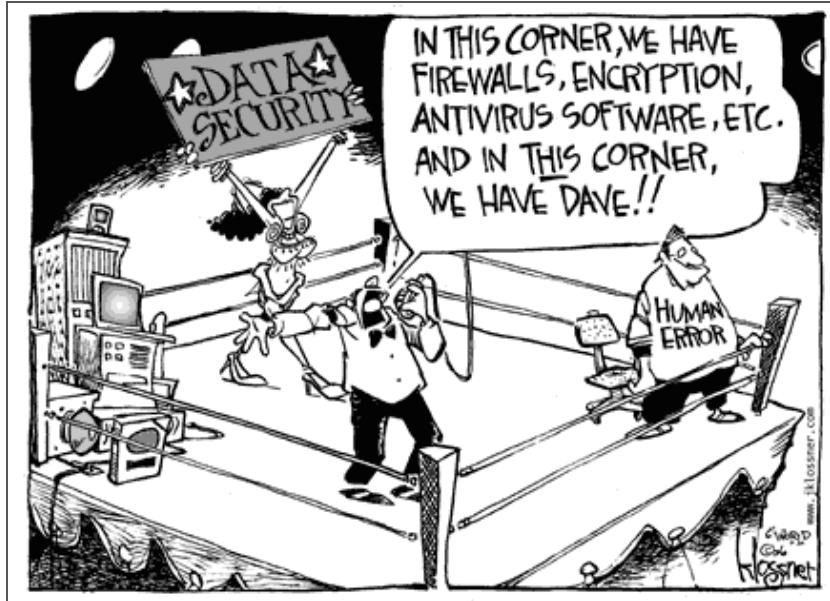
*Es un truco que he descubierto que funciona muy a menudo. Si pides información confidencial, la gente, sospecha de inmediato*

# El factor humano

*Si finges que ya tienes esa información y dices algo que está mal, la gente suele corregirte y te recompensa con la información que estabas buscando*

*Ese principio básico de la ingeniería social se unía a otro esencial: la gente suele ser el eslabón más débil de una cadena de seguridad, porque "la gente siempre tiene intención de ayudar"*

# El factor humano



# El factor humano

## Un asesor de Obama, 'cazado' en Facebook

- Jon Favreau pide disculpas a Hillary Clinton por difundir en Internet una fiesta con una silueta de la ex primera dama

EFE / ELPAÍS.COM | 6 DIC 2008 - 01:20 CET

Archivado en: Estados Unidos · Tecnología



Una de las principales características de la campaña del presidente electo de Estados Unidos, **Barack Obama**, que ha llevado al máximo partido a las redes de contacto social, particularmente a Facebook, ha traído problemas a uno de sus principales asesores.

El próximo director de Discursos de la Casa Blanca, el escritor y guionista Jon Favreau (derecha), ha sido acusado de haber difundido en Internet una foto en la que aparece bebiendo alcohol y besando a una figura que se asemeja a la ex primera dama Hillary Clinton.



El asesor Jon Favreau (derecha) aparece junto a una figura de Hillary Clinton.

# El factor humano

POLÉMICA EN LA RED

## Paula Vázquez la lía en Twitter

La popular presentadora publica por error en internet su número de teléfono móvil

22.10.12 - 19:00 - REDACCIÓN | MADRID

0 Comentarios |  Twittear

 Compartir

 Recomendar 110



Conectado a diariovasco.disqus.com...

# El factor humano

**VIRALES** 09/02/2018 11:08 CET | Actualizado 09/02/2018 11:09 CET

## Rosalía publica por error el número de teléfono de Pablo Alborán en Instagram

Se ha marcado un Paula Vázquez.

[https://www.huffingtonpost.es/2018/02/09/rosalia-publica-por-error-el-numero-de-telefono-pablo-alboran-en-instagram\\_a\\_23357228/](https://www.huffingtonpost.es/2018/02/09/rosalia-publica-por-error-el-numero-de-telefono-pablo-alboran-en-instagram_a_23357228/)

# El factor humano

Tweets

Fátima Báñez García @FatimaBanez  
¡Obtuve 5390 puntos en Bubble Shooter Adventures! ¿Puedes mejorararlo? ghh [goo.gl/S44Cb](http://goo.gl/S44Cb) [pic.twitter.com/P48LDY49](http://pic.twitter.com/P48LDY49)

 Ocultar aplicación    Responder    Retwittear    Favorito

desarrollado por  Photobucket    Reporta este archivo

# El factor humano

## Cosidó, pillado jugando en horas de trabajo

El SUP denuncia que el director general de la Policía se dedica a jugar por Internet mientras que los policías "tienen que ir a trabajar estando enfermos"

Estrella Digital, @Estrella\_digi. 12/06/2013 | 10:26 h.

