

# Giza faktorea

Mikel Egaña Aranguren

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

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



# Giza faktorea

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

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



# Giza faktorea

“

*Azkenean, segurtasun-sistema bat bere kate-begi ahulena bezain eraginkorra da.*

*Online segurtasunaren kasuan, kate-maila ahulena giza faktorea da beti.*

**Eugene Kaspersky**

# Giza faktorea

“

*Teknologiarik onena izan dezakezu, firewall-ak, IPS-ak, gailu biometrikoak, eta abar. Behar duzun bakarra langile bati ustekabeen deitzea da eta sisteman besterik gabe sartzen zara.*

**Kevin Mitnick**

# Giza faktorea

Kevin Mitnick, 90eko hamarkadan, FBIk gehien bilatzen zuen

Cyberkriminaltzat jo zuten

Ingeniaritza sozialeko bere lehen erasoetako batean azaltzen zuen nola,  
eskataile zenbaki soil batekin Ibilgailu Motordunen Departamentuak (DMV)  
sartu ahal zen

# Giza faktorea

Hori lortzeko komisaria batera deitu eta DMVko norbaiten itxura hartu zuen.

"Zure eskatzaile-kodea 36472 da?". Agenteak erantzun zuen: "Ez, 62883 da".

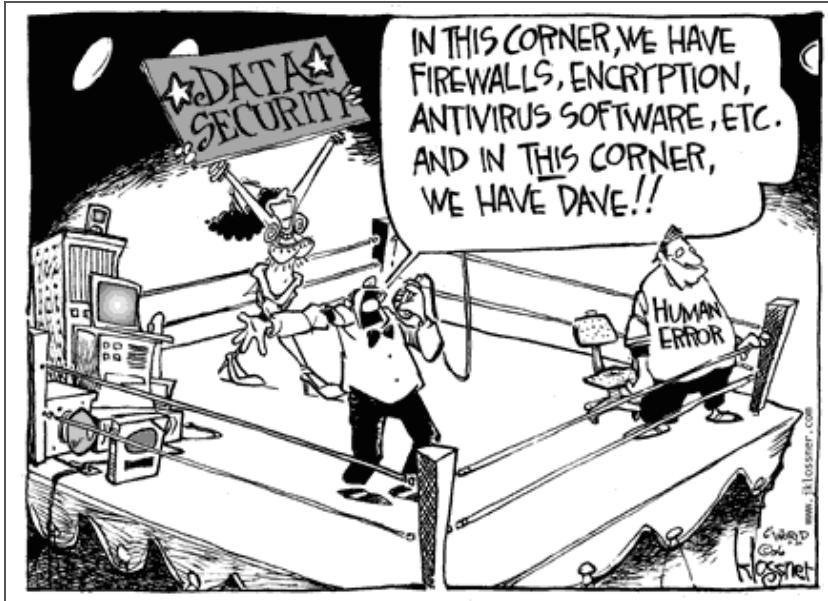
*Oso maiz funzionatzen duen trikimailu bat da. Informazio konfidentziala  
eskatzen baduzu, jendeak berehala susmatzen du*

# Giza faktorea

*Informazio hori baduzulako itxurak egiten badituzu eta gaizki dagoen zerbait esaten baduzu, jendeak zuzentzen dizu eta bilatzen ari zinen informazioa eman*

*Ingeniaritza sozialaren oinarrizko printzipo hori funtsezko beste batekin lotzen zen: jendea segurtasun-kate baten katebegi ahulena izaten da, zeren "jendeak beti dauka laguntzeko asmo hori"*

# Giza faktorea



# Giza faktorea

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 funcionarios.

El próximo director de Discursos de la Casa Blanca, el asesor Jon Favreau (derecha) aparece junto a una figura de Hillary Clinton.



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

# Giza faktorea

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...

# Giza faktorea

**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/)

# Giza faktorea

**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

# Giza faktorea

## 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

# Giza faktorea

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/>

# Giza faktorea

## 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

Tweet 12.17 Twitter 1.51

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

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



¡HE LIGADO!

