



DIGICOM
PLAN DE DIGITALIZACIÓN
DEL COMERCIO DE GIJÓN

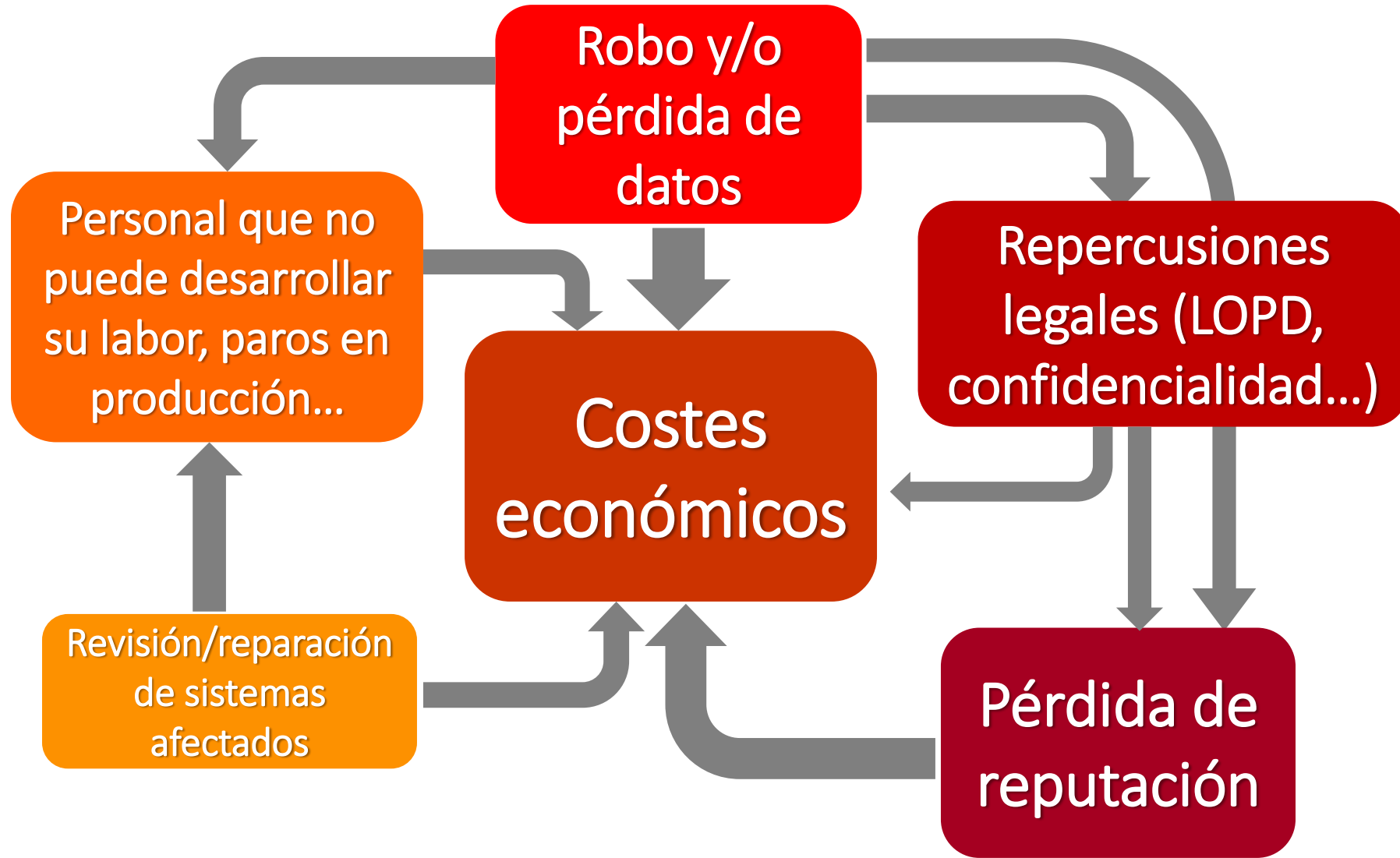
JORNADAS DIVULGATIVAS “Ciberseguridad en el comercio”



La ciberseguridad en las empresas en España

- España es el **tercer** país que más ciberataques recibe
- En 2017, el INCIBE registró **más de 120.000 incidentes** (casi el cuádruple que en los cuatro años anteriores juntos)
- El **70%** de los ciberataques se dirige contra las PYMES
- **El 80% de los ciberataques tiene su origen en fallos humanos**





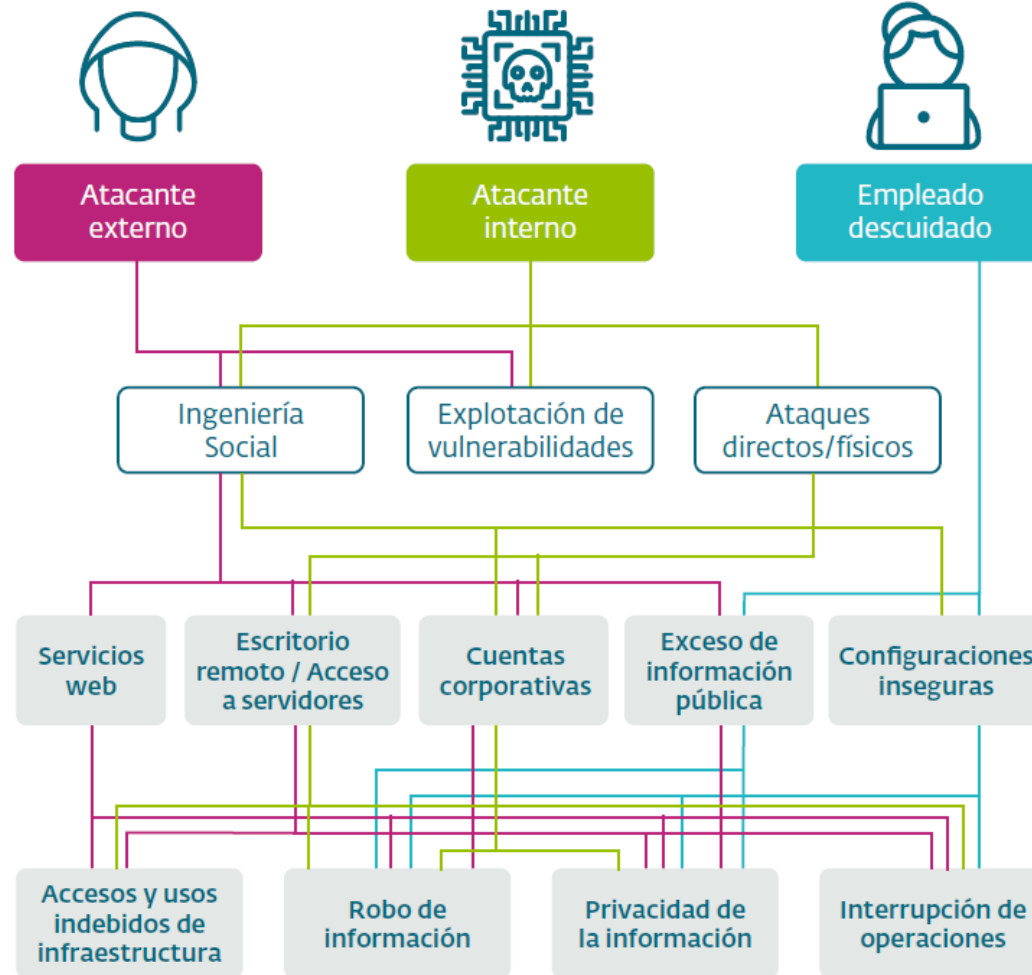
¿Cuáles son los principales riesgos de ciberseguridad a los que se enfrentan las empresas?

La amenaza humana y los falsos mitos

- **Falso Mito #1:** “quien va a querer atacarme a mí” / “total, para lo que nosotros hacemos” / “ni que fuéramos la NASA”
- **Falso Mito #2:** “en XX años que llevamos funcionando nunca pasó nada” / “se exagera todo para que gastemos el dinero en cosas que no hacen falta”
- **Falso Mito #3:** “tenemos un informático muy bueno” / “hemos comprado un antivirus de lo mejor”

- Hay que desterrar la idea de que la ciberseguridad es cosa “del informático”; ¡ni es un mago, ni tiene superpoderes! Y lo mismo ocurre con **los antivirus: no son omnipotentes**.
- Cada persona puede aportar mucho en ciberseguridad, simplemente **estando alerta y siendo proactiva** a la hora de evitar acciones de riesgo.
- En función del puesto de trabajo, existirán riesgos distintos: **el objetivo es conocerlos, y saber cómo actuar ante ellos**.
- **La ciberseguridad está estrechamente relacionada con la legislación en materia de protección de datos personales**. Por ello, trabajar para reducir los riesgos ayuda a evitar situaciones que puedan comprometer estos datos.

Principales amenazas



Malware

Se llama malware, del inglés malicious software, programa malicioso, programa maligno, badware, código maligno, software maligno, software dañino o software malintencionado a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Ransomware

Un ransomware, o "secuestro de datos" en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Criptominería

Anteriormente, la mayoría de los códigos de criptominería maliciosos trataban de descargar y ejecutar un programa de minado en los dispositivos. Sin embargo, una nueva forma de malware de criptominería se ha convertido muy popular recientemente: mina a través del navegador con un simple JavaScript. Este método (también conocido como cryptojacking) provoca la misma actividad maliciosa sin necesidad de instalar ningún software.

Phishing

Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

Exploits

Exploit es una palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Es un programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio.

Recomendación

Utilizar siempre versiones actualizadas del software (sistema operativo, navegador, aplicaciones instaladas,...).

Estar pendiente de las actualizaciones e instalar.

También es imprescindible un buen antivirus.