0 comentarios



**Ignacio Cosidó** @Ignacos

He volado 170m en un juego repleto de acción de Jetpack Joyride.  
¡Supera eso! [bit.ly/rKuWqK](http://bit.ly/rKuWqK) [pic.twitter.com/EwuXWd2Sz3](http://pic.twitter.com/EwuXWd2Sz3)

View photo

6m

# El factor humano

EN ACTITUD CARIÑOSA

## Eduardo Casanova (Fidel en 'Aída') cuelga accidentalmente una imagen en internet practicando sexo con su novio

El actor aparece frente al espejo desnudo junto a su pareja. 26 Septiembre 2012.



Los peligros de la red se hacen más latentes para los famosos. [Eduardo Casanova](#) puede dar fe

<http://www.formulatv.com/noticias/27106/eduardo-casanova-fidel-aida-cuelga-accidentalmente-imagen-sexo-novio/>

# El factor humano

## El presidente de Nuevas Generaciones del PP en Huesca se burla de la violencia machista

■ José Luis Ferrando tuiteó una imagen en la que una joven narcotizada es amordazada y arrastrada por un hombre con el texto "¡he ligado!"

eldiario.es Seguir a @eldiariօs 61 comentarios

04/10/2013 - 18:59h Me gusta 12.17 Twitter 1.51

Tweet

J.L. Ferrando Castro @JL\_Ferrando Yujuuuuuuu pic.twitter.com/i6UgjxkndP

8:05 AM - 15 sep 13 desde Huesca, Huesca



# El factor humano

## CONSEJO DE SEGURIDAD EN EL USO DEL CORREO ELECTRÓNICO

Los problemas que hemos tenido este último mes para el envío de correos se deben a que algunos usuarios han facilitado su usuario y contraseña a spammers. Por ello, desde la vicegerencia TIC queremos hacer las siguientes aclaraciones:

1.- **NUNCA LE PEDIREMOS SU USUARIO Y CONTRASEÑA** por correo electrónico. **NUNCA**.

Por tanto, cualquier mensaje que reciba en el que se le solicite, no ha sido enviado por nosotros y por tanto debe usted tratarlo como una falsificación.

2.- **NUNCA DEBE ENVIAR SU USUARIO Y CONTRASEÑA POR CORREO ELECTRÓNICO**, ni a nosotros ni a otra persona. **NUNCA**. No es el medio indicado para hacer esto.

En caso de que los necesitemos para hacer alguna prueba, no se los pediremos por correo electrónico.

3.- Los mensajes que envía esta vicegerencia se suelen enviar en castellano y euskera, y en todo caso con una sintaxis correcta. Si recibe un mensaje con muy mala sintaxis, desconfíe de él.

4.- Ante la menor duda sobre un mensaje de este estilo, descártelo. Si necesita aclaraciones, póngase en contacto con el CAU y solicítelas, siempre antes de responder.

<http://www.ehu.es/correow>

# El factor humano

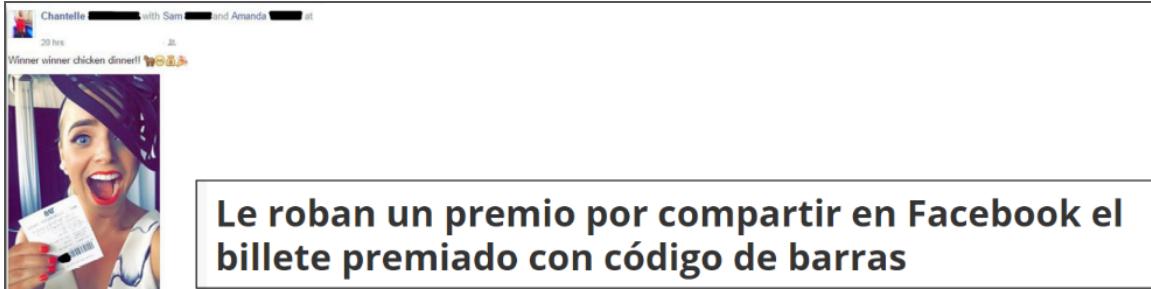
Un tuit racista provoca el despido fulminante de una directiva en pleno vuelo

Justine Sacco escribió "Me voy a África. Espero no pillar el sida. Es broma. ¡Soy blanca!" e inició una tormenta en Twitter que acabó con su carrera profesional

Tecnología | 23/12/2013 - 17:46h | Última actualización: 24/12/2013 - 17:48h

<http://www.lavanguardia.com/tecnologia/20131223/54397498289/un-tuit-racista-provoca-el-despido-fulminante-de-una-directiva-en-pleno-vuelo.html>

# El factor humano



A screenshot of a Facebook post by user Chantelle. The post shows a woman smiling and holding up a lottery ticket. The caption reads: "Winner winner chicken dinner!! 🎉🐔🎉". The post has 20 hrs since it was made and 2 likes.

