DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

JORNADAS DIVULGATIVAS
“Ciberseguridad en el comercio”

unión de comerciantes
Principado de Asturias

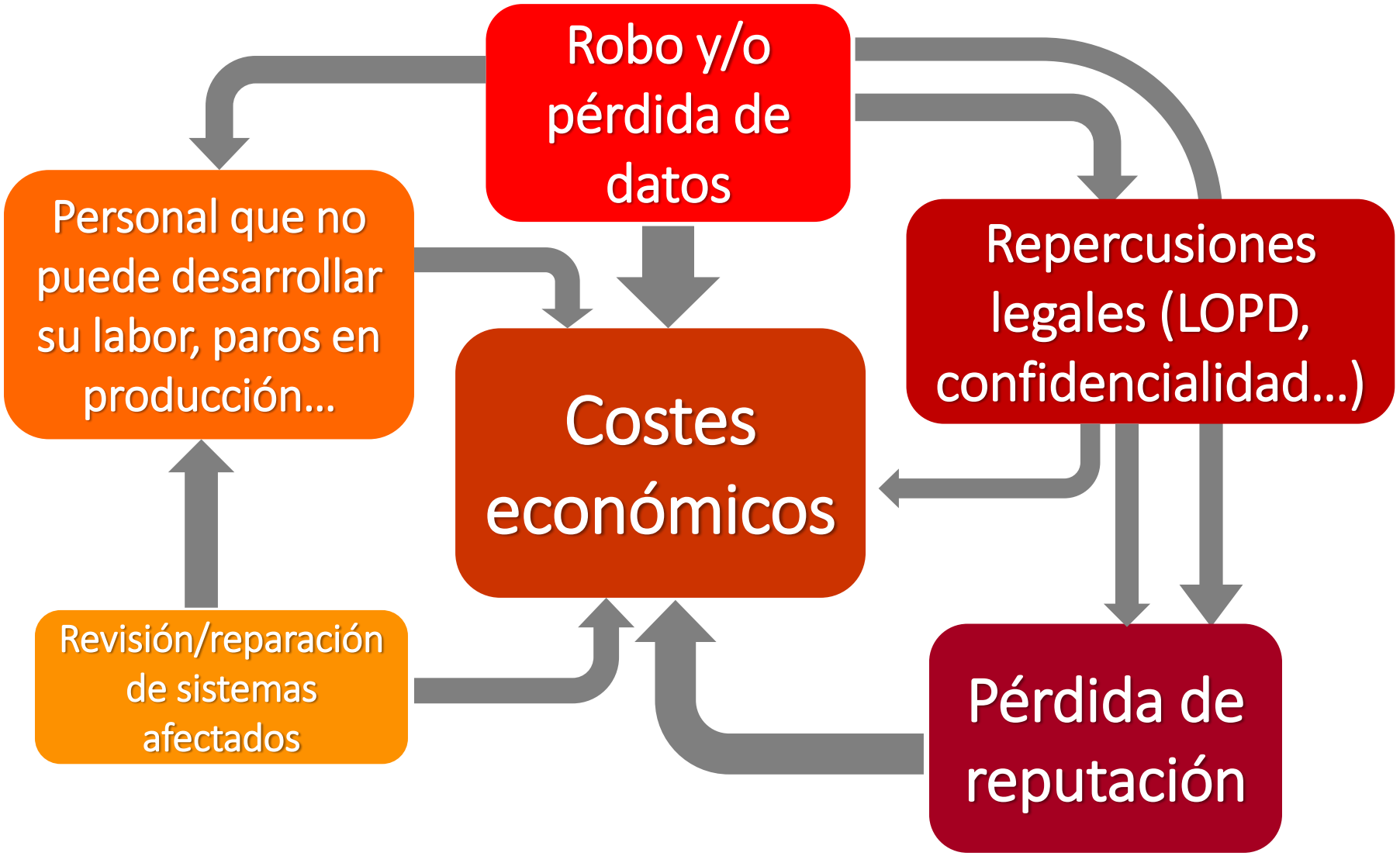
gijón reinicia 2020/2021

Gijón | impulsa

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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**


Robo y/o pérdida de datos
Personal que no puede desarrollar su labor, paros en producción…
Repercusiones legales (LOPD, confidencialidad…)
Costes económicos
Revisión/reparación de sistemas afectados
Pérdida de reputación

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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”

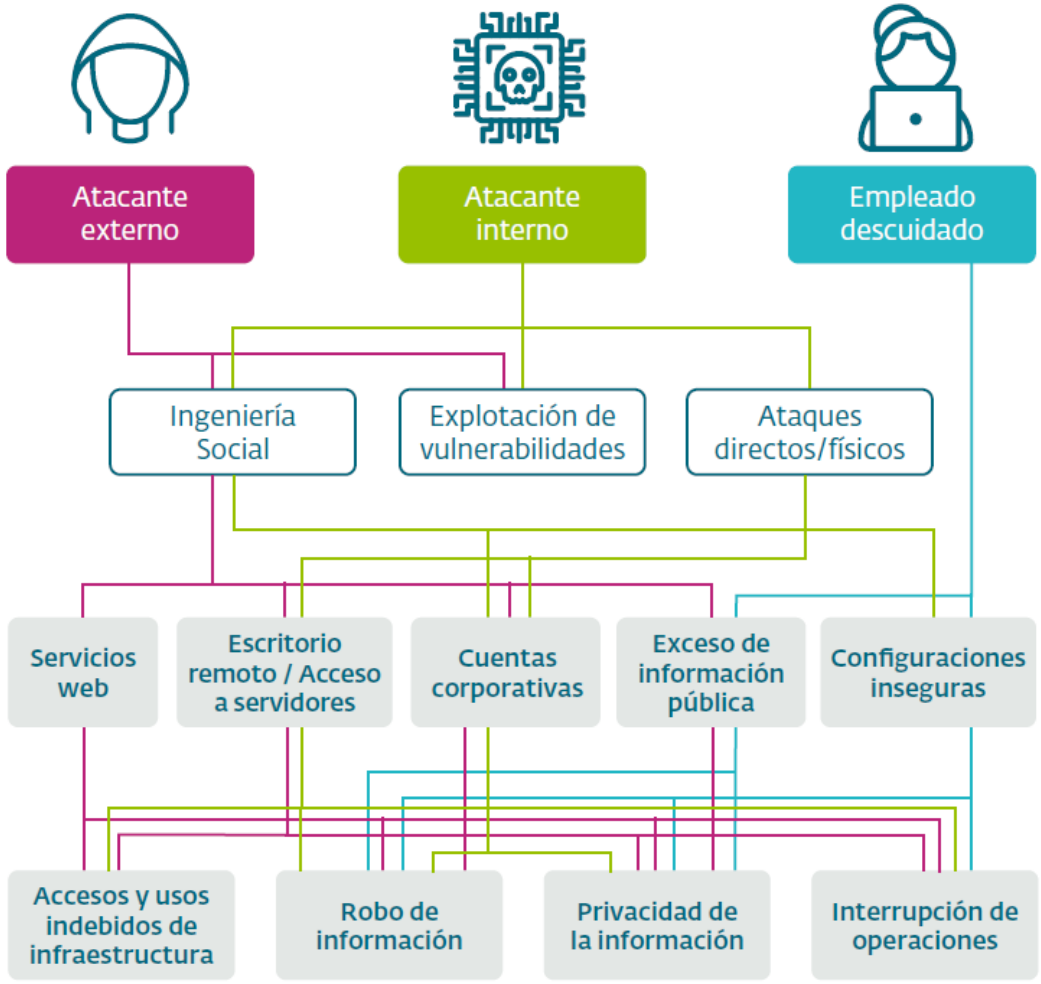
- Falso Mito #3: “tenemos un informático muy bueno” / “hemos comprado un antivirus de lo mejor”

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

- 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.

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Principales amenazas


Atacante externo
Atacante interno
Empleado descuidado
Ingeniería Social
Explotación de vulnerabilidades
Ataques directos/físicos
Servicios web
Escritorio remoto / Acceso a servidores
Cuentas corporativas
Exceso de información pública
Configuraciones inseguras
Accesos y usos indebidos de infraestructura
Robo de información
Privacidad de la información
Interrupción de operaciones

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

Mensajes electrónicos fraudulentos

¿Cómo nos pueden engañar?

- Phishing
- Suplantación de identidad
- Hoax

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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*.

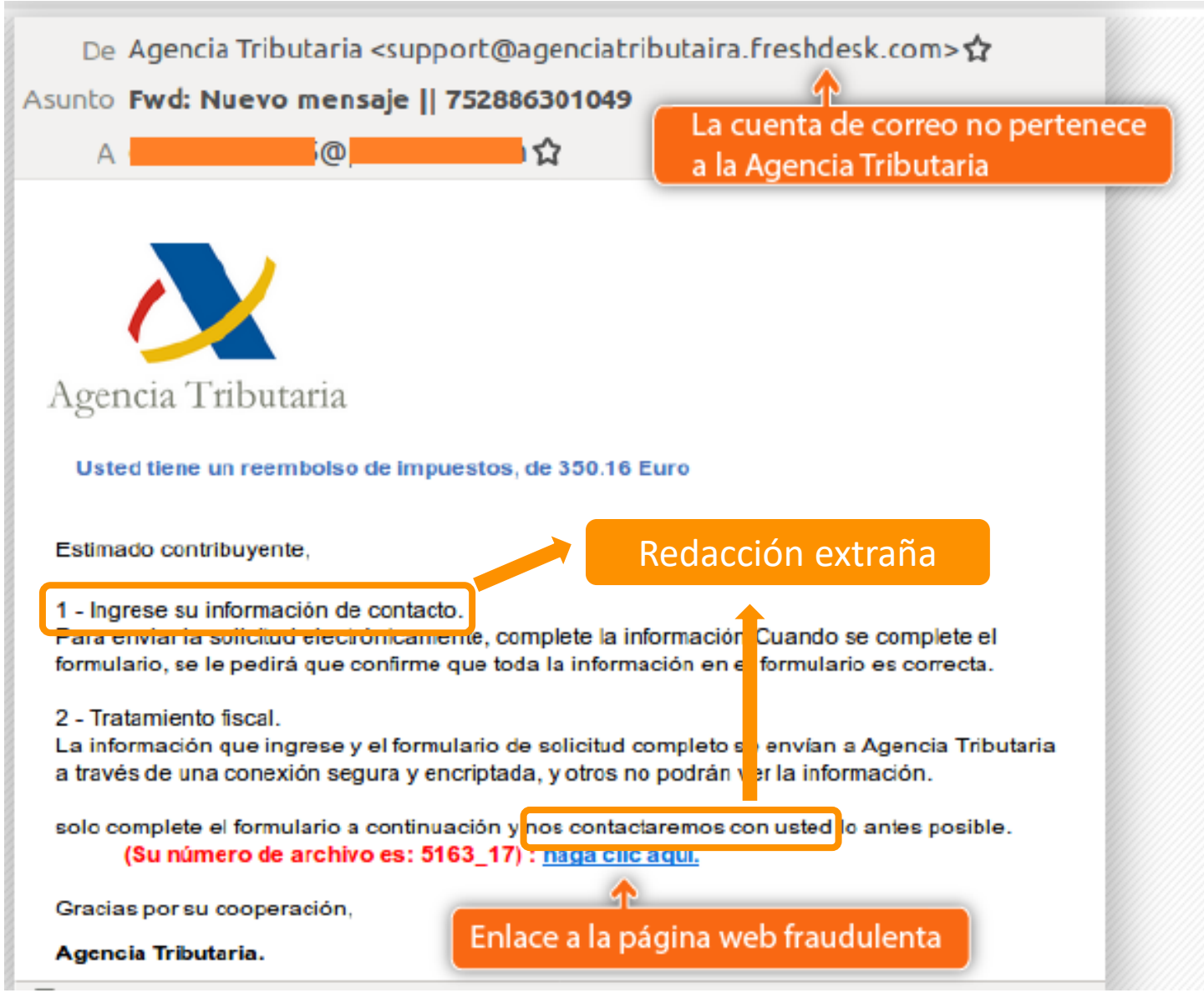
Si el usuario “muerde el anzuelo”, muchas veces será redirigido a un sitio web que también es idéntico al original, que en realidad está controlado por los atacantes.