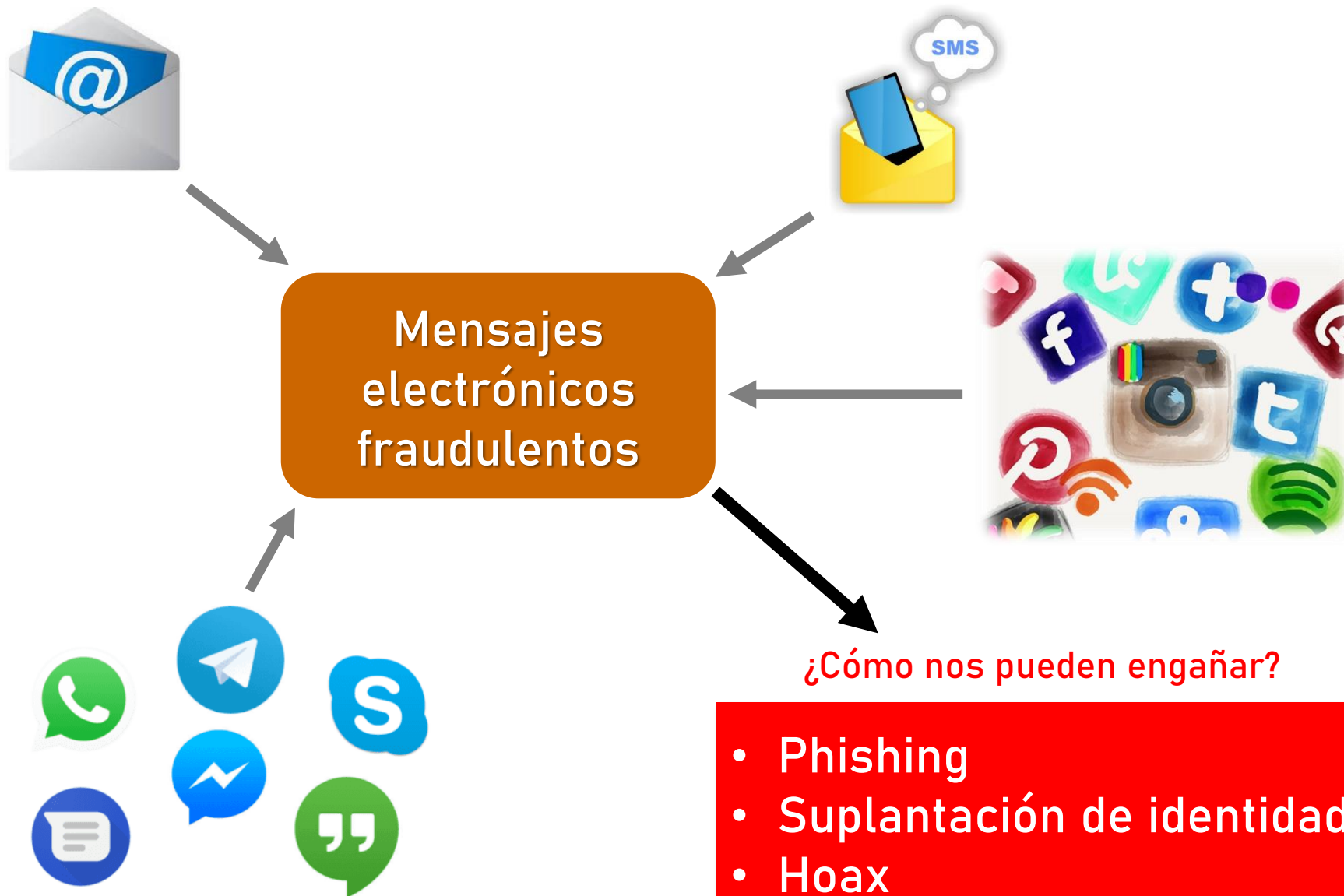
No instalar software desconocido, software pirata o software fraudulento.

Precaución con los correos de destinatarios desconocidos.

Cuidado con los enlaces: verifica el enlace. Antes de hacer clic, coloca el cursor sobre un enlace y mira la esquina inferior izquierda de la pantalla para ver la URL correspondiente.

Evita abrir archivos adjuntos de correos electrónicos no solicitados.

No facilitar datos mediante formularios proporcionados por email. Se debe ir al sitio oficial.



Phishing

¿Qué es el phishing?

Es un tipo de “ataque” caracterizado por **intentar adquirir información confidencial de forma fraudulenta** (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria).

El atacante (**phisher**) se hace pasar por una persona o entidad de confianza a través de un comunicación electrónica “oficial”, por lo común un correo electrónico, o algún sistema de mensajería instantánea (o incluso utilizando también llamadas telefónicas).

Su nombre viene del término inglés para la pesca, **“fishing”**.

Wikipedia

¿Cómo funciona?

El mensaje de phishing suele tener una **apariencia prácticamente idéntica** a la de la organización de la que supuestamente proviene, y que ***muchas veces no levanta sospechas en las aplicaciones antivirus o antispam.***

Si el usuario “muerde el anzuelo”, muchas veces será redirigido a un sitio web que también es idéntico al original, que en realidad está controlado por los atacantes.

Por lo general, tanto mensajes como sitios web presentan una serie de elementos que nos ayudan a detectar su carácter fraudulento.

¿Qué persigue?

- **Robar contraseñas**
- **Tener acceso a datos confidenciales o personales.**
- **Lograr beneficio económico**, como pago a un chantaje o secuestro de información, consiguiendo operar con las cuentas bancarias del atacado, suplantando al destinatario de transferencias o pagos...
- Lograr acceso a los dispositivos o sistemas de la organización, para acceder a su información, o utilizarlos en otras acciones maliciosas (ataques a terceros, etc.).

Por lo general, todas estas cuestiones están relacionadas en mayor o menor medida.

De Agencia Tributaria <support@agenciatributaira.freshdesk.com> ☆

Asunto **Fwd: Nuevo mensaje || 752886301049**

A [redacted]@ [redacted] ☆

La cuenta de correo no pertenece a la Agencia Tributaria



Agencia Tributaria

Usted tiene un reembolso de impuestos, de 350.16 Euro

Estimado contribuyente,

1 - Ingrese su información de contacto.

Para enviar la solicitud electrónicamente, complete la información. Cuando se complete el formulario, se le pedirá que confirme que toda la información en el formulario es correcta.

2 - Tratamiento fiscal.

La información que ingrese y el formulario de solicitud completo se envían a Agencia Tributaria a través de una conexión segura y encriptada, y otros no podrán ver la información.

solo complete el formulario a continuación y nos contactaremos con usted lo antes posible.

(Su número de archivo es: 5163_17) : [naga clic aqui.](#)

Gracias por su cooperación,

Agencia Tributaria.

Redacción extraña

Enlace a la página web fraudulenta

RV:WG: Tienes (1) documentos nuevos 5b62936506b4a !



//ABANCA <servicio-abanca1@[REDACTED]>

jue 02/08, 7:15
mail29773781@mail.com

Dirección de remitente que no corresponde con el dominio real.



Nouveau Document.txt
344 bytes

descargar Guardar en OneDrive - Personal

Adjunto sospechoso

//ABANCA

Estimado/a Cliente
Deseamos informarle de que tiene una nueva actualización !

<https://bancaelectronica.abanca.com/>

Redacción extraña

Gracias a no responder a este mensaje , usted no tendra que responder.

Atentamente,
Director General : Francisco Botas



Dirección de remitente que no corresponde con el dominio real.

URL de destino sospechosa en el botón de acceso

Solicitud que no se ajusta a la forma habitual de proceder

Redacción extraña

Expiracion del correo electrónico [redacted]@[redacted].es - Unicode (UTF-8)

Archivo Mensaje

Expiracion del correo electrónico [redacted]@[redacted].es

Arsys Servidor de Correo (webmail_admin@[redacted]ring.co.uk) Agregar contacto 15/01/2020 9:43

Para: [redacted];

arsys

Estimado cliente,

Queremos informarle que la fecha de expiración del correo electrónico [redacted]@[redacted].es será el 16 de Enero 2020.

Correo electrónico	[redacted]@[redacted].es
Fecha de expiración	16.01.2020

Quando la fecha de expiración haya transcurrido, los siguientes servicios serán deshabilitados:

- Envío y recepción de mensajes
- Las aplicaciones web que han sido vinculadas con su cuenta

[Renueva ahora](#)

La renovación es gratis

f g+ in t You

Este mensaje y sus posibles documentos adjuntos son confidenciales y están dirigidos exclusivamente a sus destinatarios. Por favor, si Ud. no es uno de ellos, notifíquenoslo y elimine el mensaje de su sistema. De conformidad con la legislación vigente, queda prohibida la copia, difusión o revelación de su contenido a terceros sin el previo consentimiento por escrito de Arsys.

Dirección de remitente que no corresponde con el dominio real.

Enlace fraudulento, a URL que no corresponde a Arsys

Account Notification !

Inbox x



Team Support
to me

Service@account.com via [redacted] hostgator.com

7:45 AM (15 hours ago)

Dirección de remitente que no corresponde con el dominio real.



Your Account PayPal is Limited, You Have To Solve The Problem In 24 Hours.

Hello PayPal Customer,

We are sorry to inform you that you can't access all your paypal advantages like sending money and purchasing, due to account limitation .

Why my account PayPal™ is limited?

Because we think that your account is in danger from stealing and unauthorized uses .

What can I do to resolve the problem?

You have to confirm all your account details on our secure server by clicking the link below and following all the steps

Confirm Your Information

Enlace fraudulento, a URL que no corresponde a PayPal

From confirm@amazon.com <"confirm@amazon.comasis.cartera"@colchonesrelax.com.co>

Subject Amazon Order #154-1238066-0002647

To [REDACTED]

Note the difference between the friendly signature - and the actual sender.



[Your Recommendations](#) | [Your Account](#) | [Amazon.com](#)



Links go to legitimate Amazon webpages.

Order Confirmation

Order #154-1238066-0002647

Hello ,

Thank you for shopping with us. We confirmation that your item has shipped. Your order details are available on link below. The payment details of your transaction can be found on the [order invoice](#).

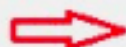
Your estimated delivery date is:

Tuesday, December 18, 2018 - Thursday, December 20, 2018

Your shipping speed:

Standard

Links to virus laden document

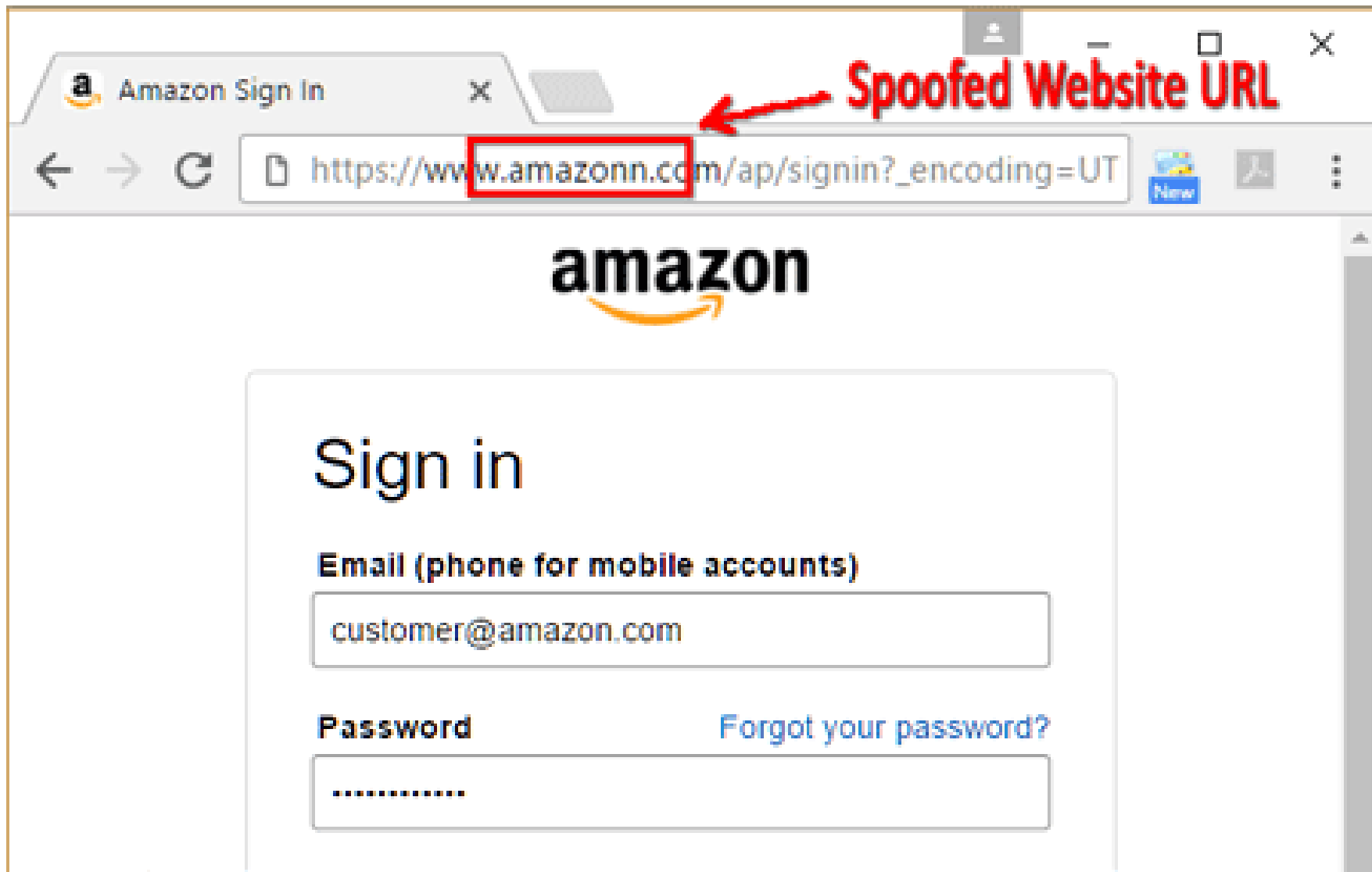


[Order Details](#)

Payment Summary

Order #154-1238066-0002647

Item Subtotal:	\$11.13
Shipping & Handling:	\$2.87
Total Before Tax:	\$14.00
Estimated Tax:	\$1.26
Order Total:	\$15.26





¿Cómo podemos detectarlos?