**Le roban un premio por compartir en Facebook el billete premiado con código de barras**

[https://www.abc.es/recreo/abci-roban-todas-pertenencias-publicar-foto-facebook-201608081854\\_noticia.html](https://www.abc.es/recreo/abci-roban-todas-pertenencias-publicar-foto-facebook-201608081854_noticia.html)

# El factor humano

PIRATERÍA INFORMÁTICA ›

## Los altavoces inteligentes pueden recibir órdenes de terceros inaudibles para el usuario

El fallo es una puerta para que los 'hackers' puedan actuar sobre unos dispositivos que cada vez son más populares

[https://elpais.com/tecnologia/2018/05/11/actualidad/1526030082\\_845494.html](https://elpais.com/tecnologia/2018/05/11/actualidad/1526030082_845494.html)

# El factor humano

**Strava: cómo una aplicación de deportes dejó al descubierto secretos de bases militares de Estados Unidos**

Redacción  
BBC Mundo

© 29 enero 2018

f t e m Compartir



<https://www.bbc.com/mundo/noticias-42859883>

# El factor humano

Los usuarios también son parte del sistema

- También generan problemas de seguridad (Involuntarios o intencionados)
- Hay que tenerlos en cuenta en las políticas de seguridad
- Detrás del éxito de una gran parte de los ataques informáticos se encuentra un usuario “inocente”

# El factor humano

¿Cómo son los ataques intencionados?

- El 75% de las empresas temen represalias de ex empleados
- Robo de información
- Sabotaje

# El factor humano

¿Cómo se evitan los ataques intencionados?

- No siempre se puede, sobre todo a priori (¿Cómo distinguir si la intención es buena o mala?)
- Ante las dudas, auditorías

# El factor humano

Las empresas deberían

- Evaluar los riesgos
- Evaluar su exposición a los mismos
- Preparar una respuesta por si se producen

# El factor humano

A nivel preventivo

- Acceso limitado a los datos
- Medidas “extra” de seguridad para datos importantes

# El factor humano

¿Cómo se aprovechan del factor humano los hackers/crackers?

- Desconocimiento / Ignorancia
- Dejadez / Pereza
- Curiosidad / Ganas de saber / Ganas de lucrarse
- Comunicación / Ganas de darse a conocer
- Miedo
- Vergüenza / Desprestigio

# El factor humano

Desconocimiento / Ignorancia

- ¿Cómo se actualiza el sistema operativo?
- ¿Hay que actualizar las aplicaciones?
- Este mensaje de nueva versión de Java que aparece, ¿Qué hago?
- Mejor no toco nada no vaya a dejar de funcionar
- Total, ¿quién va a querer acceder a mi ordenador?
- ¿Necesitas mi password? Apunta, es ...

# El factor humano

Estimado Mikel:

Atendiendo a su solicitud para usuario en WebUntis, le comunico sus datos:

Usuario: [REDACTED]

Contraseña: [REDACTED]

Saludos cordiales,

[REDACTED]

Administratiboa

Administrativo

[REDACTED]



Bilboko Ingenieritzaz Eskola Escuela de Ingeniería de Bilbao  
Euskal Herriko Unibertsitatea Universidad del País Vasco

Plaza Ingeniero Torres Quevedo, 1. 48013 Bilbao

[www.ehu.eus](http://www.ehu.eus)



# El factor humano

Dejadez / Pereza

- De 3,4 millones de claves de 4 dígitos filtradas
- 11% de las claves eran 1234
- 6% de las claves eran 1111
- 2% de las claves eran 0000

# El factor humano

Dejadez / Pereza

- 100,000 passwords de trabajadores de Apple, Google, Nasa, etc. en el IEEE
- 271 trabajadores tenían 123456
- Más de 200 tenían ieee2012 (año de la filtración)
- Más de 200 tenían 12345678

# El factor humano

Dejadez / Pereza

- Cambiar el password cada 6 meses es muy pesado
- Memorizar un password seguro para cada aplicación es muy pesado
- Instalar 21 actualizaciones de Windows... uff! Con la prisa que tengo