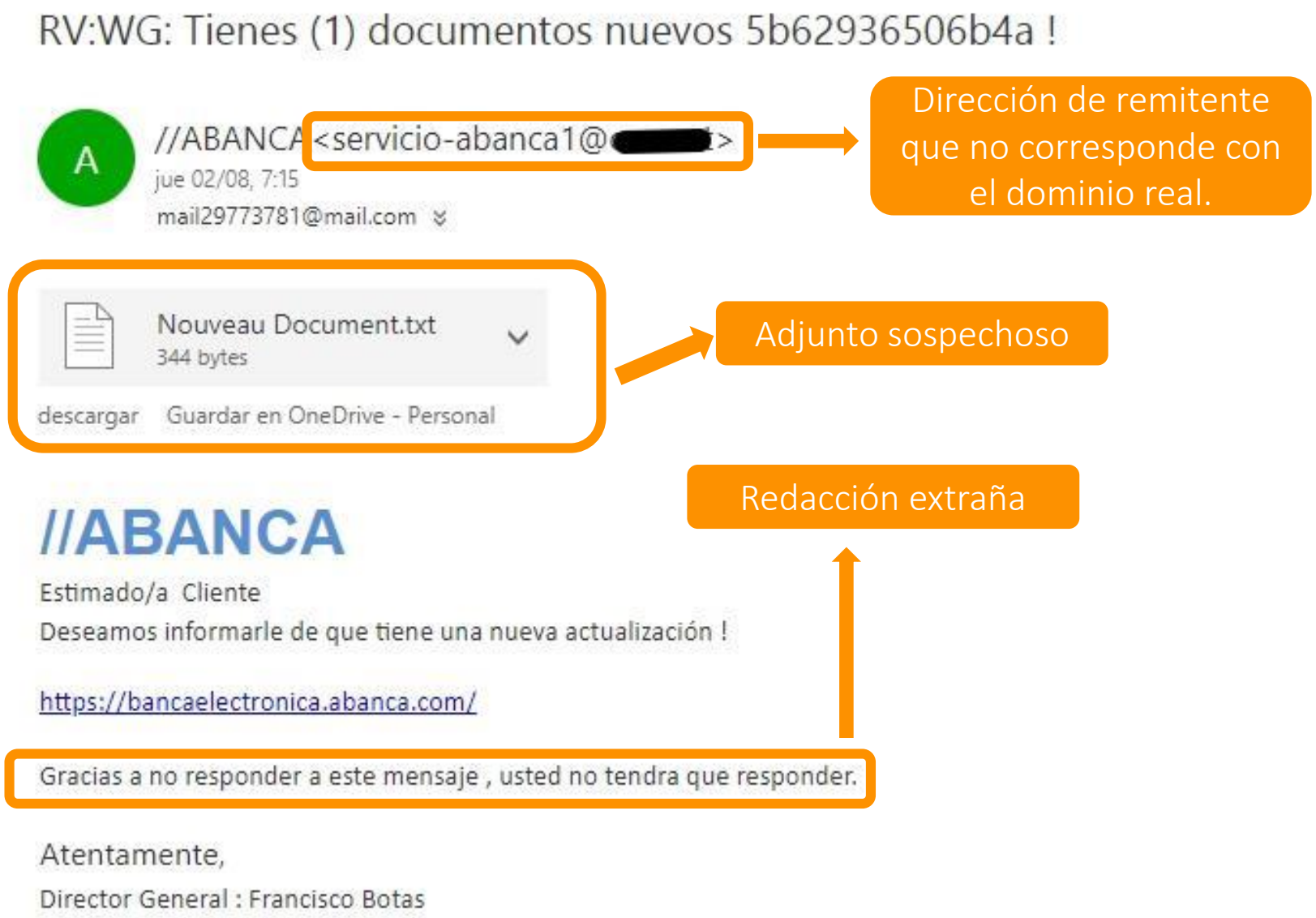
Por lo general, tanto mensajes como sitios web presentan una serie de elementos que nos ayudan a detectar su carácter fraudulento.

¿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.).

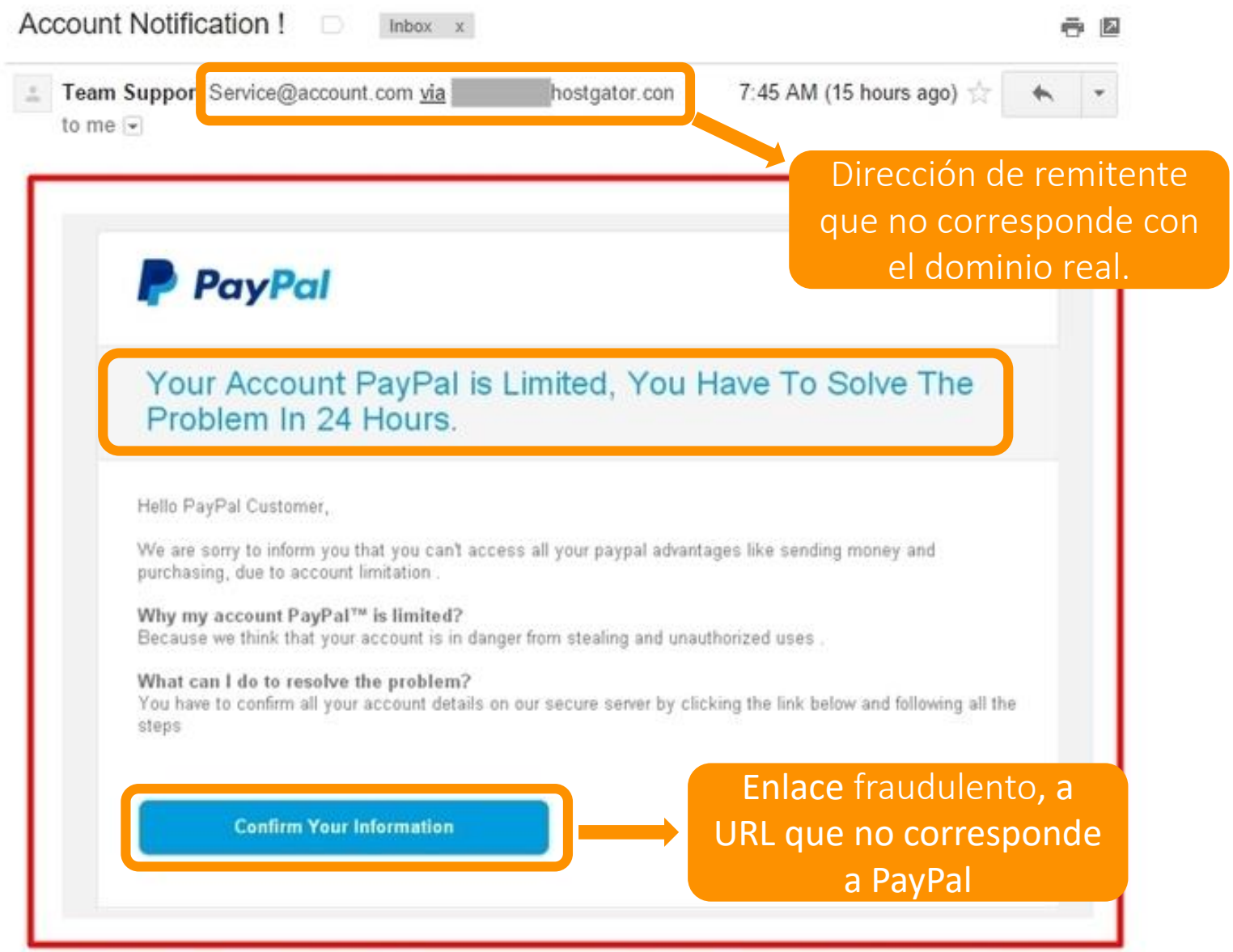
Por lo general, todas estas cuestiones están relacionadas en mayor o menor medida.