- Redacción anómala
- Peticiones poco habituales, que solicitan datos de cuentas bancarias, usuario y contraseña...
- URLs sospechosas

Suplantación de identidad

Si bien el phishing es en realidad una suplantación de identidad, por lo general se basa en suplantar entidades u organizaciones.

Sin embargo, cada vez proliferan más las suplantaciones de identidad de personas, bien pertenecientes a la propia empresa, o bien externas de confianza.

Dirección de remitente que no corresponde con el real.

De: Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológico <mariano.gonzalez@ctic.es> <marinelife@ommegaonline.org>
Enviado: jueves, 16 de enero de 2020 15:40
Para:
Asunto: Factura mensuales

Senyors,

Us adjunto comprovant de pagament de les factures de Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológico

http://myb2bcoach.com/l7hyd/private_sector/9411952_80txjHDkks_cloud/za6ahbfsa_tsux0s4591x/

Salutacions,

Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológico

Teléfono 94 418 23 05 Extensión 5836

URL sospechosa

Solicitud que no se ajusta a la forma habitual de proceder, y en otro idioma

Datos de contacto falsos

Dirección de remitente que no
corresponde con el real.

De: Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológico <r.barba@fullservicesrl.net>

Para:

Enviado: jueves, 12 de diciembre de 2019 12:48:02 CET

Asunto: Invio per posta elettronica: salario consolidato

Gentile

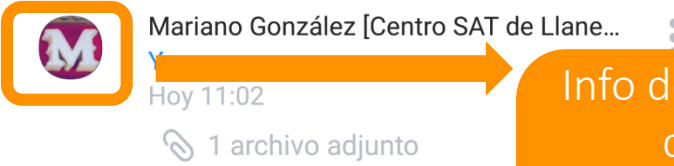
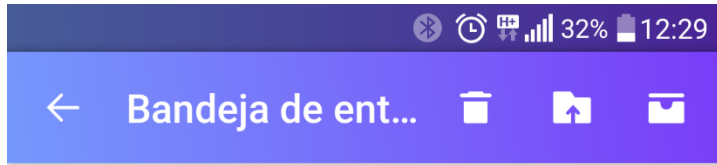
Asturias,

per l'ennesima volta il mio stipendio risulta più basso di quanto mi spetta. Attendo una spiegazione.
Di seguito il salario del mese di Novembre.
Documento disponibile qui:

<https://mariano.gonzalez@ctic.es/aknxqne/>

Cordiali saluti.

Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológico mariano.gonzalez@ctic.es



Info de remitente que no corresponde con el real (logo, dirección).

Estimado cliente:

No hemos recibido el pago de esta factura.

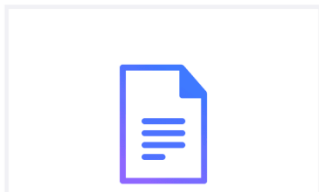
Atentamente,

Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológico

Teléfono 95 877 58 30 Extensión 4990

Datos de contacto falsos

1 archivo adjunto | 251 KB



Adjunto sospechoso



Factura P-4388

Hola,

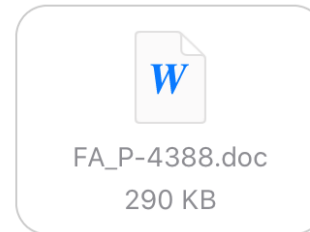
Adjunto envío la factura correspondiente al mes.

Salutacions,

Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológico

Tel. +34 968 14 03

mariano.gonzalez@ctic.es



Favor urgente, solicito confidencialidad

Recibidos x

CEO <maria.garcia@habitos-inseguros.com>
<para juan.perez@habitos-inseguros.com>

9:52 (hace 4 minutos) ☆ ↶ ⋮

Recurso a ti por tu profesionalidad y proactividad. Necesito que realices una transferencia bancaria para una nueva adquisición que se hará pública a lo largo del próximo mes. Los datos para la transferencia se encuentran en el archivo adjunto. Por favor, notifícame cuando esté lista.

Este asunto debe ser manejado sólo por ti, por tal motivo, recibirás durante el día una cláusula de confidencialidad para firmar al respecto.

Para mantener la validez jurídica de esta operación, debemos mantener esta comunicación únicamente mediante correo electrónico.

Muchas gracias



lun 14:42

Aurora
RE: CONFIDENCIAL

Para Alfonso

Perfecto, Alfonso.

Estamos en este momento efectuando una operación financiera en relación a la compra de maquinaria para la empresa. Esta operación debe ser estrictamente confidencial, y te obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono ni por voz.

El anuncio legal de esta adquisición será entre el 12 y el 15 de febrero de 2019, en nuestras instalaciones.

Para finalizar, necesito que me indiques el saldo con el que contamos y el número de cuenta.

Atentamente.

- El diseño del correo suele ser el corporativo
- *El contenido está muy bien redactado*
- Busca la respuesta inmediata de la persona, apelando a sus valores profesionales
- Persigue lograr datos o transacciones económicas, infectar los equipos...
- Suele insistir en un carácter confidencial y urgente, y a comunicarse únicamente por email

Hoax (Bulos) y otros engaños

- *Los hoax o bulos son falsedades difundidas por medios electrónicos y articuladas de manera deliberada para que sean percibidas como verdaderas* (Wikipedia).
- A diferencia del phishing, que suele tener un fin ilícito o lucrativo y un alcance más restringido o específico, los bulos buscan **difundir masivamente informaciones falsas**, y pueden llegar a generar daños considerables (reputacionales, sociales, estratégicos, etc.).
- Las *fake news* son un ejemplo de hoax.

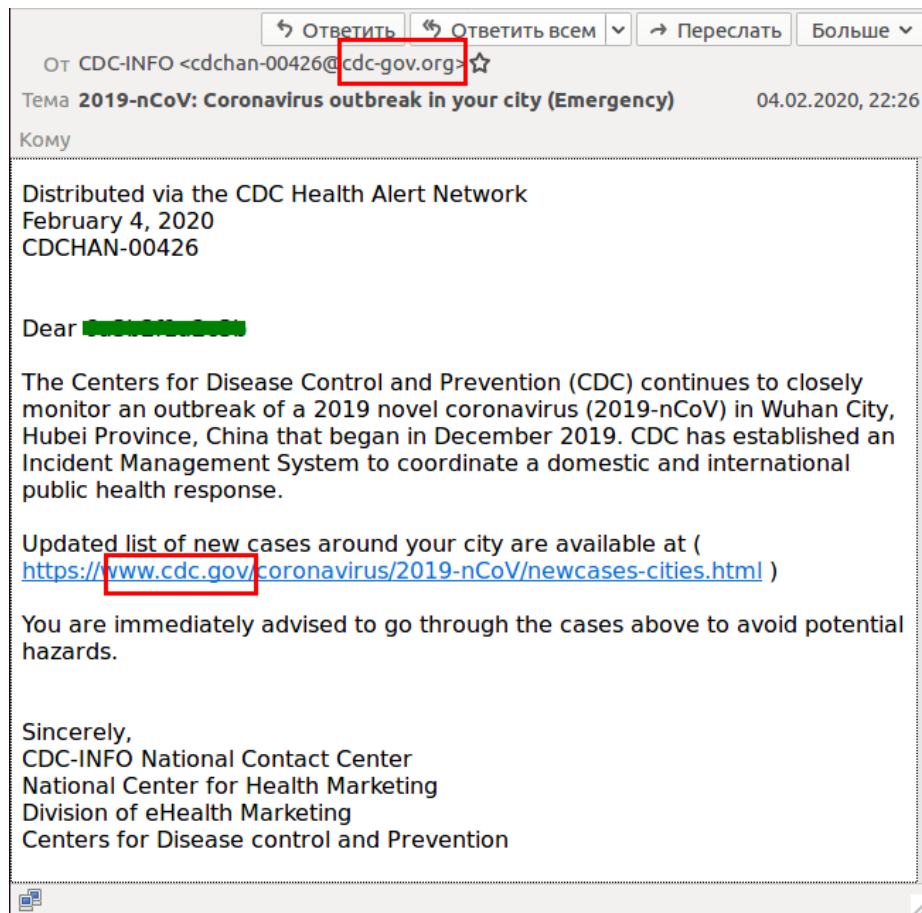
¿Cómo reconocer un bulo?

- Por lo general, no incluyen fechas ni datos sobre ellas, para lograr una imagen de “intemporalidad” que les permita estar activos más tiempo.
- No citan fuentes donde comprobar la veracidad de la información.
- Suelen contener un “gancho” para captar la atención del usuario, basado en el morbo, en temas monetarios, en causar miedo y sobre todo en que encaja con el contexto social del momento.
- Incluyen una petición de reenvío (para alertar a otras personas, por ejemplo), cuyo objetivo es captar direcciones de correo o números de teléfono y poder realizar posteriores campañas de spam, saturar ciertos canales o servicios de comunicación, o simplemente difundir la información falsa el máximo posible.

Algunos hoax populares

- **WhatsApp**: WhatsApp va a ser de pago de manera inminente... reenvía este mensaje a X personas antes del día X.
- **Hotmail**: Hotmail cerrará sus cuentas. Perderás tus contactos y tus correos.
- **Actimel**: Actimel es malo para la salud. Tu cuerpo ya produce L. Casei y si lo tomas deja de fabricar defensas.
- **RedBull**: RedBull contiene veneno en su composición química.
- **Llamada desde cierto número de teléfono**: Recibes una llamada telefónica de cierto número; si aceptas o rechazas la llamada, alguien accederá a la SIM de tu teléfono, la duplicará y la usará para cobrarte llamadas a números de tarificación especial.