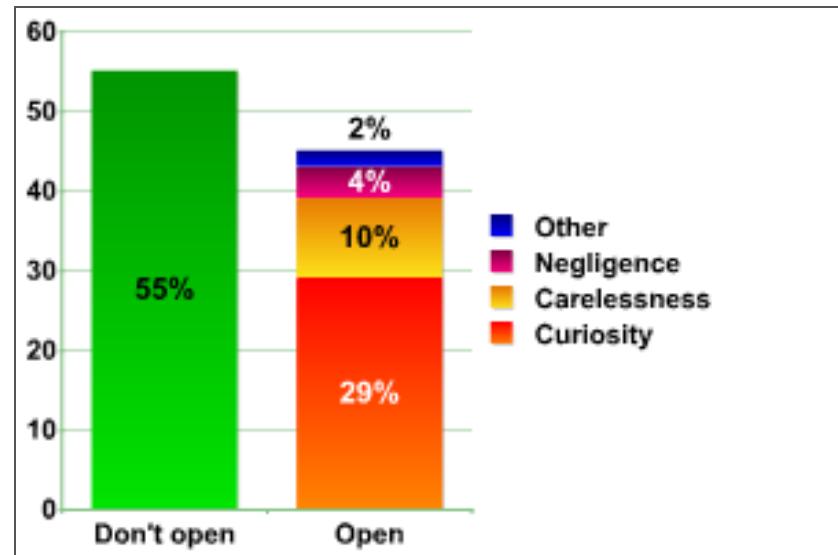
# El factor humano

Curiosidad / Ganas de saber / Ganas de lucrarse

- Mira la foto de la fiesta ...
- Han pillado a esta pareja en actitud cariñosa.. No te lo pierdas!!
- ¿Quieres un puesto de trabajo?
- Medicinas online
- Te ha tocado la lotería de Sudáfrica!!
- Tengo una herencia que no puedo cobrar, ¿lo haces tú y te llevas una comisión?

# El factor humano

Curiosidad / Ganas de saber: ¿Qué hacen los usuarios ante un correo no deseado?



# El factor humano

Comunicación / Ganas de darse a conocer: Típico en redes sociales

- Me voy de vacaciones!!
- Fotos, gustos, datos personales
- ¿Todos tus "amigos" / seguidores son amigos tuyos? ¿Les conoces personalmente? ¿Confías en ellos?
- ¿Quién tiene acceso a tu información?

# El factor humano

Vergüenza / Desprestigio

- Las personas no denuncian por vergüenza
- Las empresas no denuncian por desprestigio
- Consecuencia: Los timadores siguen lucrándose

# El factor humano

¿Cómo se aprovechan del factor humano los hackers/crackers? Ingeniería Social

- Obtener información confidencial a través de un usuario
  - De manera pasiva (sin interactuar con él)
  - A través de redes sociales
  - Seguimientos
- Se engaña al usuario para que proporcione información (técnicas activas)

# Ingeniería Social

La información obtenida de forma pasiva se puede utilizar para muchas cosas:

- Intentos de encontrar contraseñas: fechas/nombres significativos, aficiones, ...
- Para usarla luego en un ataque:
  - Correo fraudulento del banco
  - Conocimiento sobre el objetivo en general

# Ingeniería Social. Técnicas

Scam:

- Estafa a través de correo electrónico o páginas web
- Puede haber pérdida económica o no
- Hoax, phishing, spam, pharming

# Ingeniería Social. Técnicas

Hoax:

- Intento de hacer creer que algo falso es real
- No suelen tener consecuencias económicas
- Generan tráfico inútil y sobrecargan servidores
- Peligro: el cuento de Pedro y el lobo (Cuando algo sea real, el usuario no se lo creerá)
- Juegan con los miedos / buena intención de los usuarios

# Ingeniería Social. Técnicas

Hoax (Prevención):

- Suelen ser anónimos y no citan fuentes
- Contienen una petición de reenvío
- Pensar con lógica
- No reenviar / publicar aquello que no estamos completamente seguros que es real. En caso de duda, informarse

# Ingeniería Social. Técnicas

Phishing:

- Intento de lograr contraseñas o datos bancarios a través de un correo o una web que aparenta ser oficial
- Suele usarse en conjunto con el envío de SPAM
- El enlace muestra una cosa y redirige a otra
- URL muy parecida a la original: <http://www.kutzabank.es/>
- URL con mismo nombre, pero distinto dominio: <http://www.bankia.bz/>

# Ingeniería Social. Técnicas

Técnicas de Phishing:

- Cross Site Scripting (inyectar código malicioso en la página real)
- IDN Spoofing (vulnerabilidad en nombres de dominio internacionales por el uso de Unicode). Los navegadores actualizados no son vulnerables

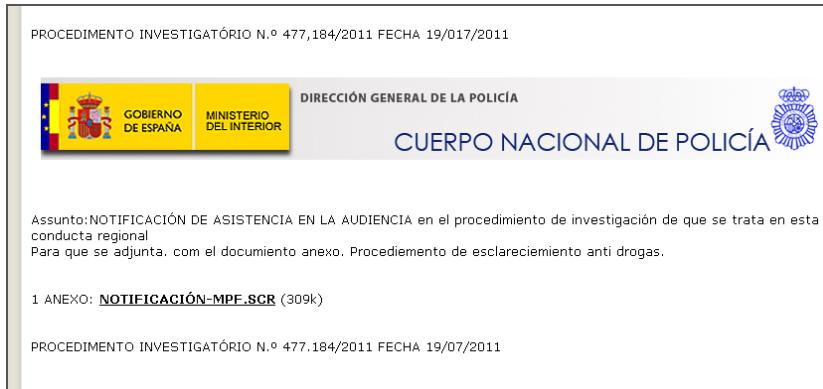
# Ingeniería Social. Técnicas

Phishing:

- Los ataques suelen ser masivos
- **Spear Phishing:** Ataques dirigidos a objetivos concretos

# Ingeniería Social. Técnicas

Correo con fichero adjunto que infecta el ordenador y "roba" información



# Ingeniería Social. Técnicas

Introduce tus datos para recibir la devolución de la Renta

 Agencia Tributaria

### Forma de Reembolso

Avisos:

1. Por favor, introduzca sus datos personales y una tarjeta de crédito válida a la que desea efectuar la devolución.
2. Todos los campos son obligatorios.

Nombre Completo:

Fecha de Nacimiento:  - Dia -  - Mes -  - Año -

Dirección:

Ciudad:

Código Postal:

Número de Tarjeta:

Fecha de Caducidad:  - Mes -  - Año -

Código de Seguridad:

Cantidad a devolver:  223.56 EUR

# Ingeniería Social. Técnicas

## Aplicaciones de redes sociales



# Ingeniería Social. Técnicas

Soluciones al Phishing:

- Nunca dar información confidencial por e-mail
- Teclear directamente la dirección, no pinchar un enlace
- Comprobar que la conexión esté cifrada (HTTPS)
- Comprobar los certificados

# Ingeniería Social. Técnicas

Soluciones al Phishing:

- Usar versiones actualizadas de los navegadores
- Usar un antivirus que analice las webs que se visitan
- Usar un servicio de análisis de URLs

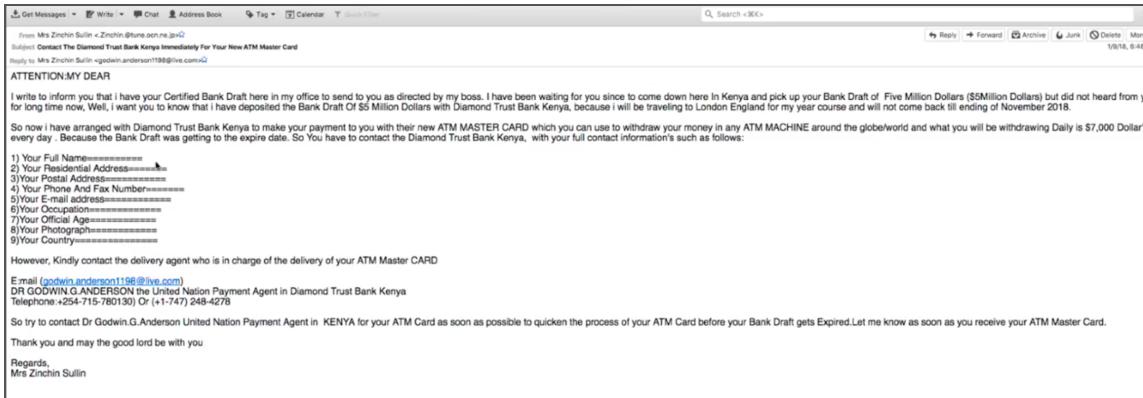
# Ingeniería Social. Técnicas

Timo nigeriano (estafa 419):

- Teclear directamente la dirección, no pinchar un enlace
- Se usa en conjunto con el SPAM
- Herencias, loterías, posibles parejas, ...

# Ingeniería Social. Técnicas

## Ejemplo variante timo nigeriano



# Ingeniería Social. Técnicas

## Ejemplo variante timo nigeriano

The screenshot shows an email inbox interface with various menu options at the top: Get Messages, Write, Chat, Address Book, Tag, Calendar, and Quick Filter. Below the menu, an incoming email is displayed:

**From:** Mrs.Melania Trump <WWW@festa.ocn.ne.jp>  
**Subject:** First notice from Mrs.Melania Trump.  
**Reply to:** Mrs.Melania Trump <melaniatrump777@gmail.com>

**First notice from Mrs.Melania Trump.**  
I am Mrs Melania Trump and I am written to inform you about your Bank Check Draft brought by United Embassy from the government of Benin Republic to the white house Washington DC and has been mandated to be deliver to your home address,as soon as you get back to me with your below information.