# Giza faktorea

## 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.

# Giza faktorea

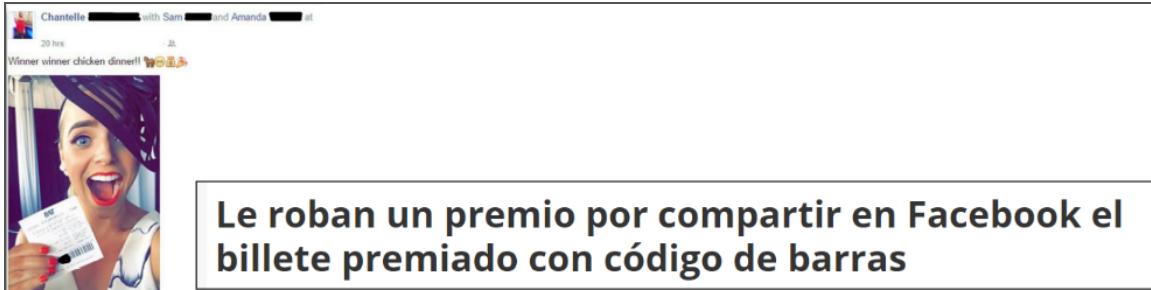
## Un tuit racista provoca el despido fulminante de una directiva en pleno vuelo

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>

# Giza faktorea



Chantelle [REDACTED] with Sam [REDACTED] and Amanda [REDACTED] at [REDACTED]  
20 hrs · [REDACTED]  
Winner winner chicken dinner!! 🍗🍗🍗

**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)

# Giza faktorea

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)

# Giza faktorea

**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>

# Giza faktorea

Erabiltzaileak ere sistemaren parte dira

- Segurtasun-arazoak sortzen dituzte ere, nahita edo nahigabe
- Segurtasun-politiketan kontuan hartu behar dira
- Eraso informatiko askoren atzean erabiltzaile "errugabe" bat dago

# Giza faktorea

Nolakoak dira nahita egindako erasoak?

- Enpresen % 75 langile ohien errepresalien beldur dira
  - Informazioa lapurtzea
  - Sabotaiak

# Giza faktorea

Nola ekidin nahita egindako erasoak?

- Ezin da beti, batez ere a priori (Nola bereizi asmoa ona edo txarra den?)
- Zalantzen aurrean, auditoriak

# Giza faktorea

Enpresek egin behar dute:

- Arriskuak ebaluatu
- Horiekiko esposizioa ebaluatu
- Erantzun bat prestatu

# Giza faktorea

Prebentzioari dagokionez

- Datuetarako sarbide mugatua
- Neurri bereziak datu garrantzitsuetarako

# Giza faktorea

Nola aprobetxatzen dira hacker/crackerrak Giza faktoreaz?

- Ezjakintasuna
- Utzikeria
- Kuriositatea / irabazteko nahia
- Komunikazioa / ezagun bihurtu
- Beldurra
- Lotsa

# Giza faktorea

## Ezjakintasuna

- Nola eguneratzen da sistema eragilea?
- Aplikazioak eguneratu behar dira?
- Agertzen den Javaren bertsio berriaren mezua, zer egin behar dut?
- Hobe dut ezer ez ukitzea
- Nortzuek nahi izango dute nire ordenadorean sartu?
- Nire pasahitzta behar duzu? Apuntatu

# Giza faktorea

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)



# Giza faktorea

## Utzikeria

- 3,4 milioi pasahitz filtratutik
  - 11% 1234
  - 6% 1111
  - 2% 0000

# Giza faktorea

## Utzikeria

- Apple, Google, Nasa, etabarreko langileen 100,000 pasahitz
  - 271 langilek 123456
  - 200 baino gehiagok ieee2012
  - 200 baino gehiagok 12345678

# Giza faktorea

## Utzikeria

- Pasahitza 6 hilean behin aldatzea oso astuna da
- Pasahitz seguru bat aplikazio bakoitzerako gogoratzea oso astuna
- Windows-en 21 egunератзе instalatzea ... uff!