Coronavirus



Re:SAFTY CORONA VIRUS AWARENESS WHO



World Health Organization



Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

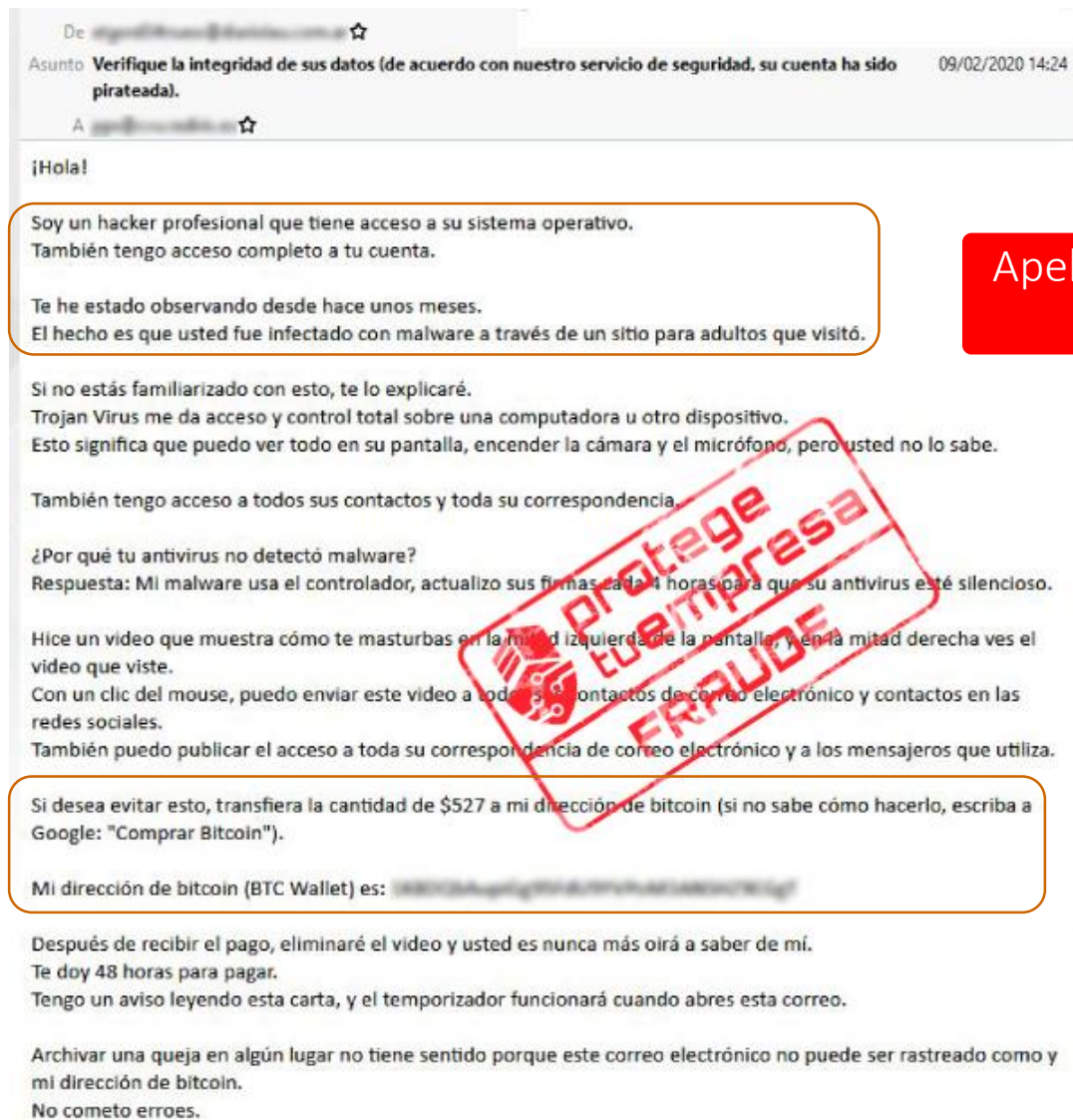
Symptoms common symptoms include fever,coughhshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE

Sextorsión



Redacción
extraña

Apela a la vergüenza
del usuario

Contraseña robada + sextorsión

Subject: password (-) for - is compromised

From:

Hello!

I'm a hacker who cracked your email and device a few months ago. You entered a password on one of the sites you visited, and I intercepted it. This is your password from - on moment of hack: -

Of course you can will change it, or already changed it. But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System. I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources. Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom. But I was struck by the sites of intimate content that you often visit.

I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!) I made screenshot with using my program from your camera of yours device. After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts! BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence. I think \$892 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1JTtwbvmM7ymByxPYCByVYCwasjH49J3Vj

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult. After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment. If this does not happen - all your contacts will get crazy shots from your dark secret life! And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

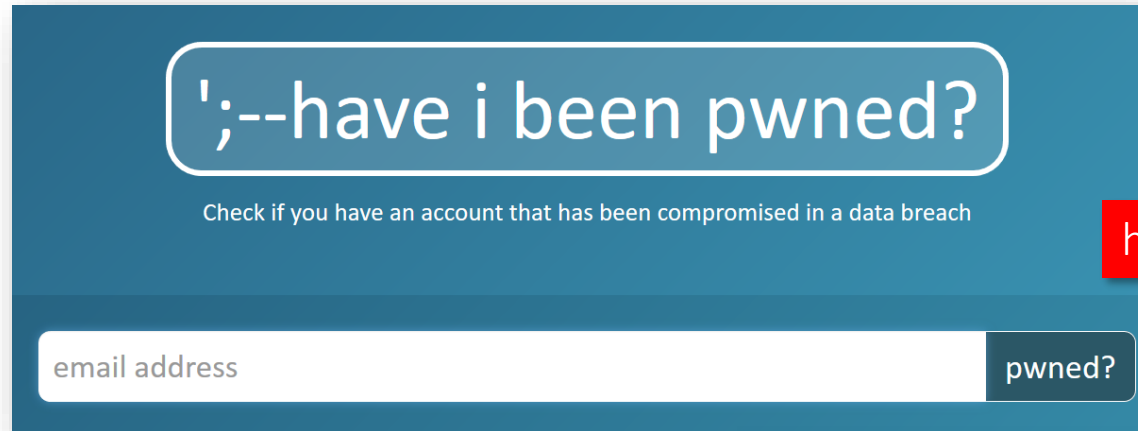
p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

I hope for your prudence.
Farewell.

Muestra una contraseña que el usuario ha utilizado, generalmente en algún servicio que ha sido atacado

Apela a la vergüenza del usuario

¿Cómo saber si mis contraseñas han sido robadas?



';--have i been pwned?


Check if you have an account that has been compromised in a data breach

email address

pwned?

<https://haveibeenpwned.com/>

<https://monitor.firefox.com/>



Firefox Monitor

Inicio Filtraciones Consejos de seguridad

Comprueba si formaste parte de una filtración de datos en línea.

Averigua qué saben de ti los hackers.
Descubre cómo ir siempre un paso por delante.

Introduce una dirección de correo electrón

Busca filtraciones

Busca tu dirección de correo en filtraciones de datos públicas hasta 2007.

¿Qué consecuencias pueden tener estos ataques?

- **Robo de datos sensibles o confidenciales** (datos personales de empleados / clientes / etc., datos de proyectos estratégicos...)
- **Robo de datos bancarios / Transacciones económicas fraudulentas**
- **Acceso ilícito a servicios o herramientas internas de manera encubierta**
- **Acceso ilícito a servicios online y suplantación de identidad**
- **Acceso remoto encubierto a dispositivos y equipos**
- **Bloqueo de información** a cambio de un rescate: ransomware

¿Cómo actuar para prevenirlos?

- Al recibir mensajes inesperados de carácter sospechoso, **comprobar si incluyen evidencias de su naturaleza fraudulenta**: remitentes anormales, contenido extraño, enlaces o archivos adjuntos sospechosos...
 - **Nunca abrir ni ejecutar los archivos adjuntos**
 - **No acceder a los enlaces incluidos**
 - **No responder al mensaje**
- **Confirmar con el supuesto remitente si el mensaje es verdadero** y ha sido enviado por él.
- **Notificarlo al responsable de sistemas** y a las personas que por su perfil sean susceptibles de recibir el mismo mensaje.
- **Evitar el uso de servicios online de carácter personal** (redes sociales, mensajería, etc.) **desde dispositivos corporativos**, puesto que tienen una mayor exposición a recibir ciertos tipos de contenido fraudulento, y además, **pueden tener repercusiones legales**.

¿Sabrías detectar ahora un correo fraudulento?

¿Puedes detectar cuándo te están engañando?

La identificación de un ataque de suplantación de identidad (phishing) puede ser más difícil de lo que piensas. El phishing consiste en que un atacante intenta engañarte para que facilites tu información personal haciéndose pasar por alguien que conoces. ¿Podrías detectar qué es falso?

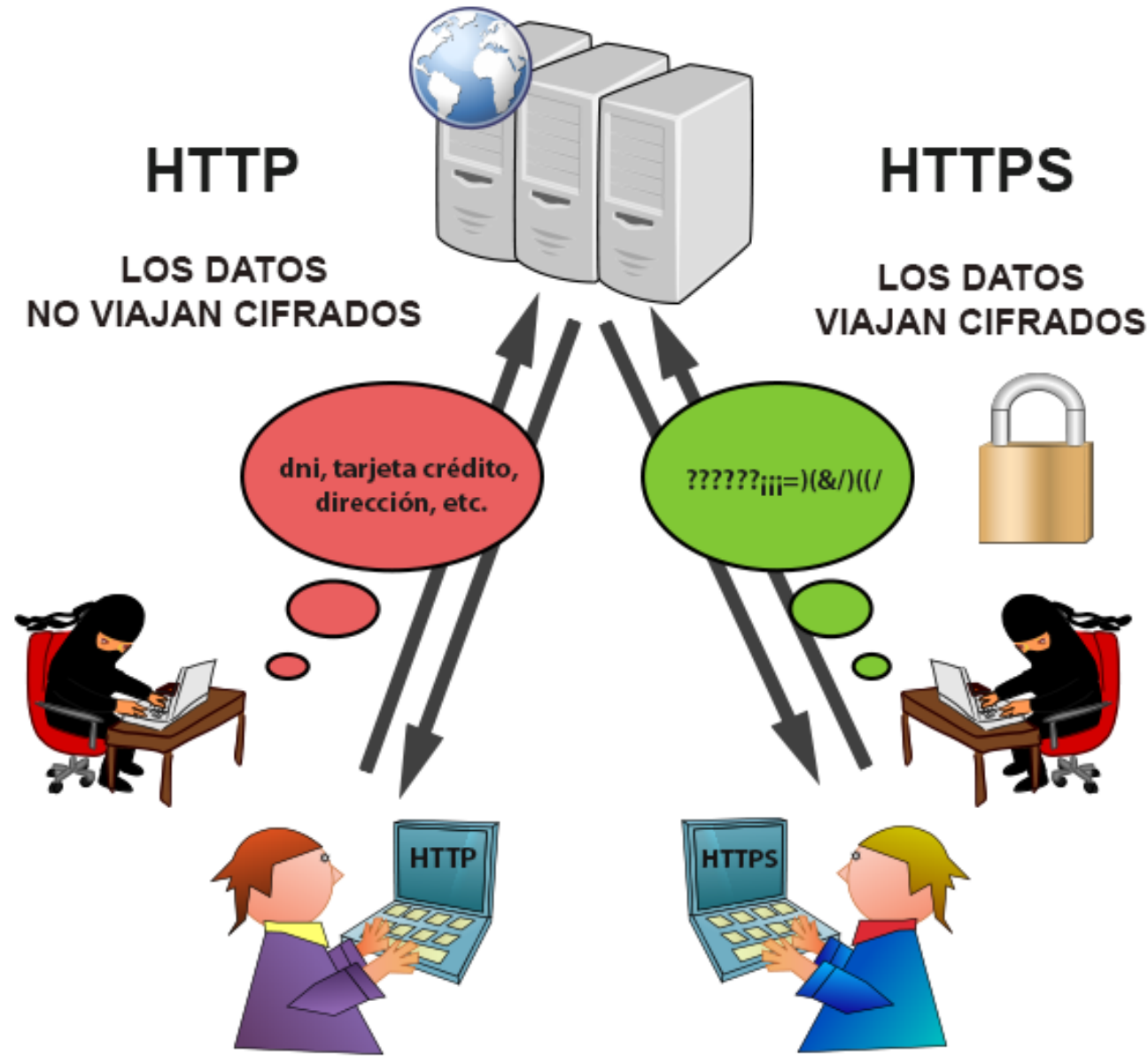
HACER EL TEST



<https://phishingquiz.withgoogle.com/>

Sitios web inseguros

La importancia de la navegación segura mediante https



Home | CTIC

https://www.fundacionctic.org

La conexión es segura

Tu información (por ejemplo, las contraseñas o los números de las tarjetas de crédito) es privada cuando se envía a este sitio web. [Más información](#)