1.Full Names :  
2.Residential Address :  
3.Mobile Number:  
4.Fax Number :  
5.Occupation :  
6.Sex :  
7.Age :  
8.Nationality :  
9.Country :  
10.Marital Status :

Your check is containing the sum of \$25 million USD.  
Here is my email or send me an sms,+1(407) 990-1723 but i prefer sms because ill always busy in the white house and i cant be able to

# Ingeniería Social. Técnicas

Soluciones al timo nigeriano:

- Pensar antes de actuar
  - Nadie regala dinero
  - Si no se juega a la lotería, es imposible que toque
- No dar información confidencial a desconocidos

# Ingeniería Social. Técnicas

## Herencias

Estimado amigo,

Soy Emmanuel Egobiawa, un abogado en derecho y abogado personal para fines Ingeniero S. García, que murió con su esposa y su único hijo en un accidente de coche espantoso en el día 13 de diciembre de 2008, que utilizan para trabajar en la Compañía de Desarrollo de Shell y También era un contratista del gobierno aquí en Lomé. Deseo llamar su atención para informarle que Engr tarde. S. García antes de su muerte dejó a la suma de dieciocho millones de dólares (EE.UU. \$ 18,000,000, 00) solo en su cuenta bancaria que quiero poner en su atención ahora. Él murió sin dejar ninguno de sus familiares la información a mí o a cualquier otra persona y tengo mis mejores tratar de localizar a sus parientes o familiares, incluso en la embajada de su país, pero sin ningún éxito. Ahora bien, como su abogado personal y por la ley y el orden, el banco me pedirá que proporcione a sus familiares o parientes más cercanos a este hombre para que el fondo / el dinero se traslado a su familia que no tienen.

Ahora ya no tiene ningún miembro de la familia o parientes como (familiares hermano, hermana, tío o familiar), y tener / respuesta el mismo apellido (García) con él, quiero y han decidido a presentar al banco como uno de sus miembros de la familia o pariente más cercano a él por lo tanto ponerse en contacto con usted para que el banco va a transferir este dinero / fondos en su cuenta. Después de recibir este fondo / dinero en su cuenta en su país, voy a venir a su país a efectos de compartir y de la inversión porque parte de este fondo / el dinero se debe utilizar para la Fundación del Orfanato y otras inversiones como la construcción de una buena Estate en su país que se nos está dando otro fondo adicional / dinero. Pero esto no se puede lograr sin un socio extranjero como a ayudar a mí llevar a cabo esta operación, y que es por eso que estoy en contacto con usted hoy en día para que me ayude en este tema. Tengo los documentos necesario para que nos ayude en la toma de este éxito.

# Ingeniería Social. Técnicas

## Loterías



The National Lottery®

Premio Asegurado

PO Box 251 Watford WD18 9BR  
Inglaterra.

24<sup>th</sup> junio 2011.

Desde: International Award Dept.  
Reference Number: WB/2011/0018  
Batch Number: BC-00067/5808

Attention: Beneficiario

PREMIO ASEGURADO

Tenemos el immense placer de informarle hoy día 08 de Abril 2011, el resultado de las promociones de loterías "UK NATIONAL LOTTERY". llevado a cabo el dia 22 de Abril 2011.

Su nombre con su email ha sido premiado adjunto al boleto: 026-9-2 con número de serie: 7-8 mostró el número afortunado De Remesa: 1-8-3. En consecuencia, ganador de la lotería en tercera categoría. Por lo tanto, a usted le ha correspondido un premio de €915.000,00 euros (NOVECIENTOS QUINCE MIL EUROS) en efectivo. El número de referencia de archivo para reclamar su premio es: GTC1/2551256003/09. El premio total en efectivo es €19.733.910 euros (DIECINUEVE MILLONES SETECIENTOS TREINTA Y TRES MIL NOVECIENTOS DIEZ EUROS). Compartido entre varios ganadores a diferente escala internacional en esta categoría 3. Felicitaciones!

Todos los participantes han sido seleccionados a través de un sistema informático, llevado a cabo anualmente. En este momento, su dinero se encuentra depositado en una cuenta provisoria a su nombre, bajo un seguro que nuestra empresa ha puesto a su dinero para tenerlo asegurado. Para mayor seguridad, le pedimos que guarde bien esta documentación, ya que aquí figura su número de referencia y cualquier persona que posea estos datos podría reclamar el dinero en su nombre.

Para comenzar su demanda, debe ponerse en contacto con el número de teléfono que aquí le indicamos, y su agente le informara el procedimiento para el cobro correspondiente a su dinero. Teléfono: +44 [REDACTED] Email: [REDACTED]@in.com FIRST SECURITY COMPANY LTD Persona responsable de asesoramiento: ALAMS DOUGLAS. Horario comercial: Lunes a Viernes de 10 a 14 hs y de 17 a 20 hs. NOTA: Todo premio debe ser reclamado antes de 26 de Julio de 2011. Despues de esta fecha, los fondos serán devueltos al MINISTERIO DE ECONOMIA Y HACIENDA como no reclamado.

RELLENE EL FORMULARIO Y ENVIARLO POR E-MAIL AL TU AGENCIAS JUNTO CON TU PHOTOCOPIA DE TU DNI EMAIL: [REDACTED]@IN.COM

# Ingeniería Social. Técnicas

## Trabajo (Muchas veces ilegal)

Asunto: Trabajar en casa, pago semanal de 1.768 euros por semana.