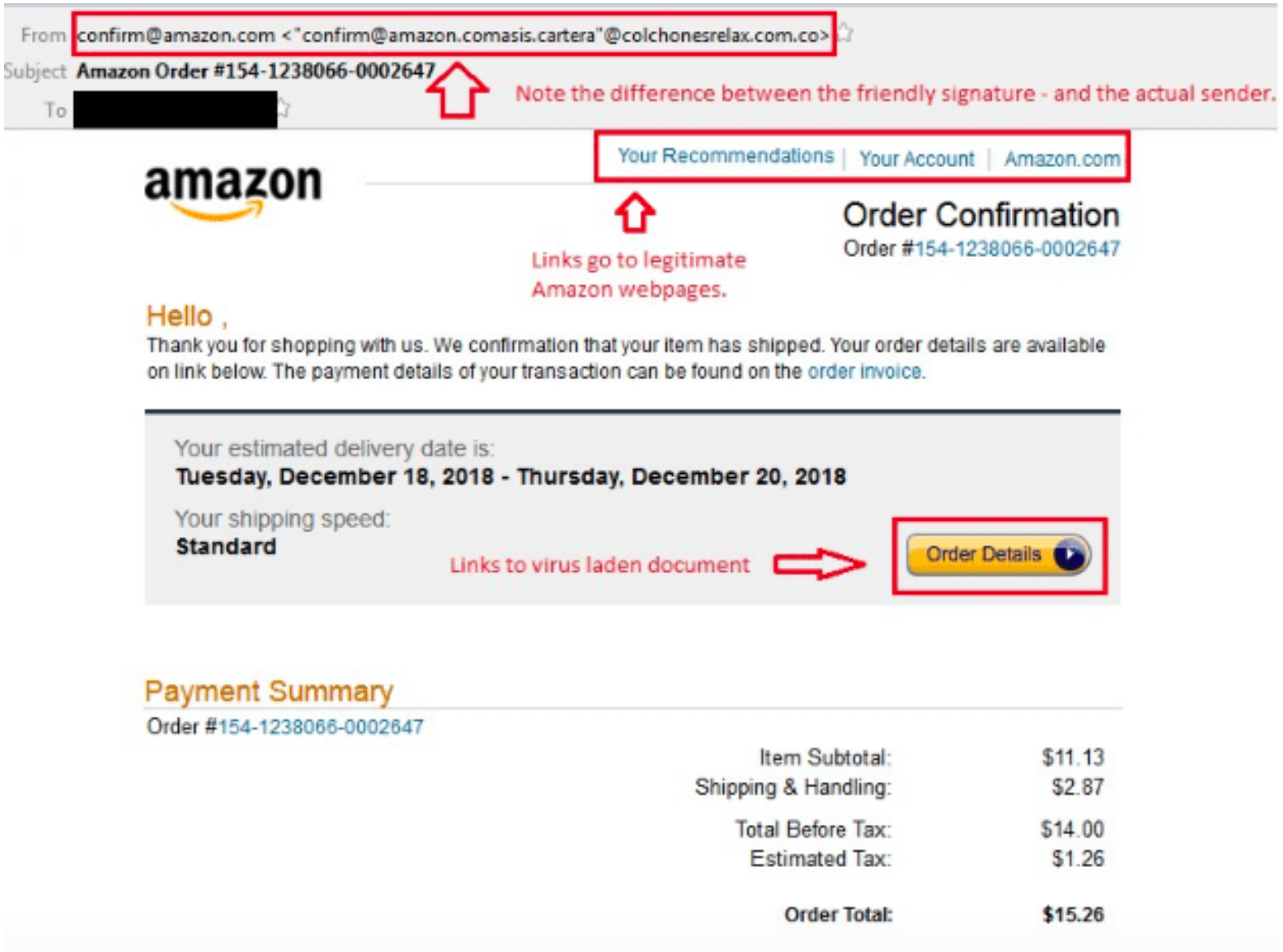

De Agencia Tributaria <support@agenciatributaira.freshdesk.com>
Asunto Fwd: Nuevo mensaje || 752886301049
A [redacted]
La cuenta de correo no pertenece a la Agencia Tributaria
Agencia Tributaria
Usted tiene un reembolso de impuestos, de 350.16 Euro
Estimado contribuyente,
Redacción extraña
1 - Ingrese 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) : haga clic aquí.
Enlace a la página web fraudulenta
Gracias por su cooperación,
Agencia Tributaria.

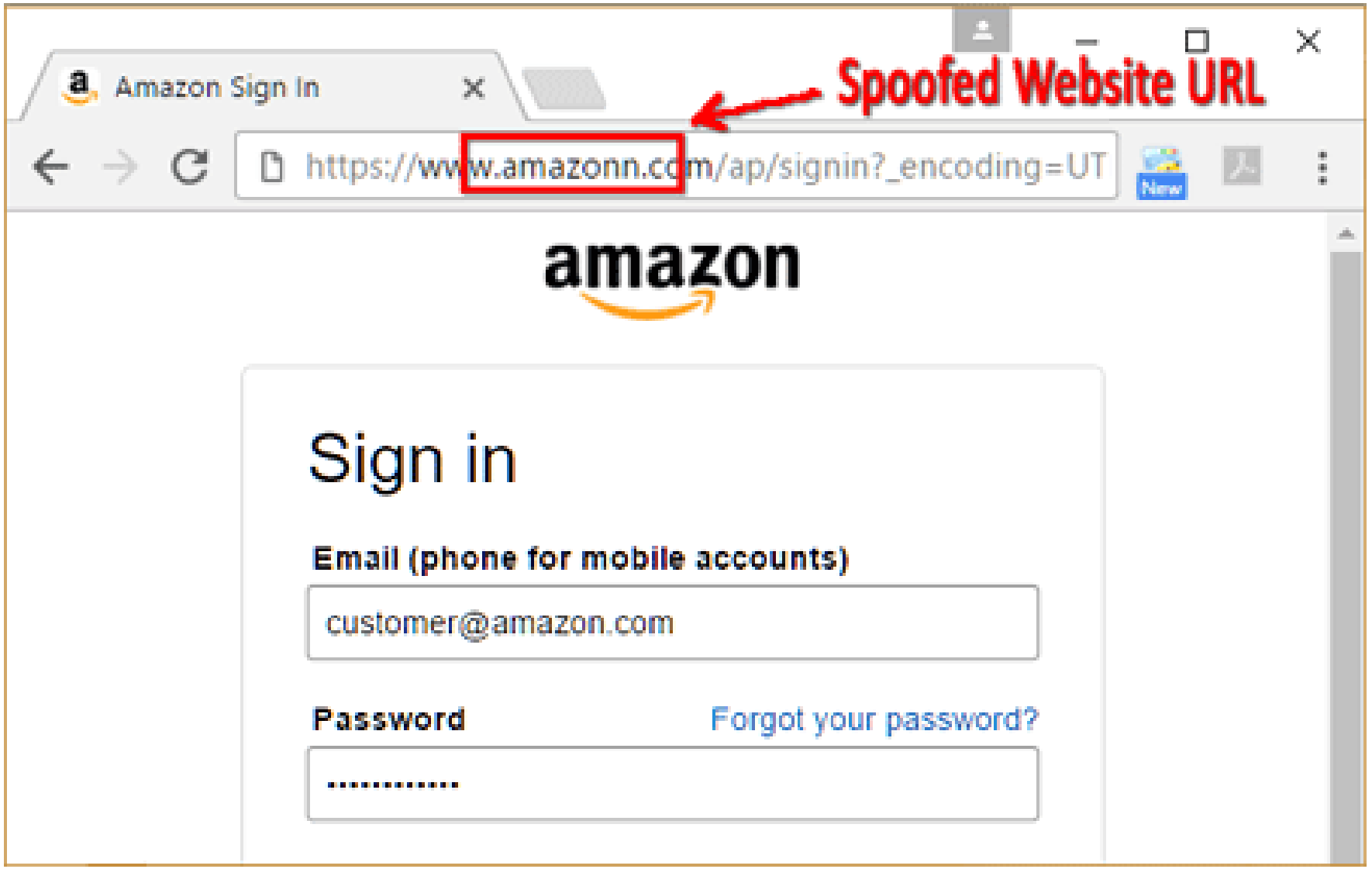

RV:WG: Tienes (1) documentos nuevos 5b62936506b4a !
A
//ABANCA <servicio-abanca1@[redacted]>
jue 02/08, 7:15
mail29773781@mail.com
Dirección de remitente que no corresponde con el dominio real.
Nouveau Document.txt
344 bytes
descargar Guardar en OneDrive - Personal
Adjunto sospechoso
Redacción extraña
//ABANCA
Estimado/a Cliente
Deseamos informarle de que tiene una nueva actualización !
https://bancaelectronica.abanca.com/
Gracias a no responder a este mensaje , usted no tendra que responder.
Atentamente,
Director General : Francisco Botas

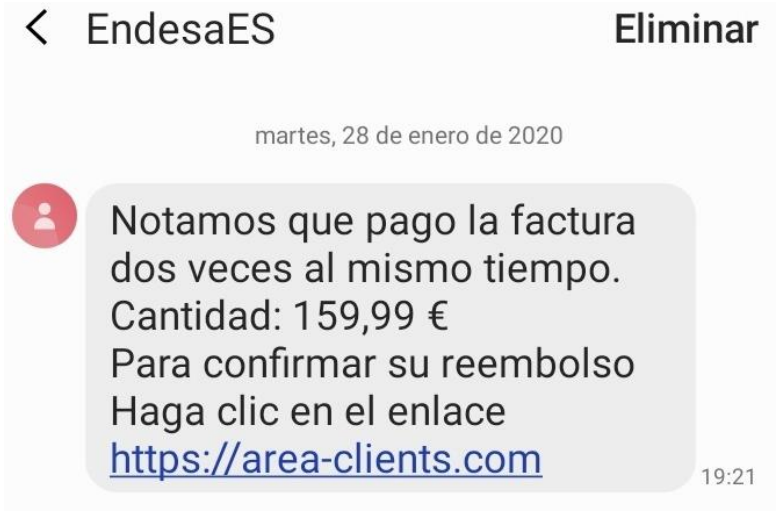

Responder
Reenviar
Archivar
No deseado
Eliminar
Más
De Online Bbva.es <info@graexcon.com>
Asunto Bbva(es): verifique su cuenta introduciendo...
A undisclosed-recipients:;
Dirección de remitente que no corresponde con el dominio real.
BBVA
Hola, su cuenta en línea ha sido suspendida temporalmente.
Necesitamos que verifique su cuenta introduciendo sus credenciales y SMS verificacion .
Asegurese de introducir sus datos correctamente y su numero de telefono esta cerca de usted para verificar su identidad por el telefono adormecer: .
1- Acceder a mi
2- Ingrese el codigo de verificacion de SMS en la pagina de verificacion
3- inicie sesion y siga los pasos haciendo clic a continuacion:
Acceder a mi
Nota: Si usted no activa su cuenta en el próximo 24Hours usted será suspendido de nuestros servicios bancarios.
Solicitud que no se ajusta a la forma habitual de proceder
URL de destino sospechosa en el botón de acceso
Redacción extraña
http://fortyone.web.id/dist/re/


Expiracion del correo electrónico [redacted].es - Unicode (UTF-8)
Archivo
Mensaje
Expiracion del correo electrónico [redacted]@[redacted].es
Ansys Servidor de Correo (webmail_admin@ul[redacted]ring.co.uk)
Agregar contacto
15/01/2020 9:43
Para: [redacted];
Dirección de remitente que no corresponde con el dominio real.
arsys
Estimado cliente,
Queremos informarle que la fecha de expiración del correo electrónico [redacted].es será el 16 de Enero 2020.
Correo electrónico
[redacted].es
Fecha de expiración
16.01.2020
Cuando la fecha de expiración haya transcurrido, los siguientes servicios serán deshabilitados:
- Envió y recepción de mensajes
- Las aplicaciones web que han sido vinculadas con su cuenta
Renueva ahora
La renovación es gratis
Enlace fraudulento, a URL que no corresponde a Ansys
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.


Account Notification !
Inbox x
Team Suppor
Service@account.com via hostgator.con
7:45 AM (15 hours ago)
to me
Dirección de remitente que no corresponde con el dominio real.
PayPal
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.
amazon
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


Amazon Sign In
Spoofed Website URL
https://www.amazonn.com/ap/signin?_encoding=UT
amazon
Sign in
Email (phone for mobile accounts)
customer@amazon.com
Password
Forgot your password?