Certificado (válido)

Cookies: (37 en uso)

Configuración del sitio web

Stop slider

TECNOLO

f m

tic y de e

Certificado

General Detalles Ruta de certificación

Información del certificado

Este certif. está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto
- Prueba su identidad ante un equipo remoto
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

* Para ver detalles, consulte la declaración de la entidad de c

Emitido para: *.fundacionctic.org

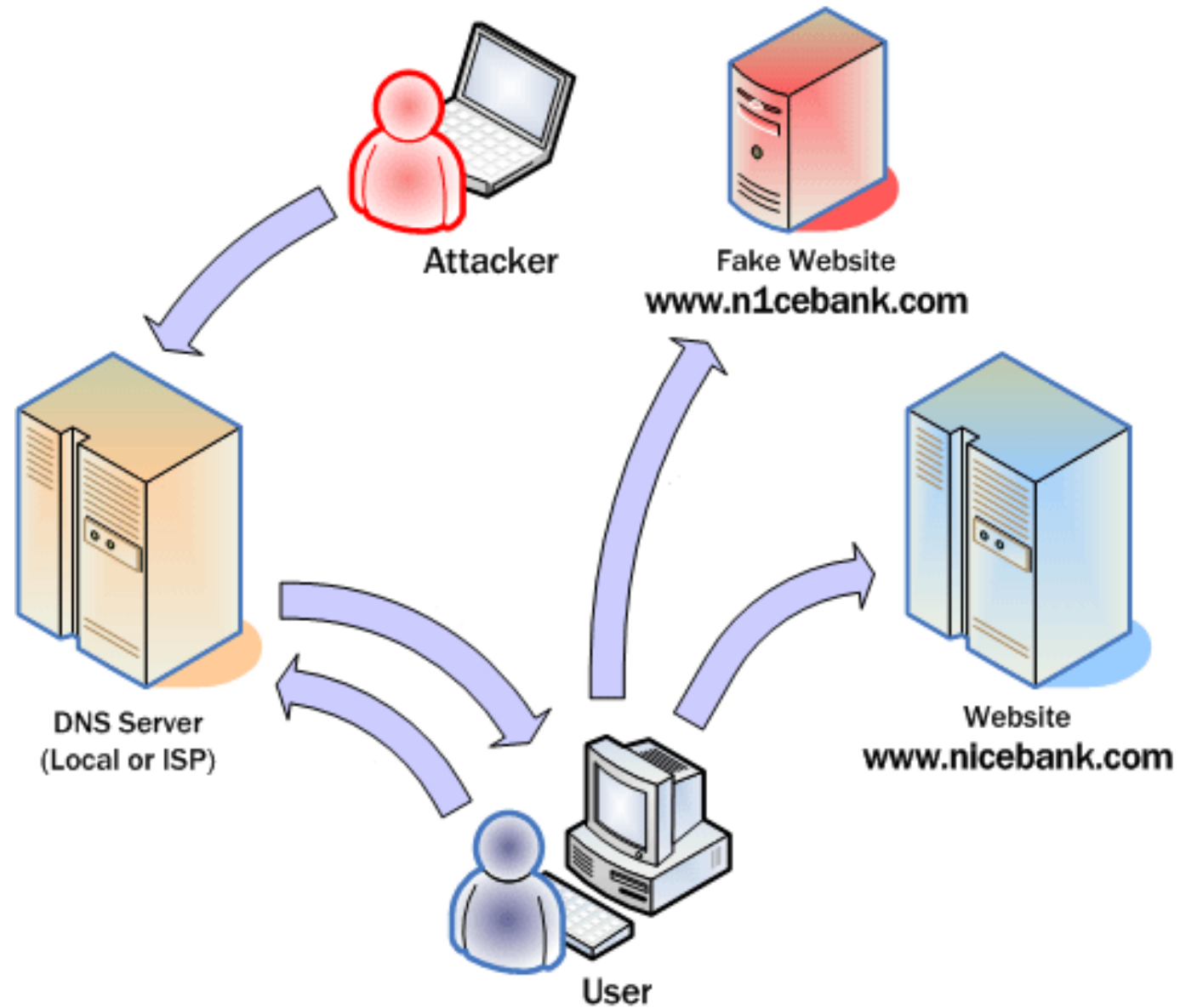
Emitido por: Let's Encrypt Authority X3

Válido desde 18/02/2019 **hasta** 19/05/2019

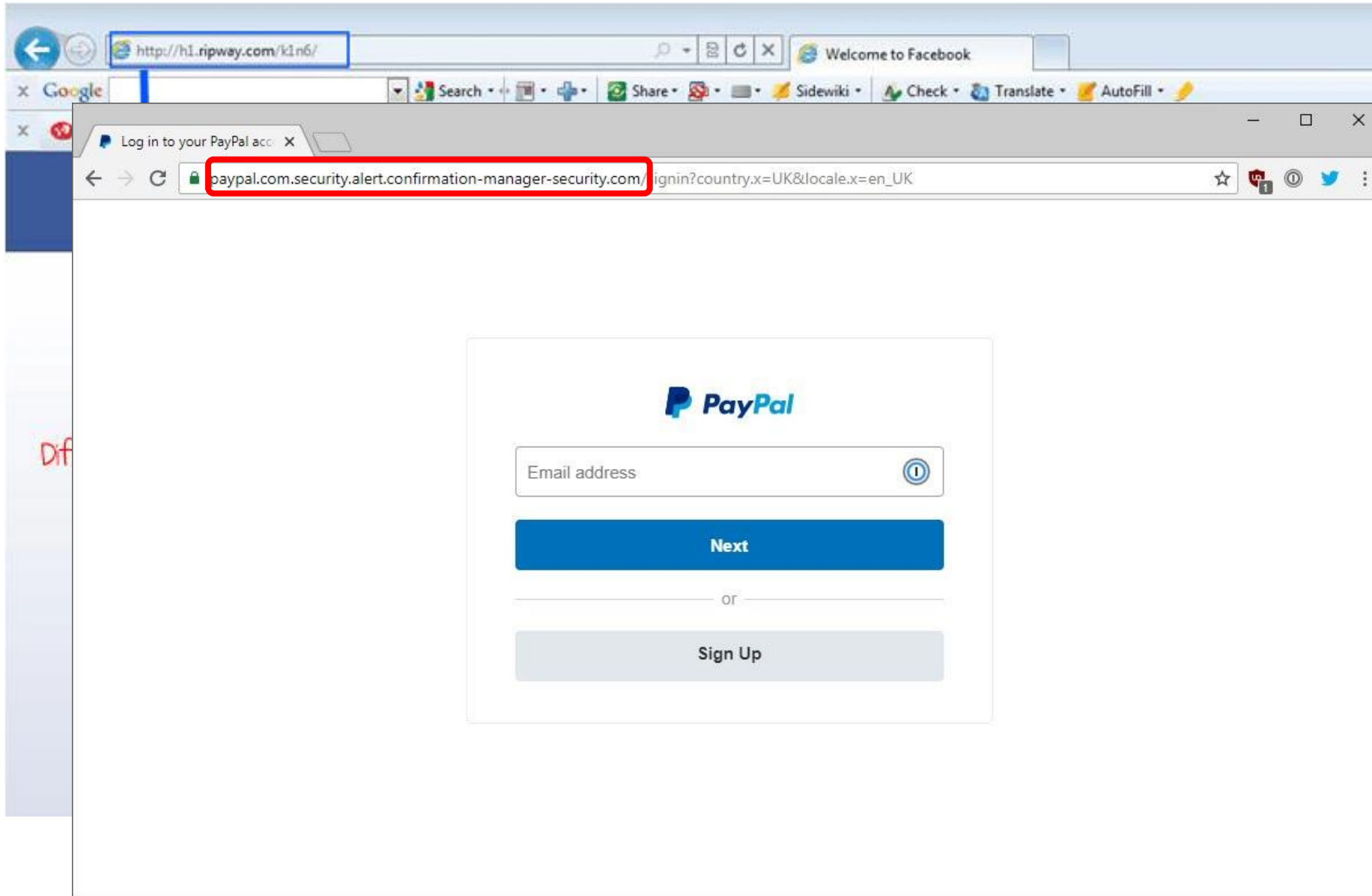
Declaración del emisor

Aceptar

El pharming, un sistema basado en la suplantación de un sitio web



¡¡Ojo a la URL del sitio!!



Software malicioso

- **No es recomendable emplear software de descarga de ficheros en un entorno corporativo**, por los riesgos que llevan aparejados estos sistemas.
 - Si es necesario utilizarlo, procurar **instalarlo en un equipo sin información sensible**, o en su defecto configurarlo de forma que no quede compartida ninguna información.
 - Igualmente, es recomendable que ese equipo **no esté conectado a la red interna**.
- **Debe extremarse la precaución a la hora de abrir o ejecutar los archivos descargados**, pues pueden contener malware, troyanos, etc.
- **No deben instalarse aplicaciones adicionales salvo en entornos de prueba seguros** (equipos sin conexión a la red interna, sin información sensible, con antivirus, etc.).