Bienvenida.

Aumentamos nuestra dependencia y necesitamos le..

Si no esta satisfecho con sus ingresos- aprovechar la oportunidad para convertirse en remoto te propuesto nuestro corporacion y cobrar de 10 a 30 euros por hora en la Internet.

Todo lo que necesita- posesion nivel de usuario de PC, disponibilidad y una demanda enviada,  
que contengan datos de nombre completo, edad y lugar de residencia.

Encuesta que desea expulsar aqui [www@west-ug.org](mailto:www@west-ug.org)

Ya un par de horas. Le enviaremos una carta en respuesta con explicaciones de la obra detalladas.

Solo esperamos de usted responsabilidad y el deseo para ganar. Y ningunos costes iniciales!

# Ingeniería Social. Técnicas

## Regalos



# Ingeniería Social. Técnicas

Para detectar SPAM, revisar la cabecera:

- From -- el remitente
- To -- El destinatario
- Subject -- El asunto del mail
- Date -- La fecha de envío
- **Received** -- Indica en cada línea por qué servidores ha pasado (en orden inverso) -- Se puede usar el Servicio [Whois](#)

# DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) es un estándar que autentica el dominio del remitente de correos electrónicos, para que tanto los remitentes como los destinatarios puedan verificar los mensajes entrantes

Se definen las medidas que deben aplicarse a los mensajes sospechosos que se reciban

# DMARC

Comprobaciones de DMARC:

- Los mensajes entrantes deben estar autenticados por SPF, DKIM o ambos
- El dominio autenticado debe concordar con el que figura en la dirección del encabezado "De:" del mensaje

# Spoofing de correo electrónico

- Spoofing (suplantación): cambiar el contenido de un mensaje, para que parezca que proviene de una fuente que no es la real
- Los spammers pueden enviar correos electrónicos de modo que parezca que proceden de tu dominio

# DKIM (Domain Keys Identified MaiL)

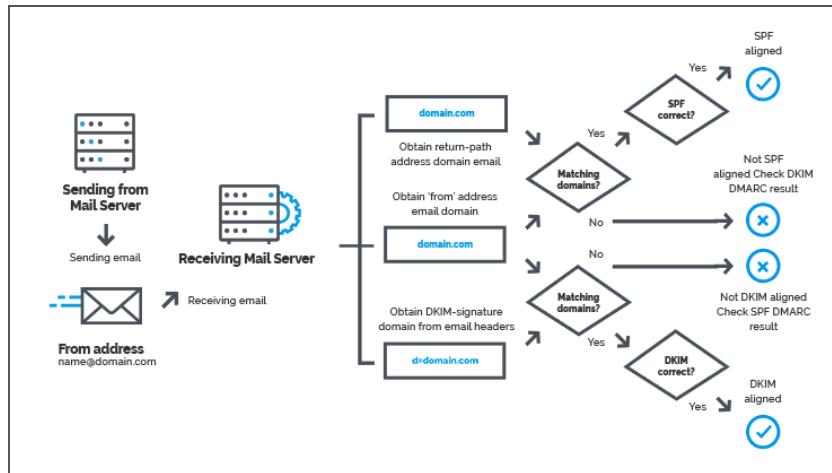
- DKIM previene más fácilmente el spoofing en los mensajes salientes que se envíen desde tu dominio
- DKIM incluye una firma cifrada en el encabezado de todos los mensajes salientes: Los servidores de correo electrónico que los reciben descifran su encabezado mediante DKIM y verifican que no se haya modificado tras el envío

# SPF (Sender Policy Framework)

- Protegerse frente a correos falsificados que parecen proceder de tu dominio

# DMARC

Google, Facebook, Microsoft, etc. están bloqueando el phishing y ataques de spam con DMARC



# Ejemplo real Media Markt

Gmail lo clasifica como spam

The screenshot shows an email from MediaMarkt in the inbox. The subject line is: "Y para el fin de semana... ACER y ROWENTA ¡2ª unidad de la misma marca al -50%! + solo hasta el 26/10 LG, XIAOMI, OPPO, VSMART y ORAL B". A "Spam" button is visible next to the message. Below the message, there's a warning box with an exclamation mark asking: "¿Por qué está en Spam este mensaje? Se parece a otros mensajes que se han anteriormente." It includes a "No es spam" button. At the bottom, there are language options: "inglés" and "español", and a "Traducir mensaje" link. A red banner at the bottom of the email body says: "¡2ª unidad al 50% de la misma marca!". Below the email, there's a link: "Haz click aquí si no puedes visualizar correctamente esta Newsletter". At the very bottom, there are links for "Contacto", "Social Media", and "Formas de pago". A context menu is open over the email, showing options: "Responder", "Reenviar", "Filtrar mensajes como este", "Imprimir", "Eliminar este mensaje", "Bloquear a MediaMarkt", "Denunciar suplantación de identidad", "Mostrar original" (which is highlighted in grey), "Descargar mensaje", and "Marcar como no leído".