¿Cómo podemos detectarlos?

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

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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 Tecnológic <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 Tecnológic

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

URL sospechosa

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

Salutacions,

Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológic

Teléfono 94 418 23 05 Extensión 5836

Datos de contacto falsos

Dirección de remitente que no corresponde con el real.

De: Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológic <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 Tecnológic mariano.gonzalez@ctic.es

32% 12:29

Bandeja de ent...

Mariano González [Centro SAT de Llane...

Hoy 11:02

1 archivo adjunto

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 Tecnológic

Teléfono 95 877 58 30 Extensión 4990

Datos de contacto falsos

1 archivo adjunto | 251 KB

Adjunto sospechoso

telecable 17:42 51 %

17

Factura P-4388

Hola,

Adjunto envío la factura correspondiente al mes.

Salutacions,

Mariano González [Centro SAT de Llanera | CTIC Centro Tecnológic

Tel. +34 968 14 03

mariano.gonzalez@ctic.es

FA_P-4388.doc

290 KB

Favor urgente, solicito confidencialidad

Recibidos ×

CEO <maria.garcia@habitos-inseguros.com> 9:52 (hace 4 minutos)
<para juan.perez@habitos-inseguros.com>

Recurro 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 maquinara 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**

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

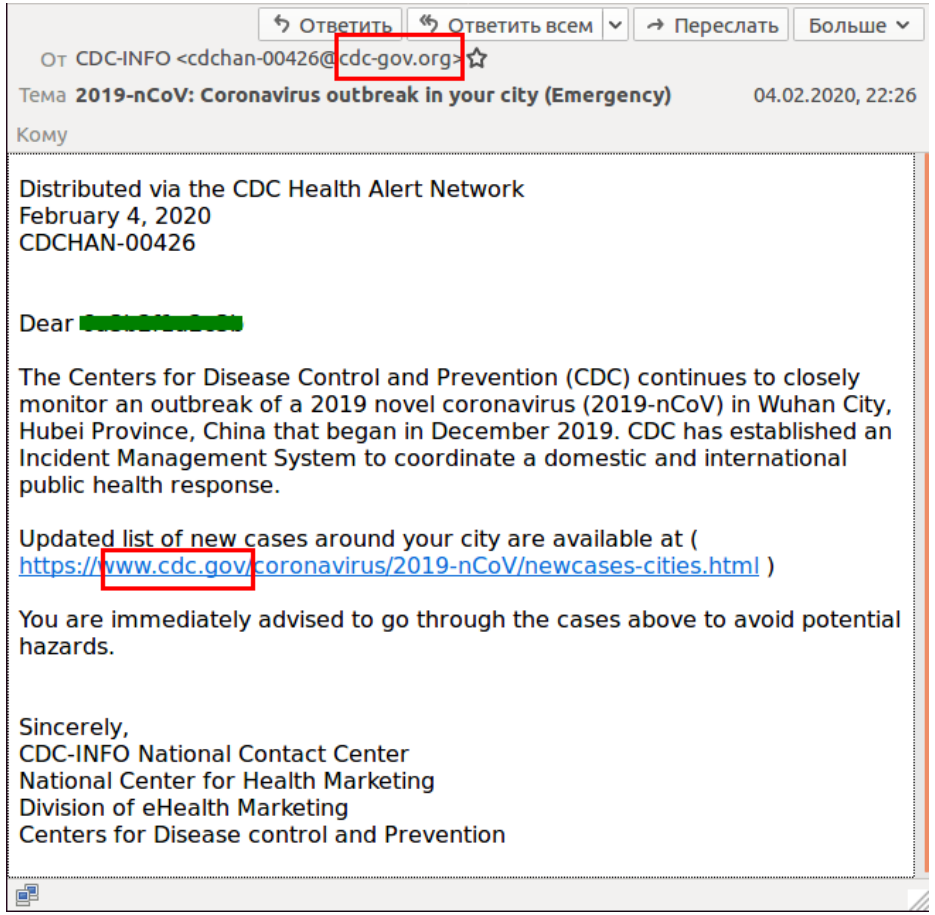
¿Cómo reconocer un bulo?

- 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



Ответить | Ответить всем | Переслать | Больше

От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

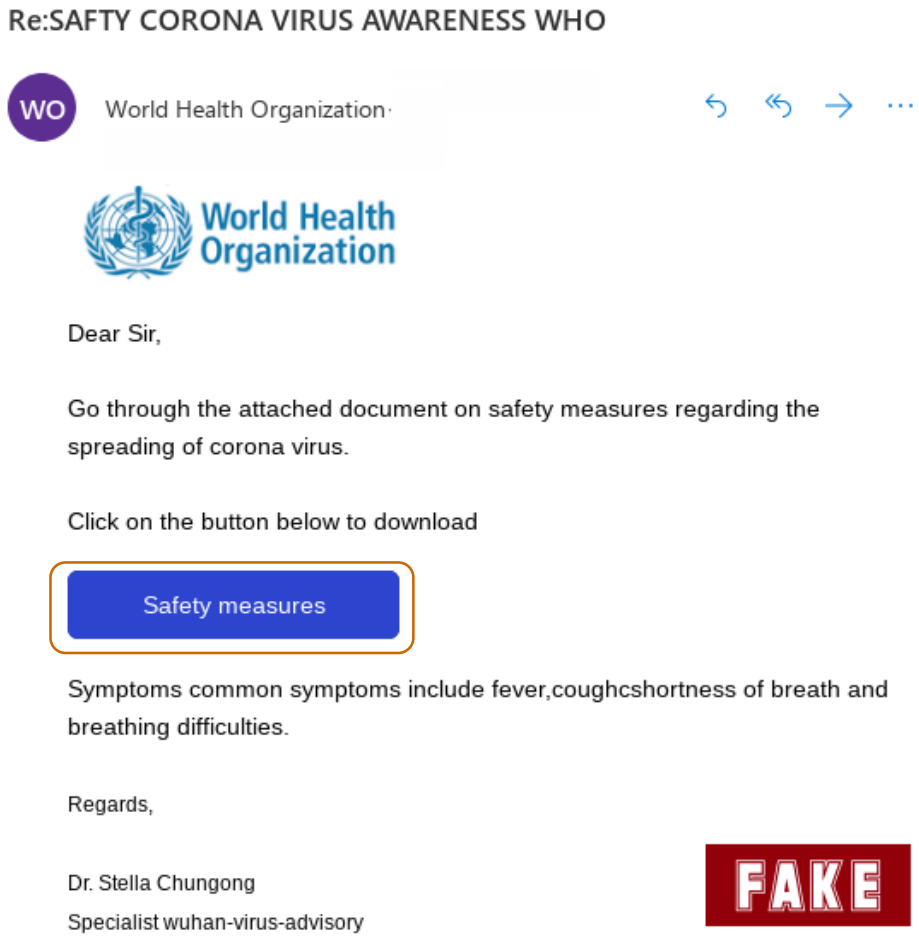
Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization

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,coughcshortness of breath and breathing difficulties.

Regards,

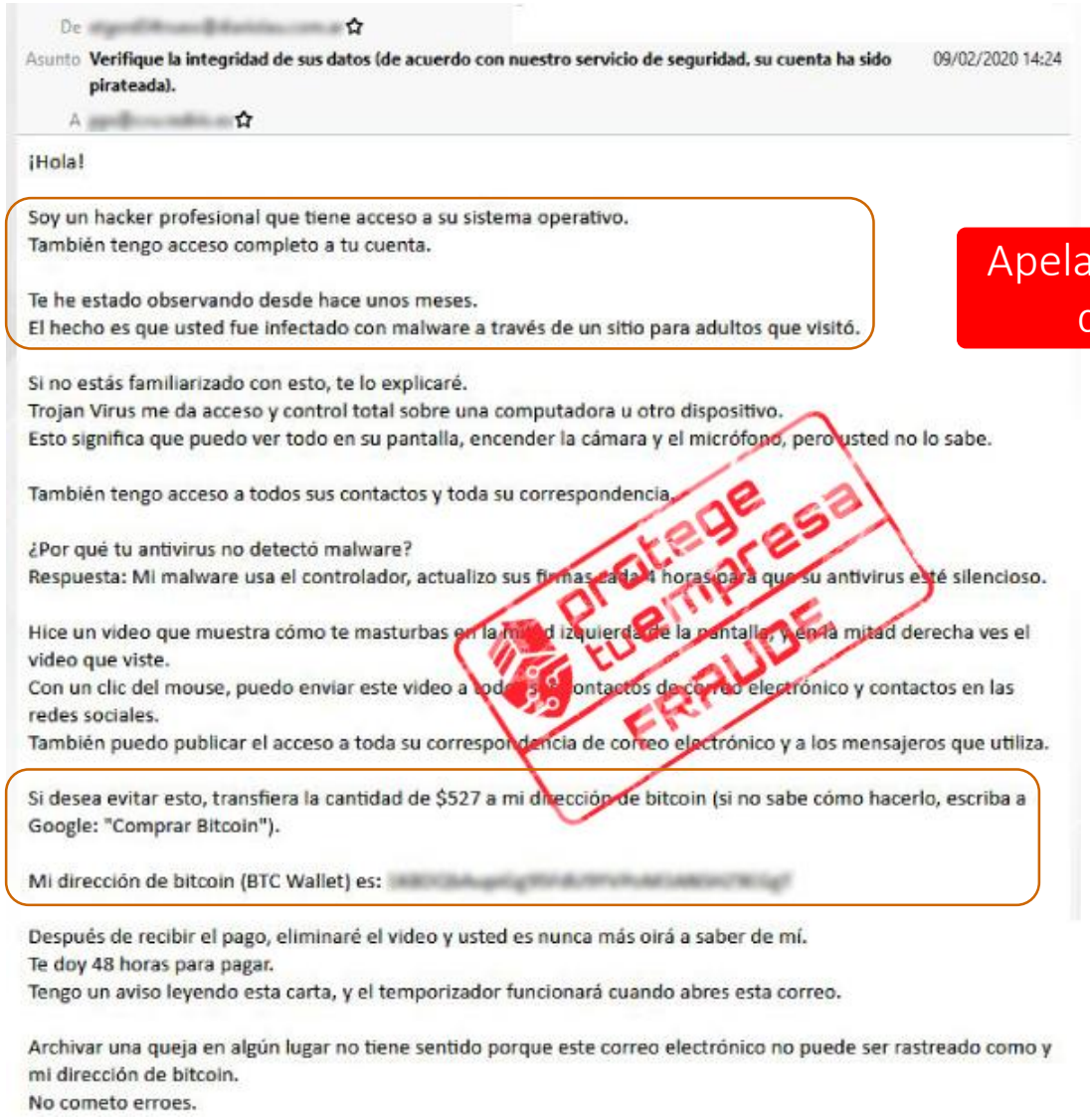
Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE

Sextorsión

Redacción extraña

Apela a la vergüenza del usuario



De [redacted]

Asunto **Verifique la integridad de sus datos (de acuerdo con nuestro servicio de seguridad, su cuenta ha sido pirateada).** 09/02/2020 14:24

A [redacted]

¡Hola!