Dispositivos de almacenamiento extraíbles

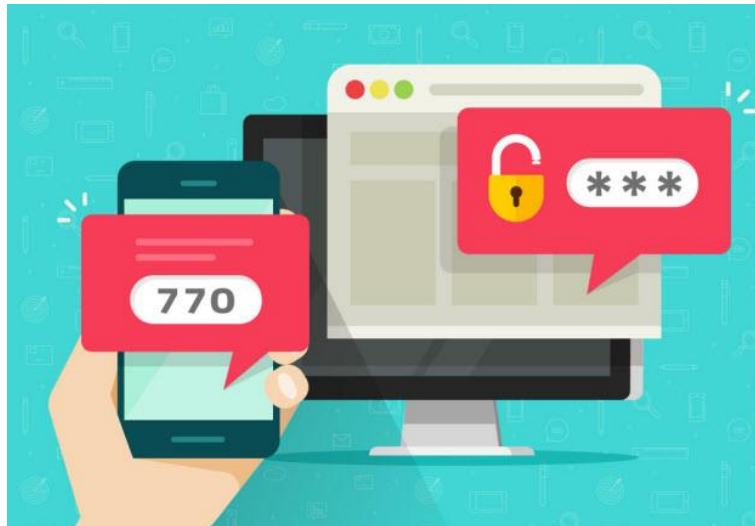
Dispositivos de almacenamiento extraíbles

- **No conectar dispositivos de almacenamiento extraíbles** (memorias y discos externos USB, tarjetas de memoria, etc.) **que no sean de la empresa** o estén verificados.
 - Si debe conectarse un dispositivo de terceros, hacerlo en un equipo aislado y con protección antivirus.
- **No almacenar información de la empresa en servicios de almacenamiento online** (Dropbox, Google Drive, etc.) **con cuentas personales**, puesto que el nivel de protección es menor, y se pierde control sobre la información. **¡Repercusiones legales!**
- **Evitar el envío de información corporativa sensible a través de mensajería instantánea estándar** (WhatsApp, Telegram...) **o cuentas de correo personales.**
- **Almacenar la información corporativa en las carpetas o unidades sobre las que se haga la copia de seguridad.**

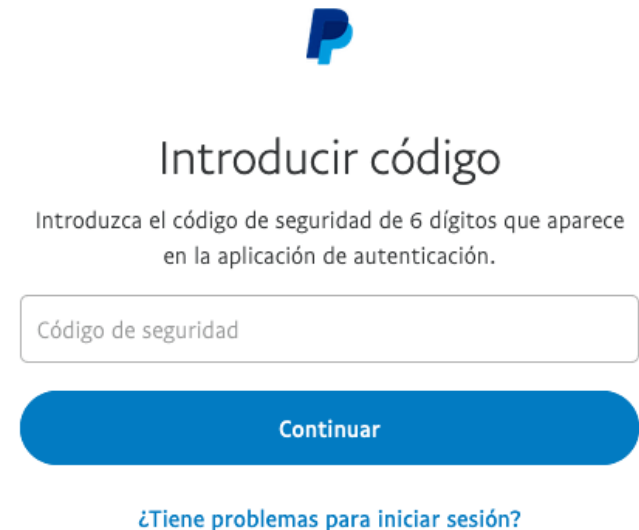
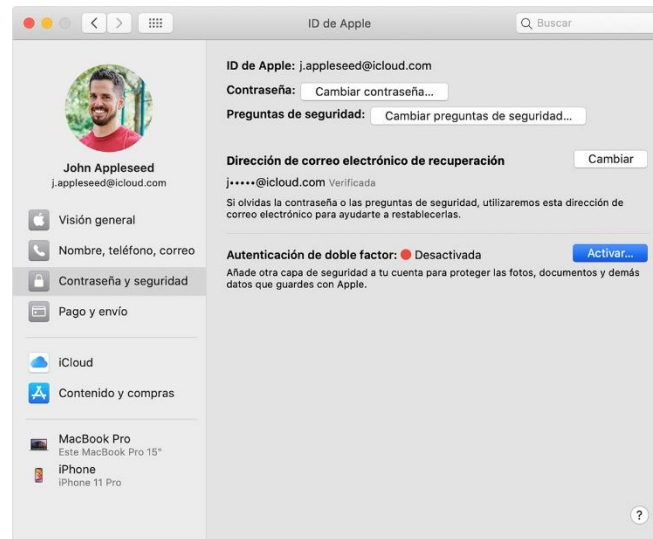
La importancia de las contraseñas y su fortaleza

Doble factor de autenticación: ¿qué es y por qué lo necesito?

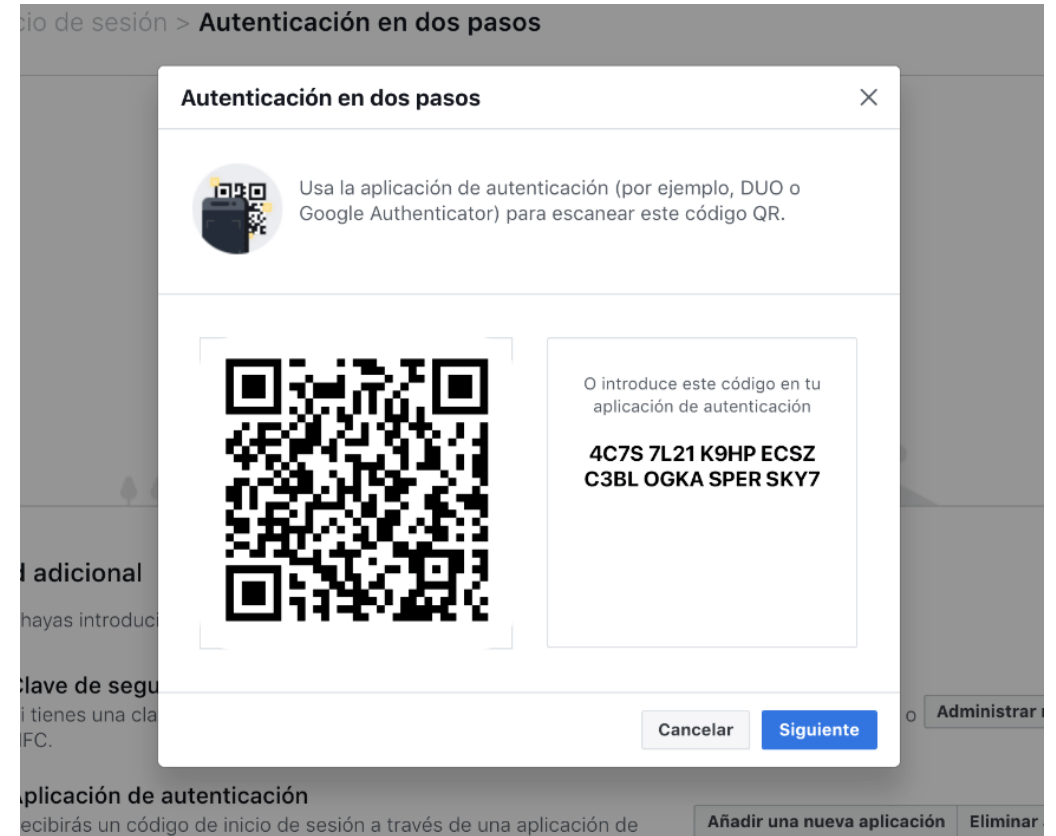
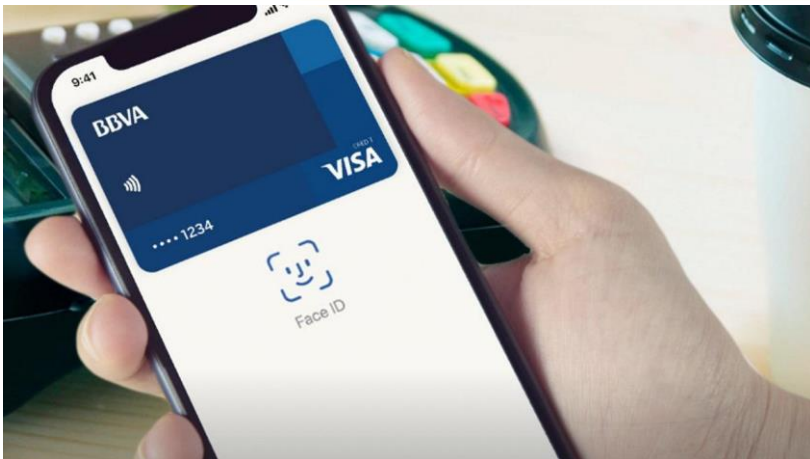
Durante los últimos dos años, muchos servicios online han comenzado a ofrecer un doble factor de autenticación. Se trata de una medida de seguridad extra que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje SMS, además de una contraseña para acceder al servicio. Los sistemas de doble factor de autenticación son mucho **más seguros que las contraseñas**.



Identificación de doble factor



Identificación de doble factor



A pesar de que se habla del final de las contraseñas como factor exclusivo de autenticación (por sistemas de doble factor, identificaciones biométricas, etc.), **a día de hoy siguen siendo el principal sistema empleado en empresas para proteger el acceso a servicios, aplicaciones, dispositivos e información.**

Por tanto, en la medida de lo posible, **debe fomentarse el empleo de contraseñas fuertes y seguras**, que ofrezcan una mayor resistencia a ataques (fuerza bruta, diccionario...)

Password:

Login

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

- Más de 8 (10) caracteres
- Minúsculas, Mayúsculas, Números y Símbolos

José.Pérez.García.11031980

¿es segura?

Cosas que NO SE DEBEN UTILIZAR en las contraseñas



- Nombres Propios
- *Contraseña*
- Nombre del servicio o aplicación (*Si la web es facebook, la clave será facebook; lo mismo con gmail, hotmail, etc.*)
- Hobbies y aficiones (*Equipos de fútbol, artistas o grupos musicales, nombres de actores o películas, etc.*)
- **Números identificativos o números de móvil:** *Son muy utilizados y dan sensación de seguridad, pero esta información se puede conseguir fácilmente por otras vías*
- Palabras completas fácilmente adivinables
- 654321, 111111, A1B2C3D4...
- *qwerty, asdfgh*, etc.

¿Cómo hacer entonces una contraseña fuerte DE VERDAD?

- Más de 8 (10) caracteres
- Minúsculas, Mayúsculas, Números y Símbolos
- Evitar nombres y palabras comunes
- Evitar datos numéricos fácilmente adivinables (teléfonos, DNI, fechas...)

 Aquí veras una
 Forma de crear 
CONTRASEÑAS SEGURAS 
PERO fáciles de RECORDAR.

http://youtu.be/iV9CmN-g_go



<https://password.kaspersky.com/es/>

 **Kaspersky Lab no guarda ni almacena tus contraseñas** 
No introduzcas tu contraseña real. Este servicio solo tiene fines educativos.