# Ejemplo real Media Markt

## MX ToolBox Email Head Analyzer

**Header Analyzed**  
 Email Subject: 📌 Y para el fin de semana... ACER y ROWENTA 📌 | 2ª unidad de la misma marca al -50%! + solo hasta el 26/10 LG, XIAOMI, OPPO, VSMART y ORAL B

**Delivery Information**

- > DMARC Compliant
- > SPF Alignment
- > DKIM Unauthenticated
- > DKIM Authenticated

**Relay Information**

Received	Delay
923 seconds	

From uspmta194148.emarsys.net to mx.google.com  


Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	.	uspmta194148.emarsys.net 217.175.194.148	mx.google.com	ESMTPS	10/25/2019 10:08:54 PM	●
2	0 seconds		2002:a2e:9c12:0:0:0:0	SMTP	10/25/2019 10:08:54 PM	
3	15 minutes		2002:a92:6c09::	POP3	10/25/2019 10:24:16 PM	
4	1 Second		2002:a05:6214:8f:0:0:0	SMTP	10/25/2019 10:24:17 PM	

**SPF and DKIM Information**

# Black list

blacklist:217.175.194.148 [Monitor This](#) [Solve Email Delivery Problems](#) [blacklist](#)

! We notice you are on a blacklist. [Click here for some suggestions](#)

Checking 217.175.194.148 against 99 known blacklists...  
Listed 2 times with 3 timeouts

	Blacklist	Reason	TTL	ResponseTime	
<span>✗</span> LISTED	SORBS SPAM	217.175.194.148 was listed <a href="#">Detail</a>	3600	0	<a href="#">Ignore</a>
<span>✗</span> LISTED	UCEPROTECTL2	217.175.194.148 was listed <a href="#">Detail</a>	2100	0	<a href="#">Ignore</a>
<span>✓</span> OK	0SPAM			0	
<span>✓</span> OK	Abuse.ro			142	
<span>✓</span> OK	Abusix Mail Intelligence Blacklist			0	

# Black list

**SORBS** (Spam and Open Relay Blocking System) proporciona acceso a la lista negra antispam

**UCEPROTECTL2** (Unsolicited Commercial E-mail). Las listas negras (mala reputación) basadas en spam son aquellas que enumeran direcciones IP individuales o rangos completos, del que se han recibido spam. Por ejemplo, correo electrónico masivo no solicitado

# Ingeniería Social. Pharming

Redireccionar el tráfico de una web legítima a otra falsa

- Atacando el servidor DNS
- Atacando el fichero hosts en local

Peligroso porque el usuario ha introducido correctamente la URL: El redireccionamiento es “invisible”. Prevención:

- Si el aspecto de la web es diferente, sospechar
- Comprobar certificados

# Ingeniería Social

La única forma de luchar contra la Ingeniería Social

- Educación de los usuarios
- Implementación de políticas de seguridad que realmente se sigan

Cuanta más información nuestra tengan los timadores, más fácil será que nos engañen

# Casos reales. El director general chulito

Auditoría de seguridad para una compañía

El director general alardea de su seguridad

El consultor descubre los donativos a instituciones de lucha contra el cáncer

# Casos reales. El director general chulito

A través de Facebook se descubre el restaurante y el equipo deportivo favoritos del director general

Llama al director general haciéndose pasar por una de las asociaciones de lucha contra el cáncer con las que colabora habitualmente

A cambio de la donación entra en sorteos de cenas en su restaurante favorito y entradas para su equipo favorito

El director general accede a recibir más información por correo electrónico

# Casos reales. El director general chulito

Para asegurarse que no va a haber problemas al abrir el fichero, se le pregunta al director qué versión de Adobe Reader usa

Se le envía un fichero .pdf con código malicioso para esa versión concreta

Se consigue acceso total al ordenador del director general y desde ahí a toda la empresa

# Casos reales. El parque temático

Contratan a una consultora para analizar la seguridad de sus sistema de venta de entradas

El consultor llamó al parque temático haciéndose pasar por vendedor de software

Tras hablar un rato con los empleados obtuvo la información de qué versión de Adobe Reader se usaba en el parque

# Casos reales. El parque temático

El consultor se presenta en el parque simulando una familia (con niños)

Pide acceso a un ordenador para poder imprimir las entradas que tiene en el correo electrónico

La empleada le permite el acceso (a pesar de tenerlo prohibido)

# Casos reales. El parque temático

Al abrir el archivo .pdf con las entradas, se instala un software malicioso que permite controlar el ordenador

Desde ese ordenador se accede a los servidores de la empresa