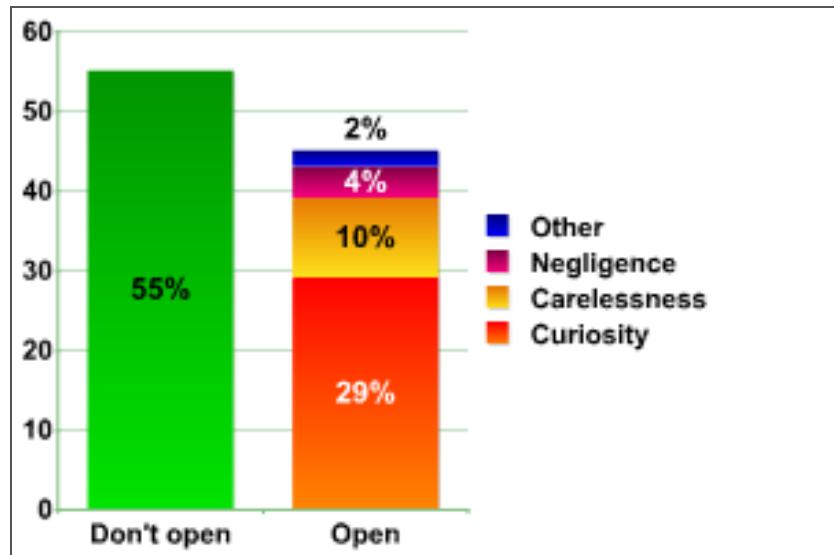
# Giza faktorea

Kuriositatea / irabazteko nahia

- Begiratu jaiaren argazkia ...
- Bikote hau larrutan harrapatu dute!
- Lanpostu bat nahi duzu?
- Online sendagaiak
- Hegoafrikako loteria tokatu zaizu!
- Kobra tu ezin dudan herentzia bat daukat, zerorrek egin eta komisio bat eraman

# Giza faktorea

Kuriositatea / irabazteko nahia: Zer egiten dute erabiltzaileek nahi ez duten mezu elektroniko baten aurrean?



# Giza faktorea

Kuriositatea / irabazteko nahia: Ohikoa sare sozialetan

- Oporretan noa!!
- Argazkiak, gustuak, datu pertsonalak
- Zure "lagun"/jarraitzaile guztiak zure lagunak dira? Pertsonalki ezagutzen dituzu? Fidatzen zara haiekin?
- Nork eskura dezake zure informazioa?

# Giza faktorea

Lotsa

- Pertsonek ez dute salatzen lotsagatik
- Enpresek ez dute salaketarik jartzen izen ona ez galtzeko
- Ondorioa: iruzurgileek irabaziak izaten jarraitzen dute

# Giza faktorea

Nola aprobetxatzen dira hacker/crackerrak Giza faktoreaz? Ingeniaritza soziala

- Erabiltzaile baten bidez isilpeko informazioa lortzea
  - Modu pasiboan (harekin elkarreragin gabe)
  - Sare sozialen bidez
  - Jarraitzea
- Erabiltzailea engainatzen da informazioa eman dezan (teknika aktiboak)

# Ingenieritzako soziala

Modu pasiboan lortutako informazioa gauza askotarako erabil daiteke:

- Pasahitzak aurkitzeko ahaleginak: datak/izen esanguratsuak, zaletasunak,...
- Gero eraso batean erabiltzeko:
  - Bankuaren iruzurrezko posta
  - Helburuari buruzko ezagutza, oro har

# Ingenieritzas soziala. Teknikak

Scam:

- Posta elektronikoaren edo webguneen bidezko iruzurra
- Galera ekonomikoa egon daiteke edo ez
- Hoax, phishing, spam, pharming

# Ingenieritzia soziala. Teknikak

Hoax:

- Gauza faltsu bat benetakoa dela sinestarazten saiatzea
- Ez dute ondorio ekonomikorik izaten
- Alferreko trafikoa sortzea eta zerbitzuak gain-kargatzea
- Arriskua: zerbait erreala denean, erabiltzaileak ez du sinetsiko
- Erabiltzaileen beldurrekin/asmo onarekin jolasten dute

# Ingenieritzia soziala. Teknikak

Hoax (Prebentzioa):

- Anonimoak dira eta ez dute iturriak aipatzen
- Birbidalketa-eskaera dute
- Logikaz pentsatzea
- Ez birbidali / argitaratu erabat ziur ez dagoena benetakoa dela. Zalantzarik badago, ondo informatu

# Ingenieritzasoziala. Teknikak

Phishing:

- Pasahitzak edo banku-datuak lortu ofiziala dirudien posta edo webgune baten bidez
- SPAM bidalketarekin batera erabiltzen da
- Loturak gauza bat erakusten du baina beste batera birbideratzen du
- Jatorrizkoaren oso antzeko URLa: <http://www.kutzabank.es/>
- URLa izen berarekin, baina domeinu desberdinarekin: <http://www.bankia.bz/>

# Ingenieritzasun soziala. Teknikak

Phishing:

- Erasoak masiboak izaten dira
- **Spear Phishing:** helburu zehatzetara bideratutako erasoak

# Ingenieritzasoziala. Teknikak

Ordenagailua infektatu eta informazioa "lapurtzen" duen erantsitako fitxategia duen emaila

PROCEDIMIENTO INVESTIGATÓRIO N.º 477.184/2011 FECHA 19/07/2011

 GOBIERNO  
DE ESPAÑA  MINISTERIO  
DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA  CUERPO NACIONAL DE POLICÍA

Assunto: NOTIFICACIÓN DE ASISTENCIA EN LA AUDIENCIA en el procedimiento de investigación de que se trata en esta conducta regional  
Para que se adjunta, con el documento anexo. Procedimiento de esclarecimiento anti drogas.

1 ANEXO: [NOTIFICACIÓN-MPF.SCR](#) (309k)

PROCEDIMIENTO INVESTIGATÓRIO N.º 477.184/2011 FECHA 19/07/2011

# Ingenieritzas soziala. Teknikak

## Sartu zure datuak Errentaren itzulketa jasotzeko

 Agencia Tributaria

**Forma de Reembolso**

**Avisos:**

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

Nombre Completo: \_\_\_\_\_  
Fecha de Nacimiento:  -  -   
Dirección: \_\_\_\_\_  
Ciudad: \_\_\_\_\_  
Código Postal: \_\_\_\_\_  
Número de Tarjeta: \_\_\_\_\_  
Fecha de Caducidad:  -   
Código de Seguridad: \_\_\_\_\_  
Cantidad a devolver:  EUR

# Ingenieritzia soziala. Teknikak

## Sare sozialetako aplikazioak



# Ingenieritzako soziala. Teknikak

Phishing-a ekiditeko:

- Ez eman inoiz informazio pribaturik e-mail bidez
- Helbidea zuzenean tekleatu, lotura bat ez klikatu
- Konexioa zifratuta dagoela egiaztatzea (HTTPS)
- Ziurtagiriak egiaztatzea

# Ingenieritzasoziala. Teknikak

Phishing-a ekiditeko:

- Nabigatzaileen bertsio eguneraatuak erabiltzea
- Antibirus bat erabili webguneak analizatzeko (<https://www.virustotal.com/>)
- URLak aztertzeko zerbitzu bat erabiltzea

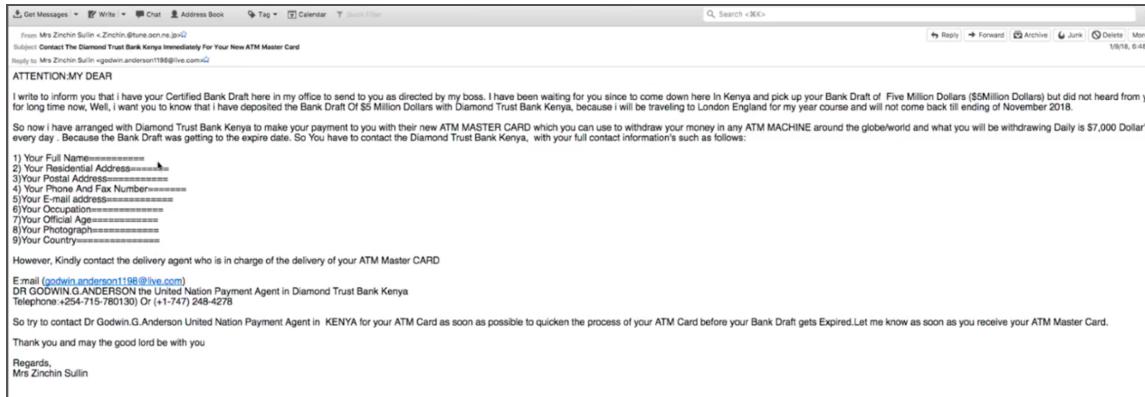
# Ingenieritzas soziala. Teknikak

Nigeriako iruzurra (419 iruzurra):

- SPAM sistemarekin batera erabiltzen da
- Herentziak, loteriak, bikoteak...