 **Contiene palabras muy usadas**

Tu contraseña puede ser descifrada con un ordenador común en

7 HORAS



Es el tiempo que necesitas para recorrer 647 km en tu Ferrari nuevo

- No usar la misma contraseña en todos los servicios
- No revelársela a nadie
- Mantenerlas guardadas en un sitio seguro
- Cambiarlas periódicamente por norma
- No reutilizarlas

Seguridad de nuestro sitio web











La seguridad de nuestro sitio web es muy importante. Debemos:

- Prevenir ataques
- Disponer de plan de contingencias

Recently Blocked Attacks

Time	IP / Action
January 23, 2021 4:00pm	195.154.232.125 (France) Blocked for FancyBox for WordPress <= 3.0.2 - Persistent XSS in query string: page=fancybox-for-wordpress
January 22, 2021 7:26am	37.120.179.241 (Germany) Blocked for Function Injection in Multiple Themes using Epsilon Framework <= 1.2.1
January 22, 2021 7:26am	37.120.179.241 (Germany) Blocked for Function Injection in Multiple Themes using Epsilon Framework <= 1.2.1
January 22, 2021 7:26am	37.120.179.241 (Germany) Blocked for Function Injection in Multiple Themes using Epsilon Framework <= 1.2.1
January 22, 2021 6:00am	51.89.204.20 (United Kingdom) Blocked for Malicious File Upload (Patterns)
January 22, 2021 2:47am	62.210.139.59 (France) Blocked for WAF-RULE-260
January 21, 2021 5:46am	54.39.131.235 (Canada) Blocked for Function Injection in Multiple Themes using Epsilon Framework <= 1.2.1
January 21, 2021 5:46am	54.39.131.235 (Canada) Blocked for Function Injection in Multiple Themes using Epsilon Framework <= 1.2.1

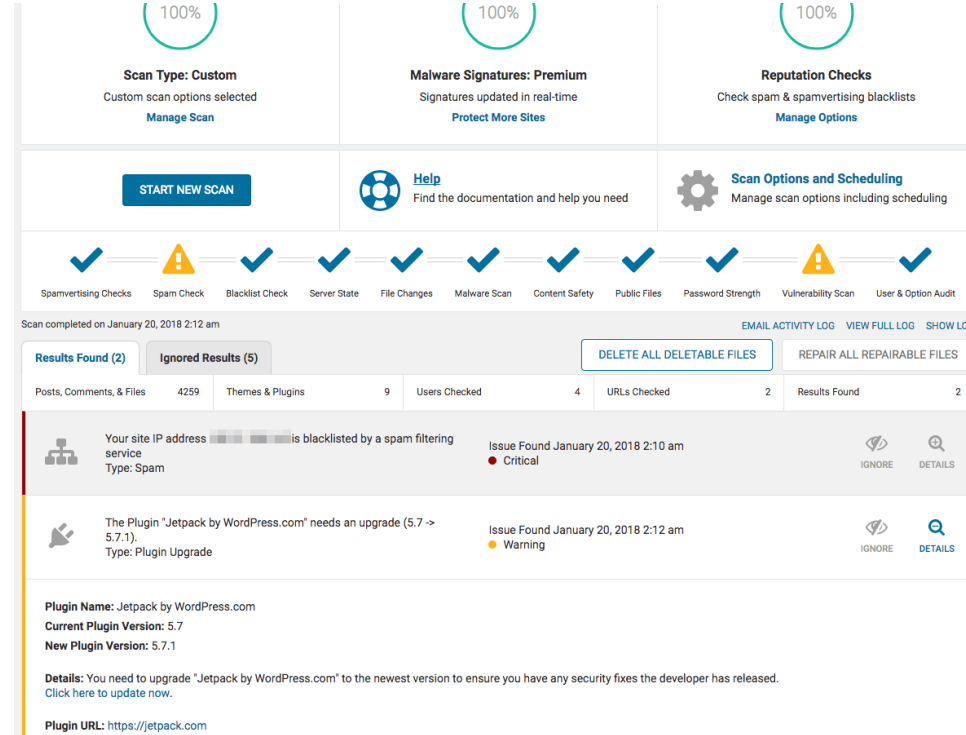
Top 10 IPs Blocked

IP	Country	Block Count
35.247.219.231	 Brazil	4
176.74.24.97	 United Kingdom	4
199.188.200.224	 United States	3
153.92.6.147	 Germany	3
157.230.44.77	 Singapore	3
91.215.216.28	 Bulgaria	3
54.39.131.235	 Canada	3
37.120.179.241	 Germany	3
34.122.18.76	 United States	3
190.107.177.240	 Chile	2

Update Blocked IPs



Wordfence Security



100% **Scan Type: Custom**
Custom scan options selected
[Manage Scan](#)

100% **Malware Signatures: Premium**
Signatures updated in real-time
[Protect More Sites](#)

100% **Reputation Checks**
Check spam & spamvertising blacklists
[Manage Options](#)

[START NEW SCAN](#) [Help](#) Find the documentation and help you need [Scan Options and Scheduling](#) Manage scan options including scheduling

Spamvertising Checks Spam Check Blacklist Check Server State File Changes Malware Scan Content Safety Public Files Password Strength Vulnerability Scan User & Option Audit

Scan completed on January 20, 2018 2:12 am [EMAIL ACTIVITY LOG](#) [VIEW FULL LOG](#) [SHOW LOG](#)

Results Found (2) **Ignored Results (5)** [DELETE ALL DELETABLE FILES](#) [REPAIR ALL REPAIRABLE FILES](#)

Posts, Comments, & Files	4259	Themes & Plugins	9	Users Checked	4	URLs Checked	2	Results Found	2
--------------------------	------	------------------	---	---------------	---	--------------	---	---------------	---

Issue Found January 20, 2018 2:10 am
Your site IP address [redacted] is blacklisted by a spam filtering service
Type: Spam
● Critical
[IGNORE](#) [DETAILS](#)

Issue Found January 20, 2018 2:12 am
The Plugin "Jetpack by WordPress.com" needs an upgrade (5.7 -> 5.7.1).
Type: Plugin Upgrade
● Warning
[IGNORE](#) [DETAILS](#)

Plugin Name: Jetpack by WordPress.com
Current Plugin Version: 5.7
New Plugin Version: 5.7.1

Details: You need to upgrade "Jetpack by WordPress.com" to the newest version to ensure you have any security fixes the developer has released.
[Click here to update now.](#)

Plugin URL: <https://jetpack.com>

















Backup / Restore
Migrate / Clone
Settings
Advanced Tools
Premium / Extensions

Files backup schedule: Weekly and retain this many scheduled backups:

Database backup schedule: Weekly and retain this many scheduled backups:

To fix the time at which a backup should take place, (e.g. if your server is busy at day and you want to run overnight), or to configure more complex schedules, [use UpdraftPlus Premium](#)

Choose your remote storage (tap on an icon to select or unselect):

 UpdraftPlus Vault	 FTP	 S3-Compatible (Generic)
 Dropbox	 Microsoft Azure	 OpenStack (Swift)
 Amazon S3	 SFTP / SCP	 DreamObjects
 Rackspace Cloud Files	 Google Cloud	 Email
 Google Drive	 Backblaze	
 Microsoft OneDrive	 WebDAV	

[You can send a backup to more than one destination with an add-on.](#)

If you choose no remote storage, then the backups remain on the web-server. This is not recommended (unless you plan to manually copy them to your computer), as losing the web-server would mean losing both your website and the backups in one event.

Include in files backup:

- Plugins
- Themes
- Uploads

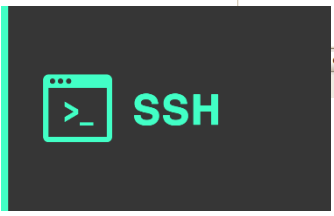
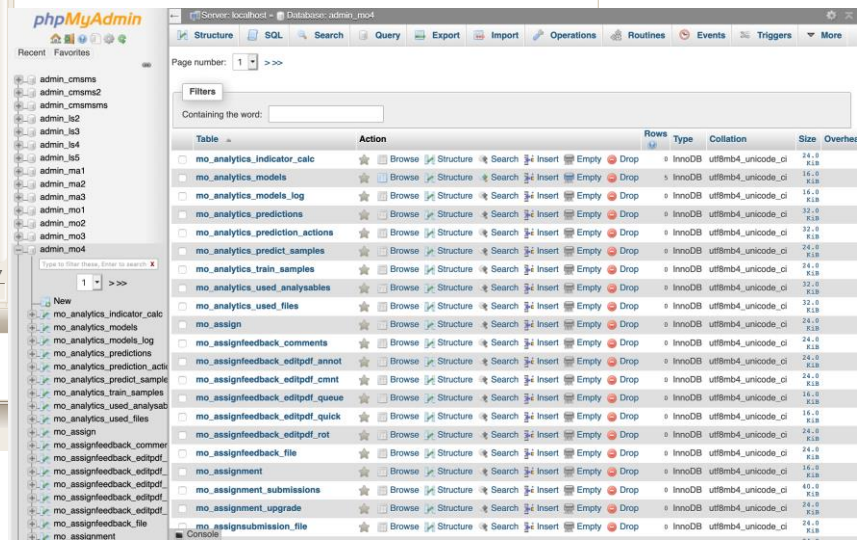
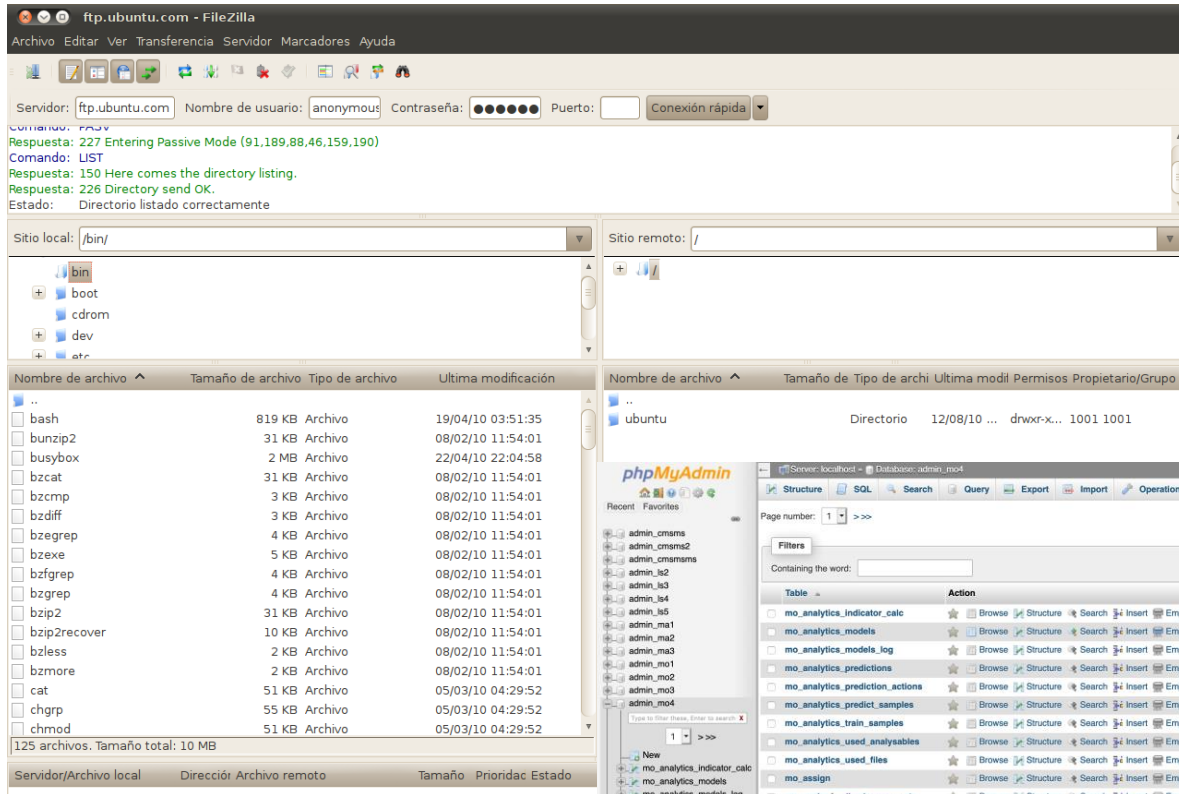
Exclude these:

Any other directories found inside wp-content

Exclude these:

The above directories are everything, except for WordPress core itself which you can download afresh from WordPress.org. [See also the "More Files" add-on from our shop.](#)





Dispositivos móviles

Cifras del año

En 2019, los productos y tecnologías de Kaspersky para dispositivos móviles detectaron:

- 3 503 952 paquetes de instalación maliciosos.
- 69 777 nuevos troyanos bancarios móviles.
- 68 362 nuevos troyanos de ransomware móviles.