Soy un hacker profesional que tiene acceso a su sistema operativo.
También tengo acceso completo a tu cuenta.

Te he estado observando desde hace unos meses.
El hecho es que usted fue infectado con malware a través de un sitio para adultos que visitó.

Si no estás familiarizado con esto, te lo explicaré.
Trojan Virus me da acceso y control total sobre una computadora u otro dispositivo.
Esto significa que puedo ver todo en su pantalla, encender la cámara y el micrófono, pero usted no lo sabe.

También tengo acceso a todos sus contactos y toda su correspondencia.

¿Por qué tu antivirus no detectó malware?
Respuesta: Mi malware usa el controlador, actualizo sus firmas cada 4 horas para que su antivirus esté silencioso.

Hice un video que muestra cómo te masturbas en la mitad izquierda de la pantalla, y en la mitad derecha ves el video que viste.
Con un clic del mouse, puedo enviar este video a todos sus contactos de correo electrónico y contactos en las redes sociales.
También puedo publicar el acceso a toda su correspondencia de correo electrónico y a los mensajeros que utiliza.

Si desea evitar esto, transfiera la cantidad de $527 a mi dirección de bitcoin (si no sabe cómo hacerlo, escriba a Google: "Comprar Bitcoin").

Mi dirección de bitcoin (BTC Wallet) es: [redacted]

Después de recibir el pago, eliminaré el video y usted es nunca más oirá a saber de mí.
Te doy 48 horas para pagar.
Tengo un aviso leyendo esta carta, y el temporizador funcionará cuando abres esta correo.

Archivar una queja en algún lugar no tiene sentido porque este correo electrónico no puede ser rastreado como y mi dirección de bitcoin.
No cometo erroes.

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: -

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

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.

Apela a la vergüenza del usuario

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!

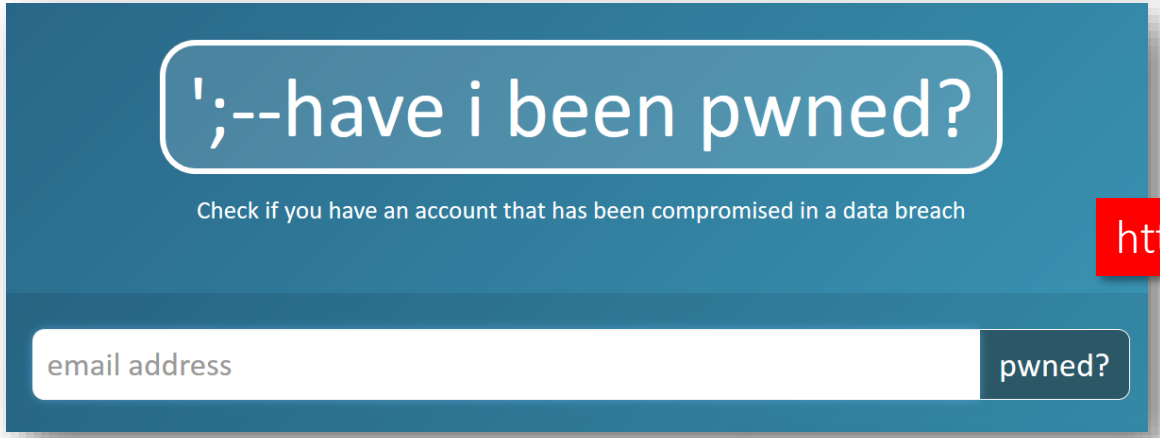
I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

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.

¿Cómo saber si mis contraseñas han sido robadas?



https://haveibeenpwned.com/

https://monitor.firefox.com/

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

¿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

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

¿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.

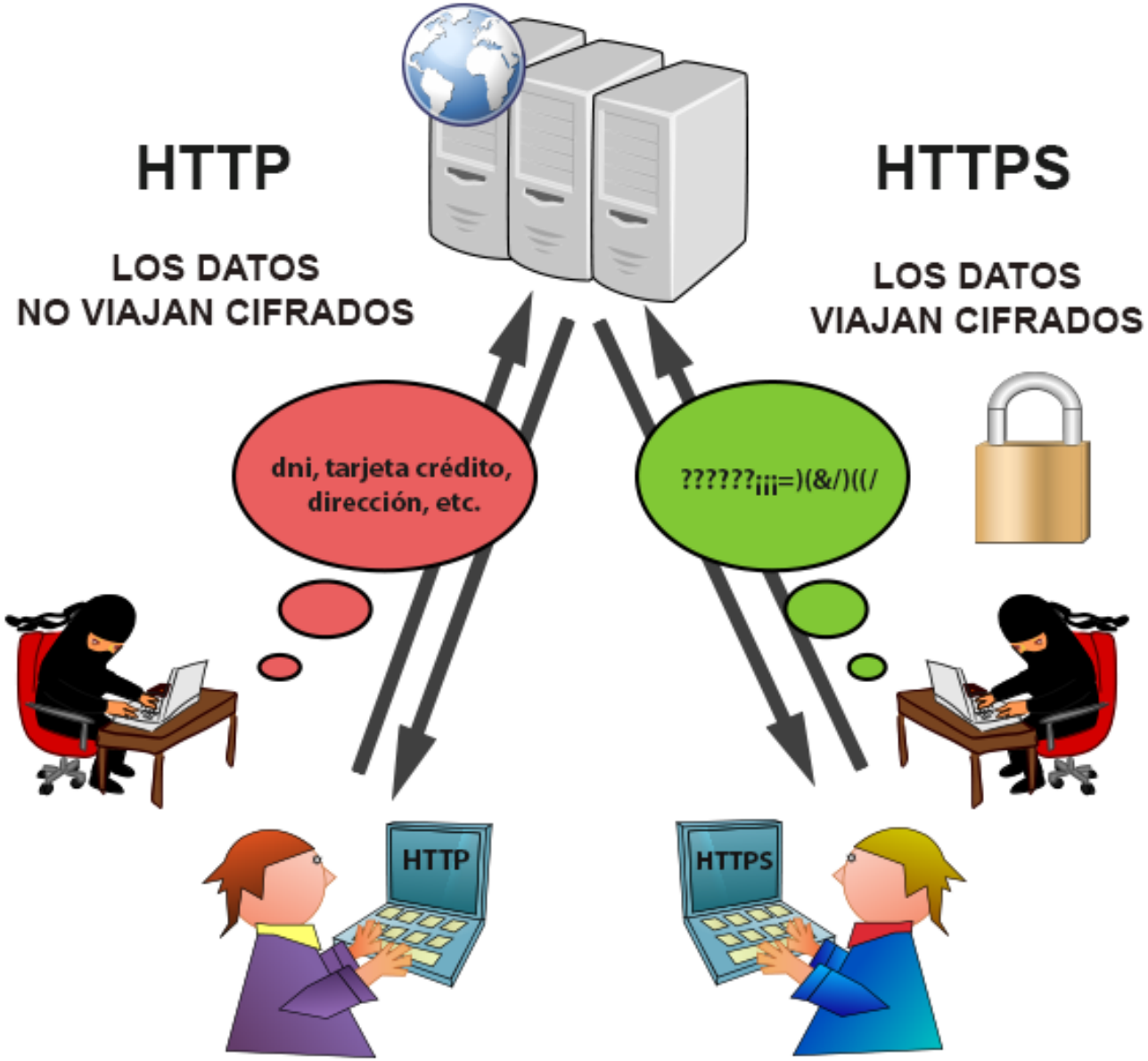
¿Sabrías detectar ahora un correo fraudulento?