# Ingenieritzia soziala. Teknikak

## Nigeriako iruzurraren aldaera



# Ingenieritzia soziala. Teknikak

## Nigeriako iruzurraren aldaera

The screenshot shows an email inbox interface with several menu options at the top: Get Messages, Write, Chat, Address Book, Tag, Calendar, and Quick Filter. Below the menu, there is an incoming email from "Mrs. Melania Trump <WWW@festa.ocn.ne.jp>" with the subject "First notice from Mrs. Melania Trump." The email body contains a scam message. It starts with "First notice from Mrs.Melania Trump." followed by a paragraph about a bank check draft from the Benin Republic to the White House in Washington DC. It then lists ten items for personal information, numbered 1 through 10. At the bottom, it says "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 I'm always busy in the white house and i can't be able to

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 I'm always busy in the white house and i can't be able to

# Ingenieritzako soziala. Teknikak

Nigeriako iruzurraren kontra:

- Pentsatu egin aurretik
  - Inork ez du dirurik oparitzen
  - Loterian jokatzen ez bada, ezinezkoa da tokatzea
- Ezezagunei isilpeko informaziorik ez ematea

# Ingenieritzas soziala. Teknikak

## Herentziak

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) sólo 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.

# Ingenieritzas soziala. Teknikak

## Loteriak



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 immenseo 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]@firstsecurity.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]@firstsecurity.com

# Ingenieritzas soziala. Teknikak

## Lana (Askotan 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-uq.org](mailto:www@west-uq.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!

# Ingenieritzia soziala. Teknikak

## Opariak



# Ingenieritzia soziala. Teknikak

SPAM detektatzeko, goiburua berrikusi:

- From -- bidaltzailea
- To -- Hartzailea
- Subject -- eMailaren gaia
- Date -- Bidaltzeko data
- **Received** -- Lerro bakoitzean zein zerbitzarirengatik igaro den alderantzizko ordenan -- [Whois](#) zerbitzua erabiltzea dago

# DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) estandarra, posta elektronikoen igorlearren domeinua autentizatzen du, bai bidaltzaileek bai hartzaileek sartzen diren mezuak egiaztatu ahal izateko

Jasotzen diren mezu susmagarriei aplikatu beharreko neurriak definitzen dira

# DMARC

DMARC konprobazioak:

- Sartzen diren mezuak SPF, DKIM edo bien bidez kautotuta egon behar dira
- Autentifikatutako domeinuak bat etorri behar du mezuaren "from" goiburuko helbidean agertzen denarekin

# Posta elektronikoaren spoofing-a

- Spoofing (ordezpena): mezu baten edukia aldatzea, benetakoak ez den jatorri batetik datorrela eman dezan
- Spammer-ek mezu elektronikoak bidal ditzakete, zure domeinutik datozena emateko moduan

# DKIM (Domain Keys Identified Mail)

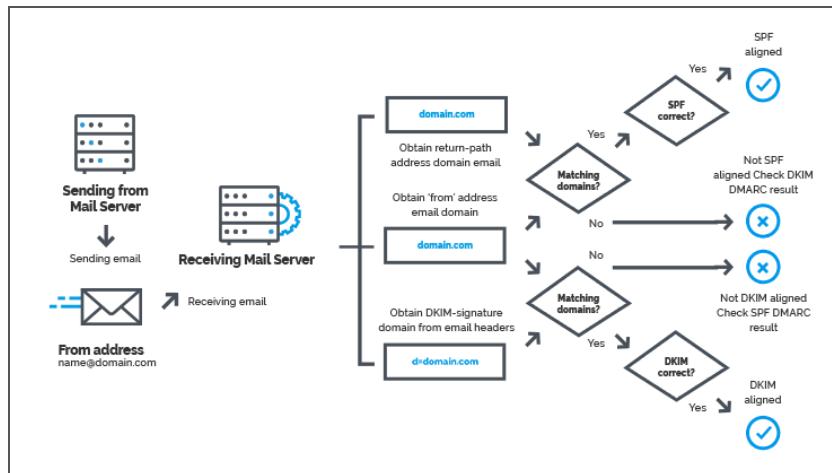
- DKIMek spoofinga errazago prebenitzen du zure domeinutik bidaltzen diren mezuetan (Irteten diren mezuetan)
- DKIMek sinadura zifratu bat du irteten diren mezu guztien goiburuan: mezu horiek jasotzen dituzten posta elektronikoko zerbitzariek DKIM bidez deszifratzen dute goiburua, eta egiaztatu egiten dute bidalketaren ondoren ez dela aldatu

# SPF (Sender Policy Framework)

- Zure domeinutik datozena diruditen posta faltsutuen aurrean babestea

# DMARC

Google, Facebook, Microsoft, etabarrek phishing eta SPAM erasoak saihesten dituzte DMARC erabiliz



# Media Markt adibidea

Gmail-ek SPAM dela dio

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 Spam

MediaMarkt <newsletter@news.mediamarkt.es>

para aserna ▾

¿Por qué está en Spam este mensaje? Se parece a otros mensajes que se han anterioriamente.