Stalkerware y adware, las dos ciberamenazas más peligrosas

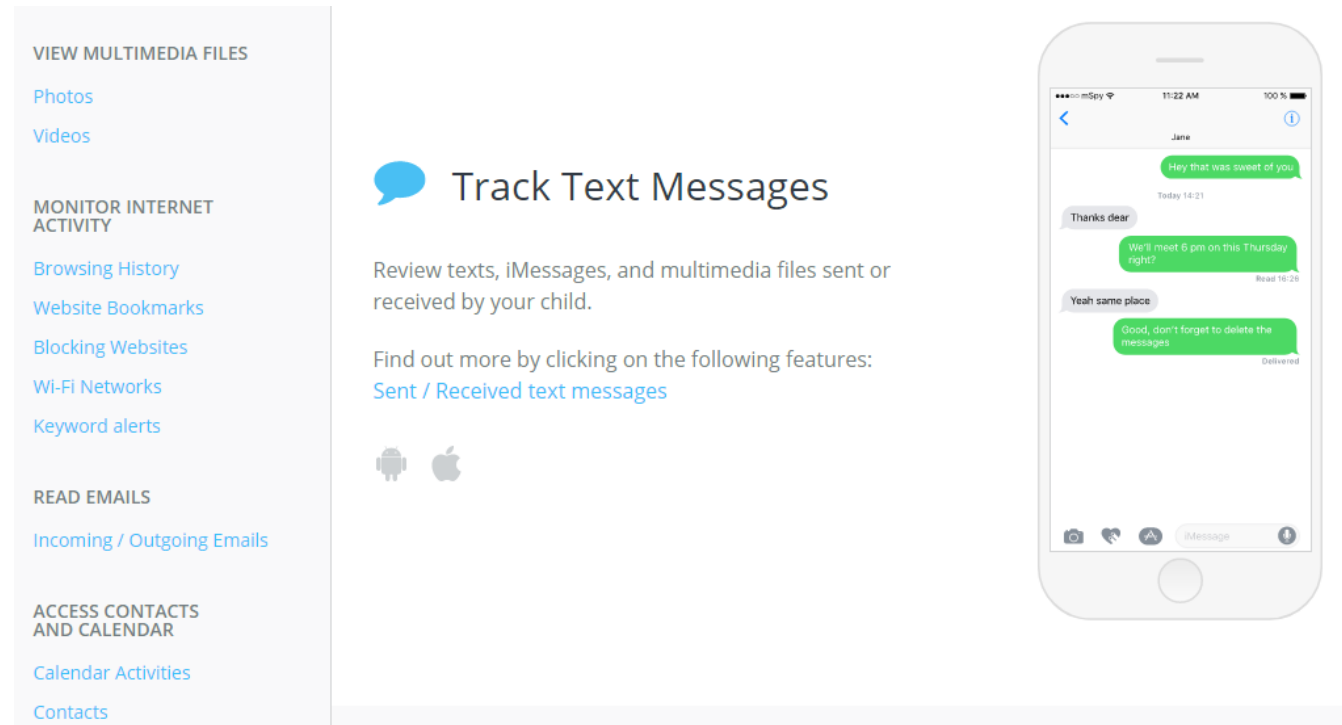
CheckPoint: «El hackeo al smartphone de Jeff Bezos no es un hecho aislado»



Aumentan los casos de mensajes en los que se suplanta la identidad de otra persona

El '**Stalkerware**' es un tipo de 'software' malicioso que permanece oculto en el teléfono de la víctima para extraer datos del dispositivo del usuario

Las aplicaciones tienen acceso a datos personales como la ubicación del dispositivo, el historial del navegador, conversaciones en redes sociales e incluso fotos.



The image shows a mobile application interface for tracking text messages. On the left, there is a sidebar menu with the following categories and links:

- VIEW MULTIMEDIA FILES
 - Photos
 - Videos
- MONITOR INTERNET ACTIVITY
 - Browsing History
 - Website Bookmarks
 - Blocking Websites
 - Wi-Fi Networks
 - Keyword alerts
- READ EMAILS
 - Incoming / Outgoing Emails
- ACCESS CONTACTS AND CALENDAR
 - Calendar Activities
 - Contacts

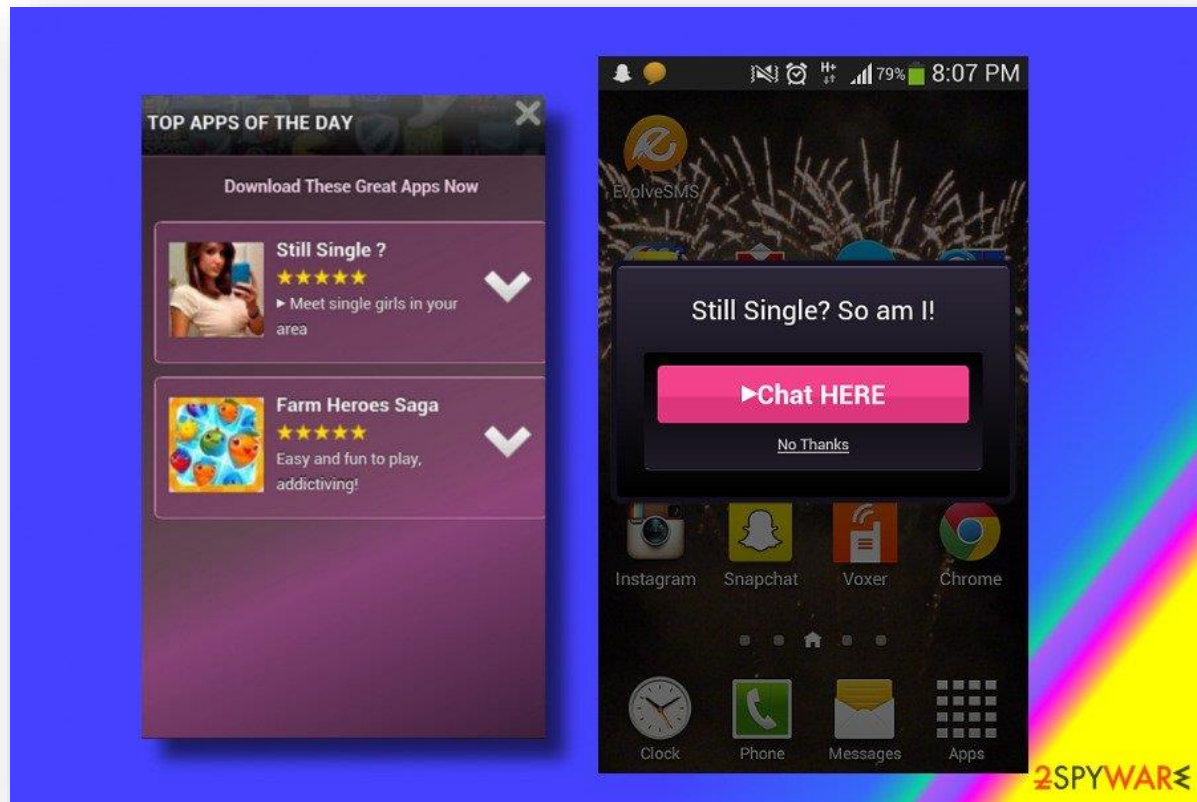
The main content area features a blue speech bubble icon and the title "Track Text Messages". Below the title, it says: "Review texts, iMessages, and multimedia files sent or received by your child." and "Find out more by clicking on the following features: [Sent / Received text messages](#)". At the bottom of this section are icons for Android and Apple.

On the right, there is a smartphone displaying a text message conversation with a contact named "Jane". The messages are as follows:

- Received: "Hey that was sweet of you"
- Sent: "Thanks dear"
- Received: "We'll meet 6 pm on this Thursday right?"
- Sent: "Yeah same place"
- Received: "Good, don't forget to delete the messages"

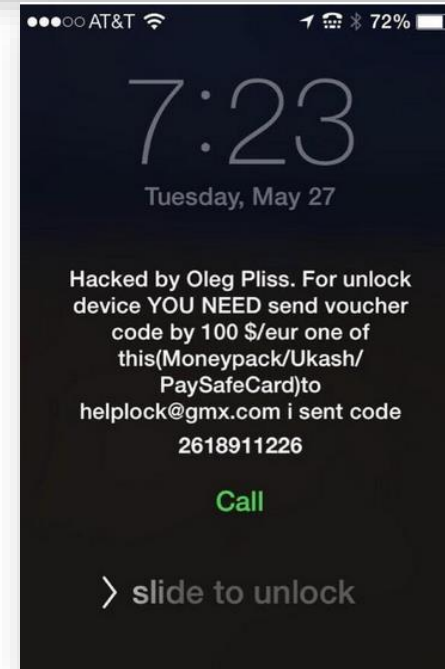
The smartphone screen also shows the time 11:22 AM, 100% battery, and a signal strength indicator.

Un **'adware'** recoge datos privados de los usuarios para después mostrarles anuncios que les interesen, e incitan a la **descarga de aplicaciones desde sitios no oficiales generalmente infectados.**



Nuevo ransomware para Android se distribuye a través de mensajes SMS

Investigadores de ESET descubren nueva familia de ransomware que afecta a usuarios de Android y que intenta distribuirse a través de mensajes SMS que son enviados a los contactos de sus víctimas



Docenas de apps con adware pululan en Google Play

ESET alerta de aplicaciones falsas de seis entidades financieras en Google Play

Malware encontrado en 8 aplicaciones de Google Play Store

Apple elimina 17 apps del App Store por tener malware





Un nuevo ataque de phishing mediante SMS afecta a los usuarios de Android



ENLACES MALICIOSOS INTENTAN QUE DESCARGUEMOS FALSAS APLICACIONES DE FORTNITE PARA ANDROID

Josep Albors | 27 Jun, 2018 | Android | No hay comentarios



Download Fortnite Thailand Free APK for android - YouTube



<https://www.youtube.com/watch?v=dpn2NO9j4dw>

31 may. 2018 - Subido por Fortnite italia

In this video I will show you how to play Fortnite on your android device. The first step you need to do is visit ...

Download fortnite APK for android mobile Thailand - YouTube



<https://www.youtube.com/watch?v=94Pzpuox-8A>

4 jun. 2018 - Subido por Fortnite italia

In this video I will show you how to play Fortnite on your android device. The first step you need to do is visit ...

Download Fortnite Thailand Free APK for android - скачать



<https://ruvid.net/video/видео-dpn2NO9j4dw.html>

31 may. 2018

In this video I will show you how to play Fortnite on your android device. The first step you need to do is visit ...

Fortnite Android - How to Download Fortnite Android - Open body phone



ohqu.com/fortnite-android-how-to-download-fortnite-android-6Y'u...

31 may. 2018

In this video tutorial I will show you how to download Fortnite on your favorite android device. The first step ...

Fortnite para Android en apk pure (Pre-registro) antes que la play ...



<https://www.hollywoodscenes.xyz/watch?v=OXETfnaN518>

20 abr. 2018 - Subido por GAME OVER

Fortnite para Android en apk pure Descargar Fortnite - Battle Royale APK (from ... Fortnite Descarguen ...

¿Crees que la seguridad es importante?
¿Crees que estás protegido?





DIGICOM

PLAN DE DIGITALIZACIÓN
DEL COMERCIO DE GIJÓN