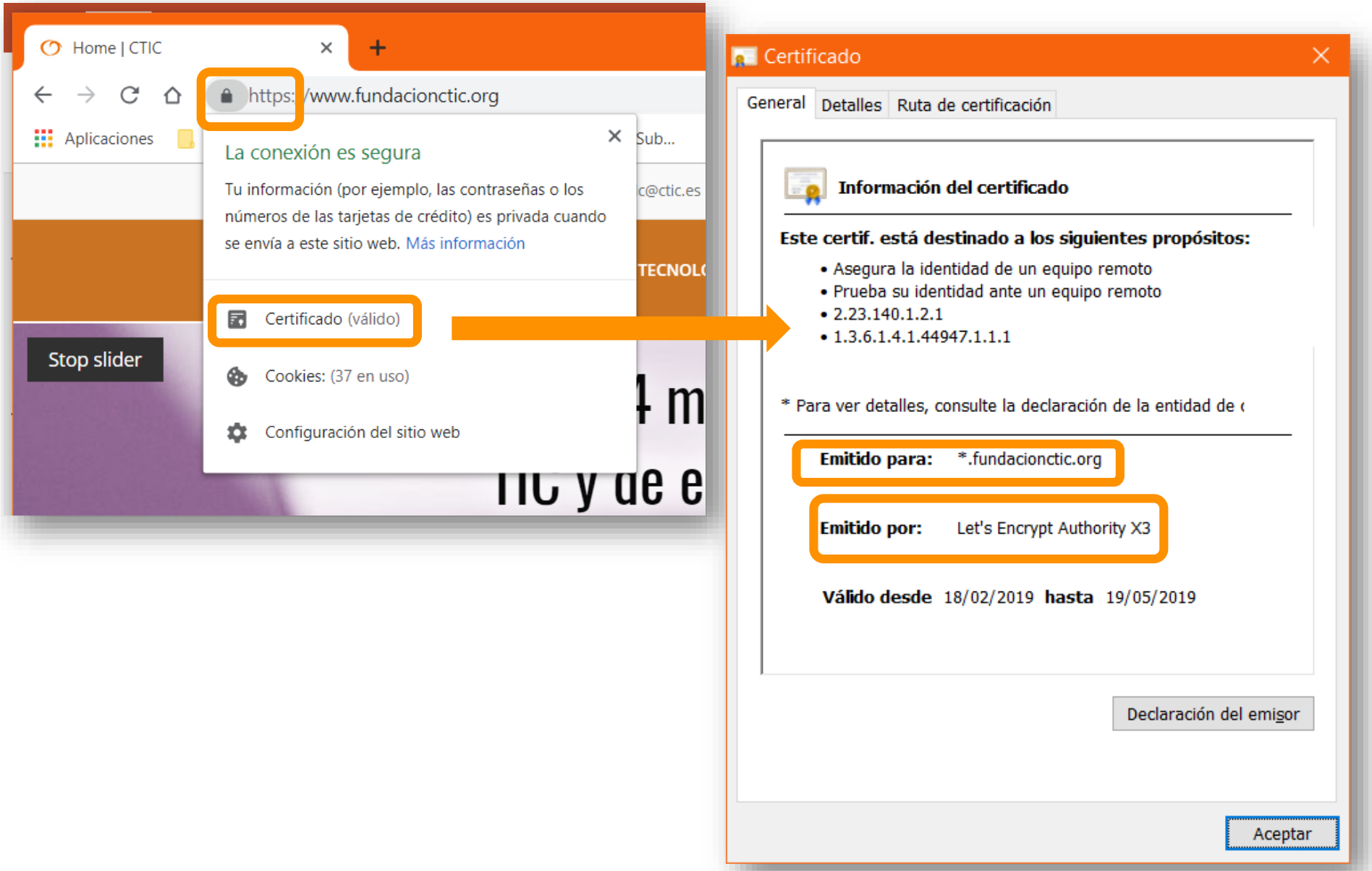
https://phishingquiz.withgoogle.com/

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

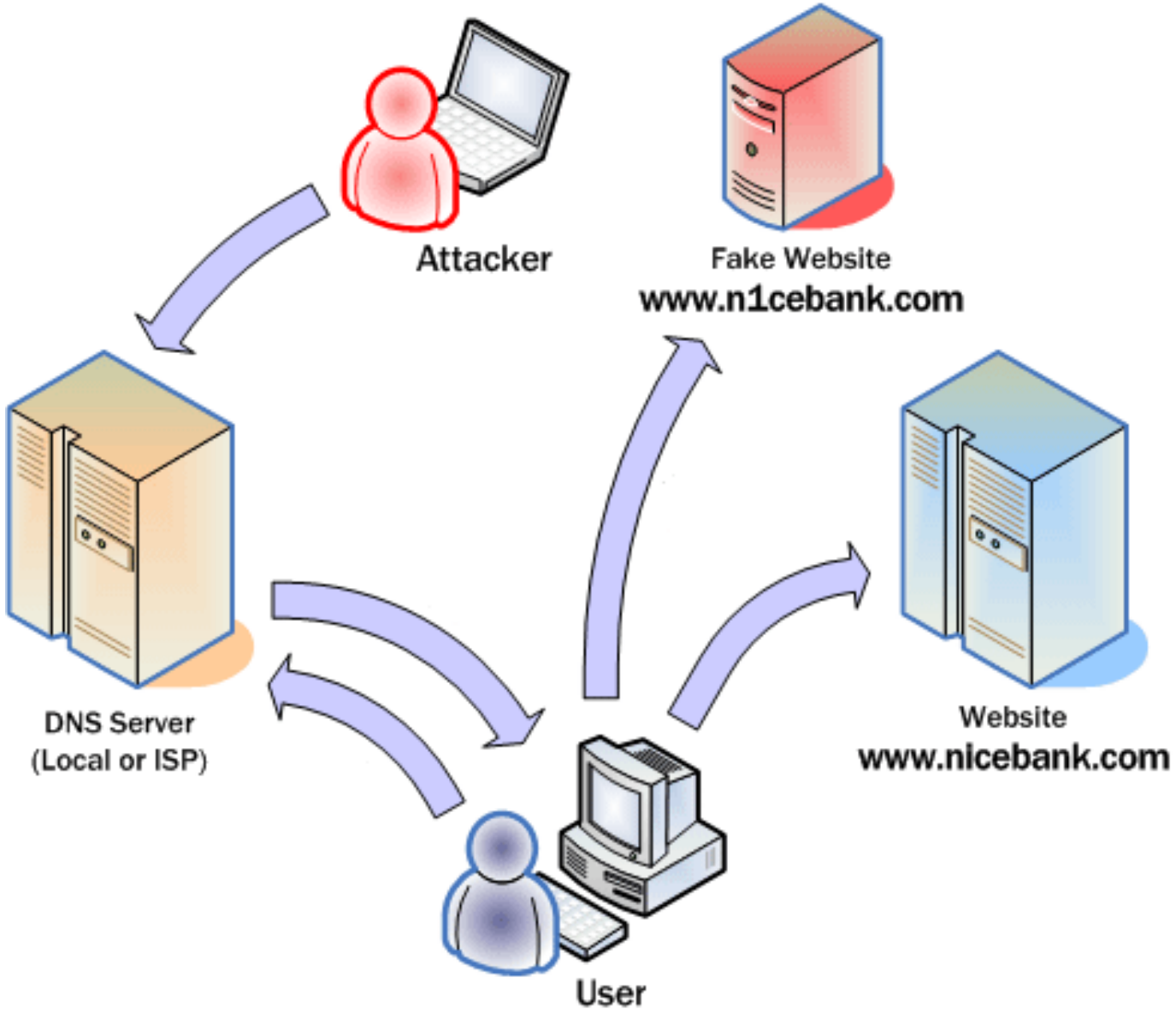
Sitios web inseguros

La importancia de la navegación segura mediante https

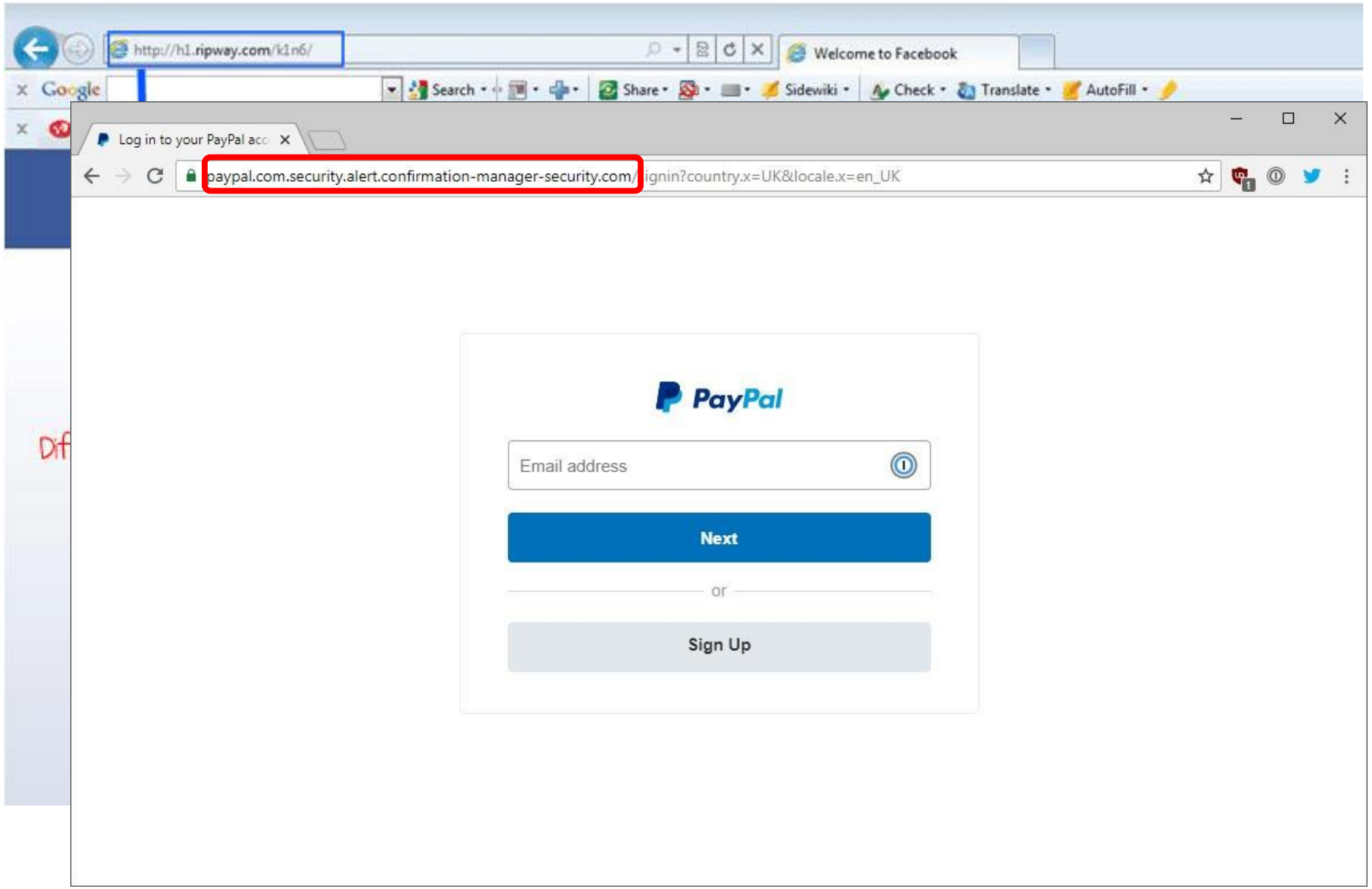



Home | CTIC
https://www.fundacionctic.org
Aplicaciones
La conexión es segura
Tu información (por ejemplo, las contraseñas o los números de las tarjetas de crédito) es privada cuando se envía a este sitio web. Más información
Certificado (válido)
Cookies: (37 en uso)
Configuración del sitio web
Stop slider
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
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!!



DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Software malicioso

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.).

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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.

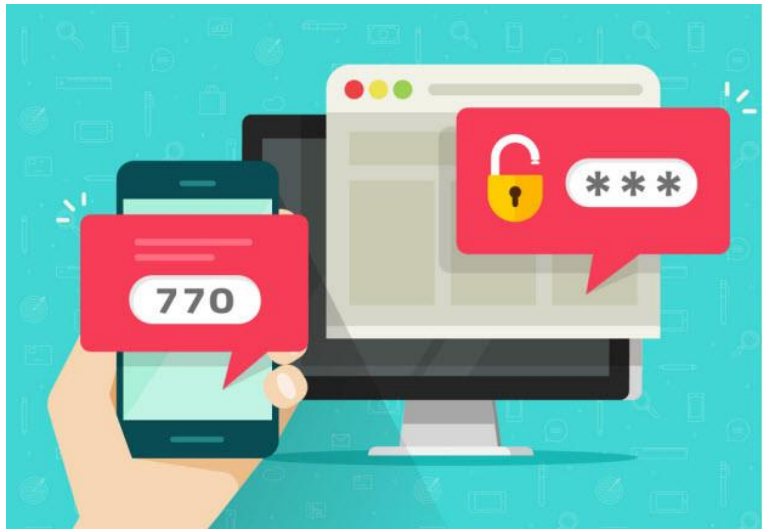
DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

La importancia de las contraseñas y su fortaleza

Identificación de doble factor

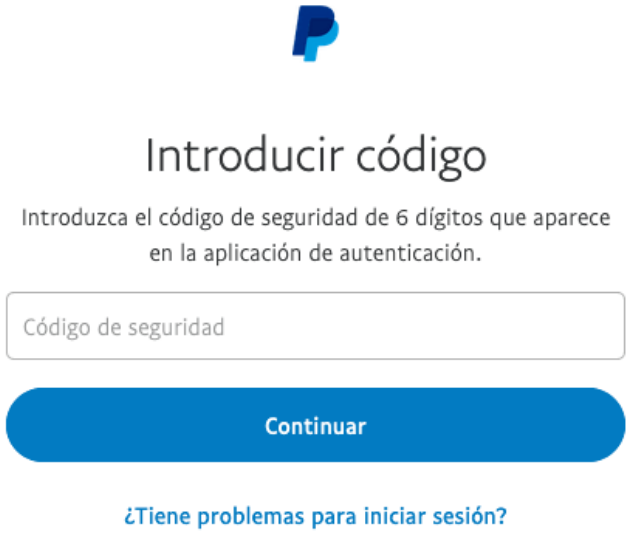
Doble factor de autenticación: ¿qué es y por qué lo necesito?