No es spam

sáb., 26 oct. 0:08

- Responder
- Reenviar
- Filtrar mensajes como este
- Imprimir
- Eliminar este mensaje
- Bloquear a MediaMarkt
- Denunciar suplantación de identidad
- Mostrar original**
- Descargar mensaje
- Marcar como no leído

inglés ▾ > español ▾ Traducir mensaje

**¡2ª unidad al 50% de la misma marca!**

Haz click aquí si no puedes visualizar correctamente esta Newsletter

Contacto Social Media Formas de pago [Descarga la app](#)

# Media Markt adibidea

## 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 Alignment
- > DKIM Authenticated

**Relay Information**

Received	923 seconds
Delay:	

From uspmta194148.emarsys.net to the 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) Antispam zerrenda beltzerako sarbidea ematen du

**UCEPROTECTL2** (Unsolicited Commercial E-mail). Spamean oinarritutako zerrenda beltzak (ospe txarra) banakako IP helbideak edo IP talde osoak zerrendatzen dituztenak dira, eta bertatik spama jaso da

# Ingenieritzia soziala. Pharming

Webgune zilegi batetik gezurrezko beste batera bideratzea trafikoa

- DNS zerbitzariari erasotzen
- Hosts fitxategia lokalean erasotuz

Arriskutsua, erabiltzaileak URLa behar bezala sartu duelako: birbideratzea ikusezina da. Prebentzia:

- Webaren itxura desberdina bada, susmatu
- Ziurtagiriak egiaztatzea

# Ingenieritzasoziala

Ingeniaritzasozialaren aurka borrokatzeko modu bakarra

- Erabiltzaileen hezkuntza
- Benetan jarraitzen diren segurtasun-politikak ezartzea

Iruzurgileek zenbat eta informazio gehiago izan, errazago engainatuko gaituzte

# Benetazko kasuak. Zuzendari harroputza

Konpainia baterako segurtasun-auditoria

Zuzendari nagusia bere segurtasunaz harrotzen da

Kontsultoreak konpainiak minbiziaaren kontrako erakundeei emandako  
dohaintzak aurkitzen ditu

# Benetazko kasuak. Zuzendari harroputza

Facebooken bidez, zuzendariaren jatetxea eta kirol-talde gogokoenak

Zuzendariari deitu, minbiziaren aurkako borrokan normalean laguntzen duen  
elkartetako baten itxura hartuz

Dohaintzaren truke, zozketetan sartzen da, jatetxean afaltzeko eta taldearen  
partiduetarako

Zuzendariak informazio gehiago jaso nahi du posta elektronikoz

# Benetazko kasuak. Zuzendari harroputza

Fitxategia irekitzean arazorik egongo ez dela ziurtatzeko, zuzendariari galdezen zaio Adobe Readerren zer bertsio erabiltzen duen

Kode maltzurra duen .pdf fitxategi bat bidaltzen zaio bertsio zehatz horretarako

Zuzendariaren ordenagailurako sarbidea lortzen da, eta hortik enpresa osora

# Benetazko kasuak. Parke tematikoa

Ahokularitza enpresa bat kontratatu zuten sarrerak saltzeko sistemaren segurtasuna aztertzeko

Ahokulariak parke tematikora deitu zuen bere burua software-saltzaile moduan aurkeztuz

Enplegatuekin pixka batean hitz egin ondoren, parkean Adobe Readerren zein bertsio erabiltzen zen jakin zuen

# Benetazko kasuak. Parke tematikoa

Aholkularia parkean agertu zen familia baten itxurak eginez (haur eta guzti)

Ordenagailu baterako sarbidea eskatu zuen, posta elektronikoan zituen  
sarrerak inprimatu ahal izateko

Langileak sartzeko aukera eman zion (nahiz eta debekatuta egon)

# Benetazko kasuak. Parke tematikoa

Sarrerekin .pdf fitxategia irekitzean, software maltzur bat instalatzen da ordenagailua kontrolatzeko

Ordenagailu horretatik enpresaren zerbitzarietara sar daiteke