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**.



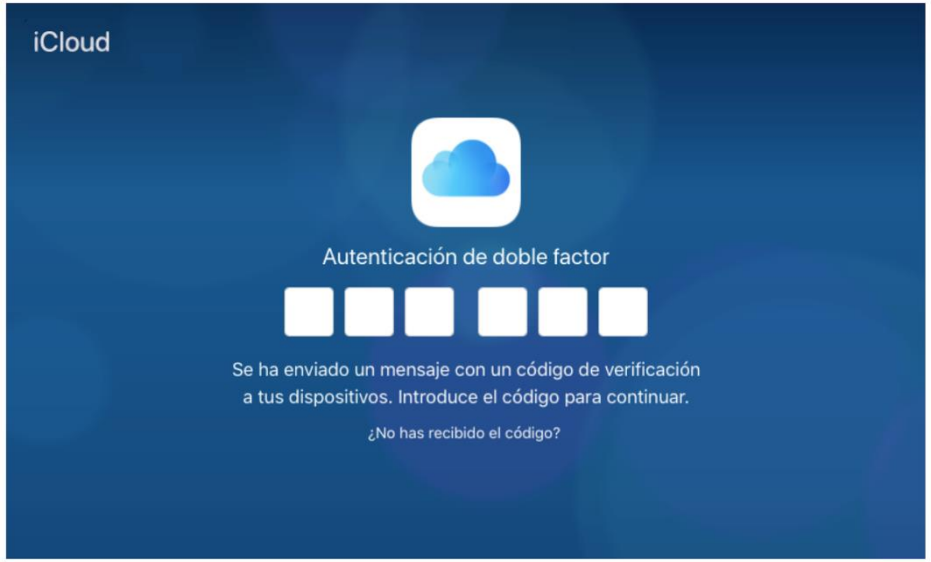
DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

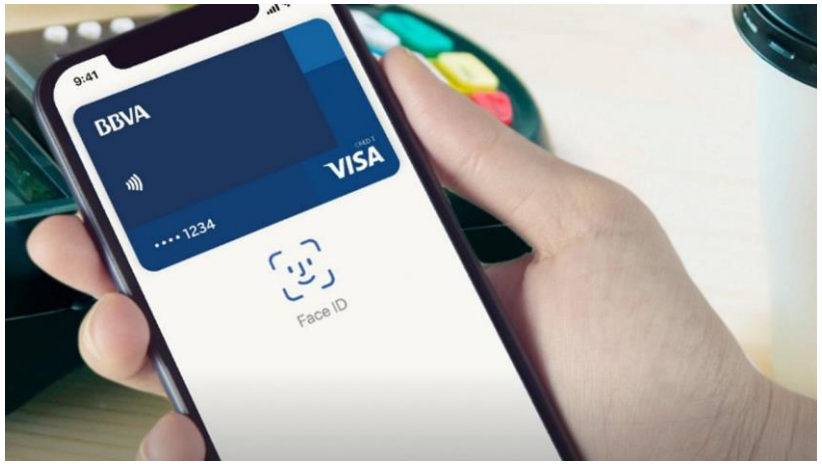
Identificación de doble factor

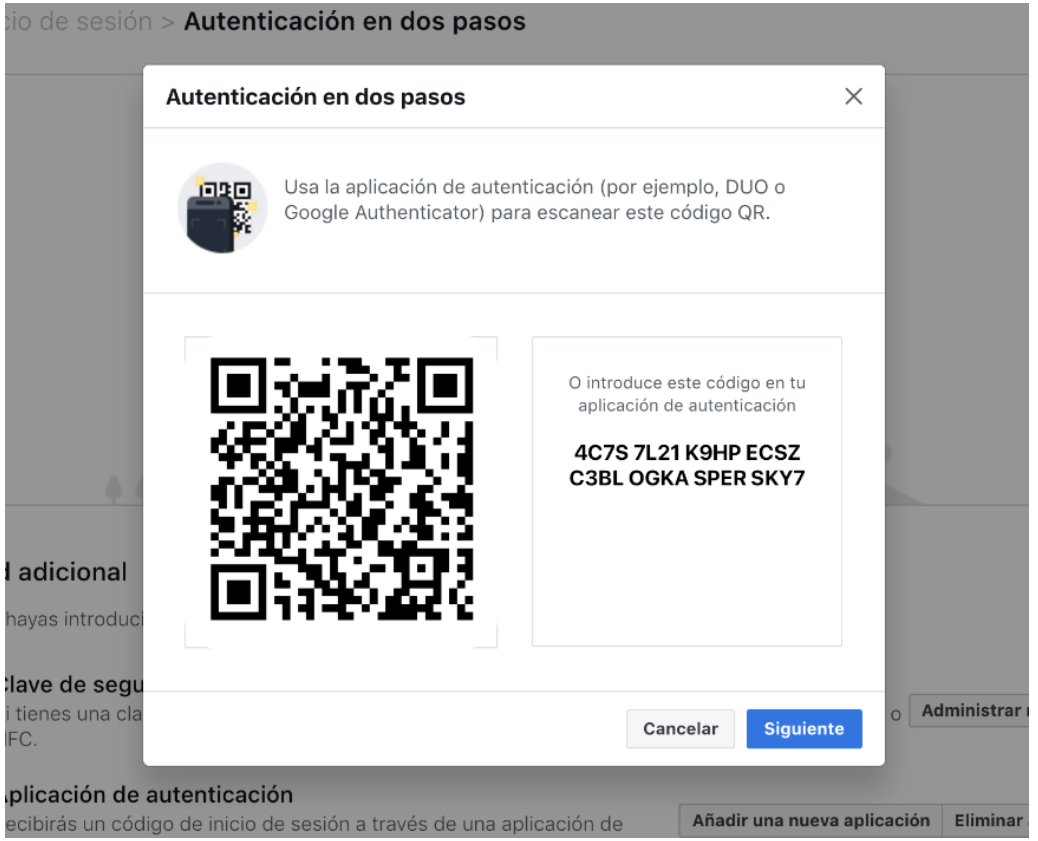


DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Identificación de doble factor





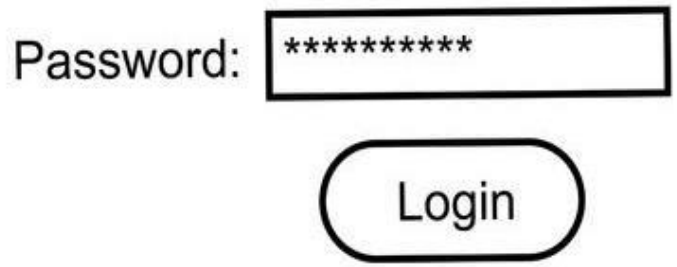


unión de comerciantes Principado de Asturias
gijón reinicia 2020/2021
Gijón impulsa

Contraseñas

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…)



DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Contraseñas

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

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Contraseñas

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

José.Pérez.García.11031980

¿es segura?

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Contraseñas

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.

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Contraseñas

¿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…)

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Contraseñas

http://youtu.be/iV9CmN-g_go

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Contraseñas

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

KASPERSKY lab
SECURE PASSWORD CHECK

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

Test your password *

••••••••••• *

⚠ 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

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

Contraseñas

- 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

DIGICOM
PLAN DE DIGITALIZACIÓN
DEL COMERCIO DE GIJÓN

Seguridad de nuestro sitio web

ecommerce

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

-Prevenir ataques

-Disponer de plan de contingencias

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

ecommerce

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

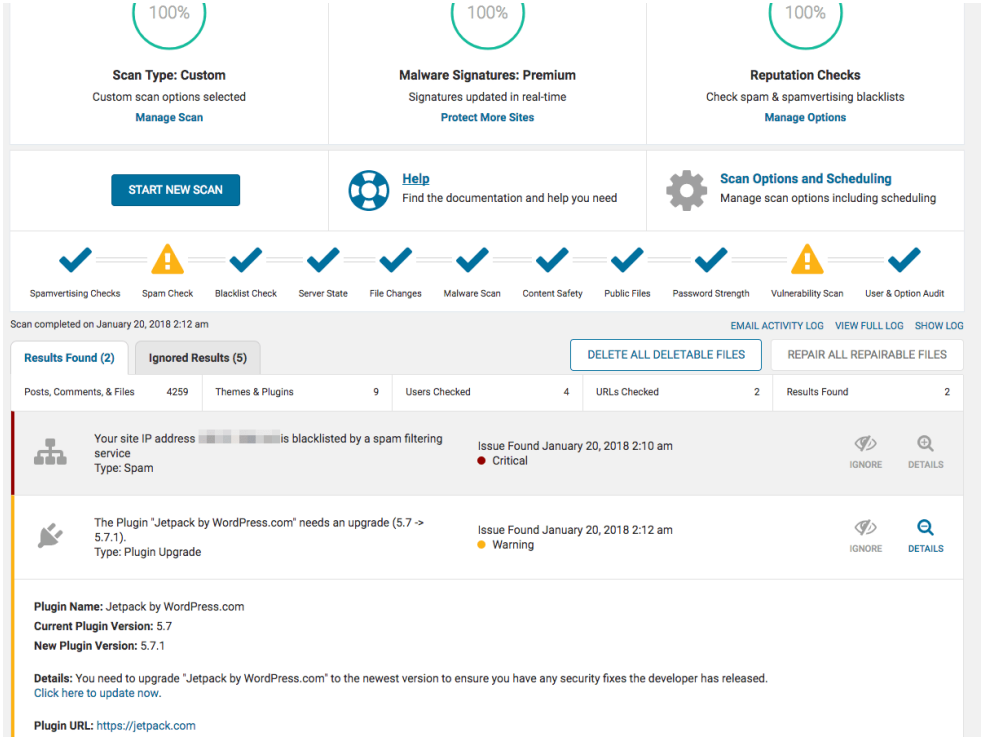
IP	Country	Block Count
35.247.219.231	Brazil	4
176.74.24.97	United Kingdom	4
199.188.200.224	United States	3
153.92.6.147	Germany	3
157.230.44.77	Singapore	3
91.215.216.28	Bulgaria	3
54.39.131.235	Canada	3
37.120.179.241	Germany	3
34.122.18.76	United States	3
190.107.177.240	Chile	2

Update Blocked IPs

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

ecommerce

Wordfence
Security

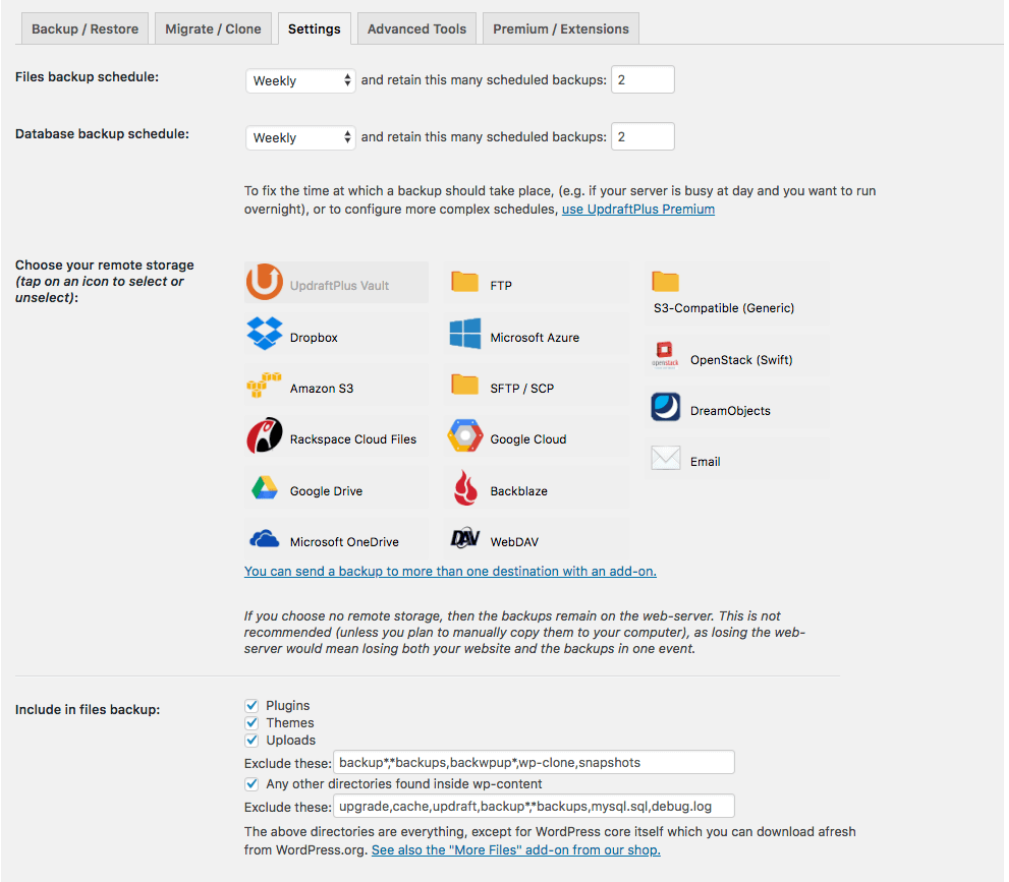


unión de comerciantes Principado de Asturias
gijón reinicia 2020/2021
gijón impulsa

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

ecommerce

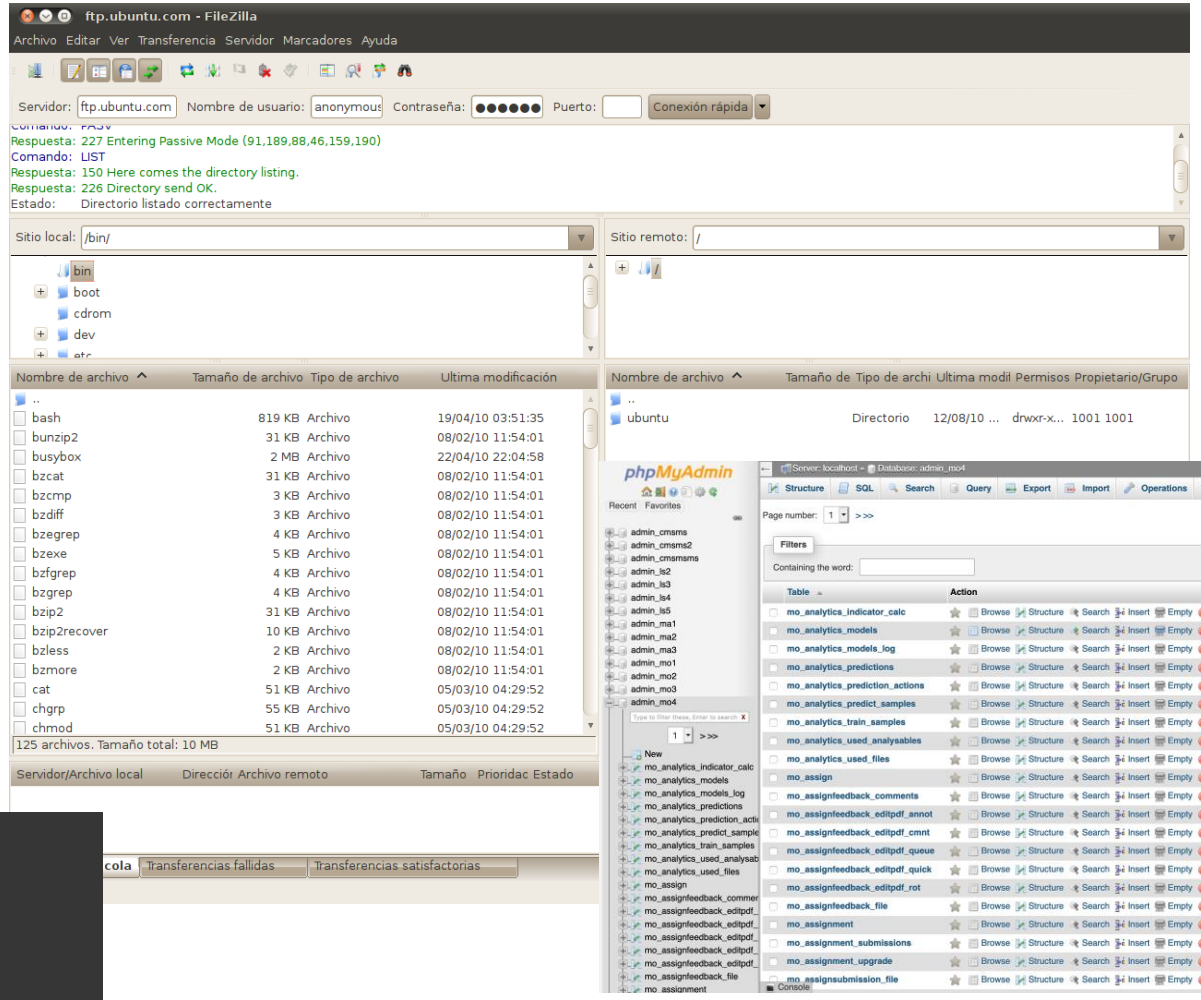
UpdraftPlus

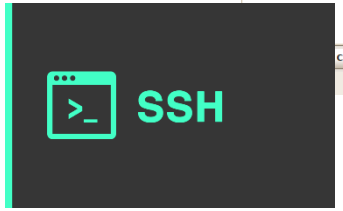


unión de comerciantes Principado de Asturias
gijónreinicia 2020/2021
Gijón impulsa

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

ecommerce





unión de comerciantes Principado de Asturias
gijónreinicia 2020/2021
Gijón impulsa

DIGICOM
PLAN DE DIGITALIZACIÓN
DEL COMERCIO DE GIJÓN

Dispositivos móviles

DIGICOM
PLAN DE DIGITALIZACIÓ DEL COMERCIO DE GIJÓ

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.

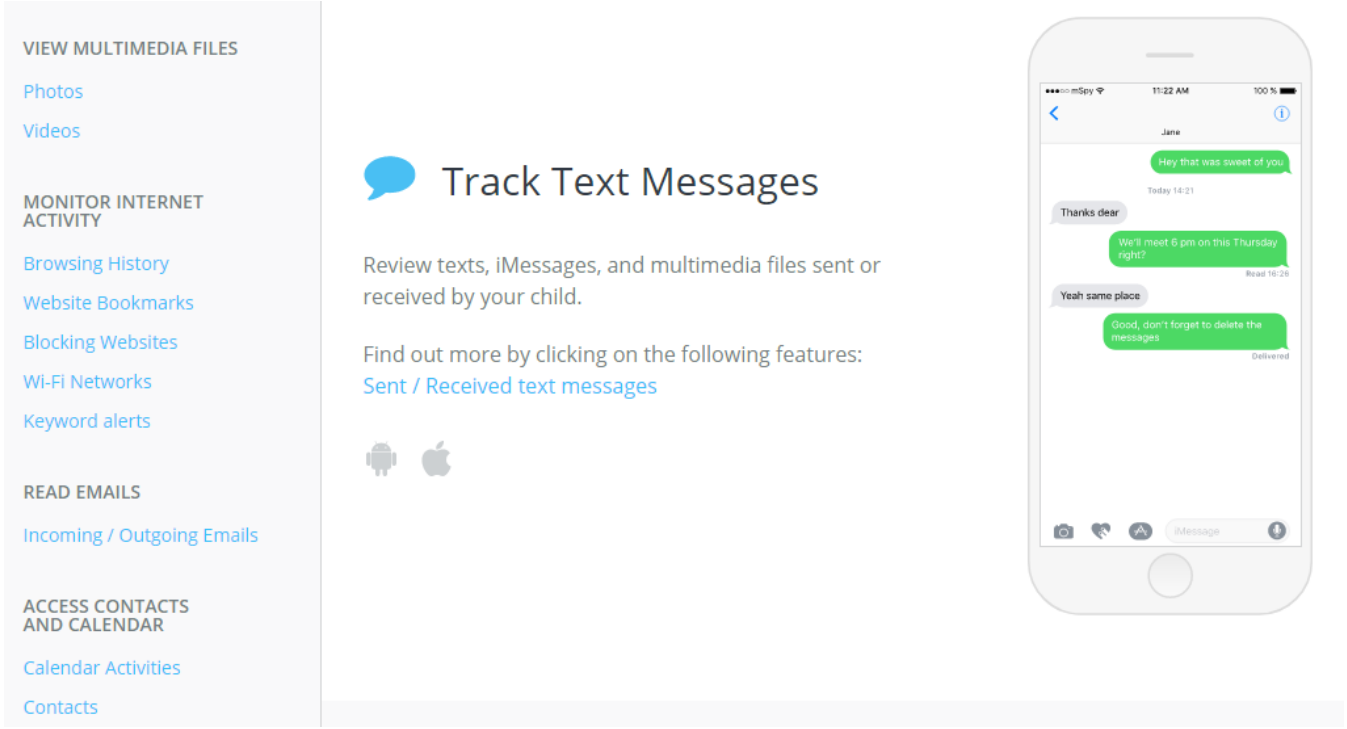
Stalkerware y adware, las dos ciberamenazas más peligrosas

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

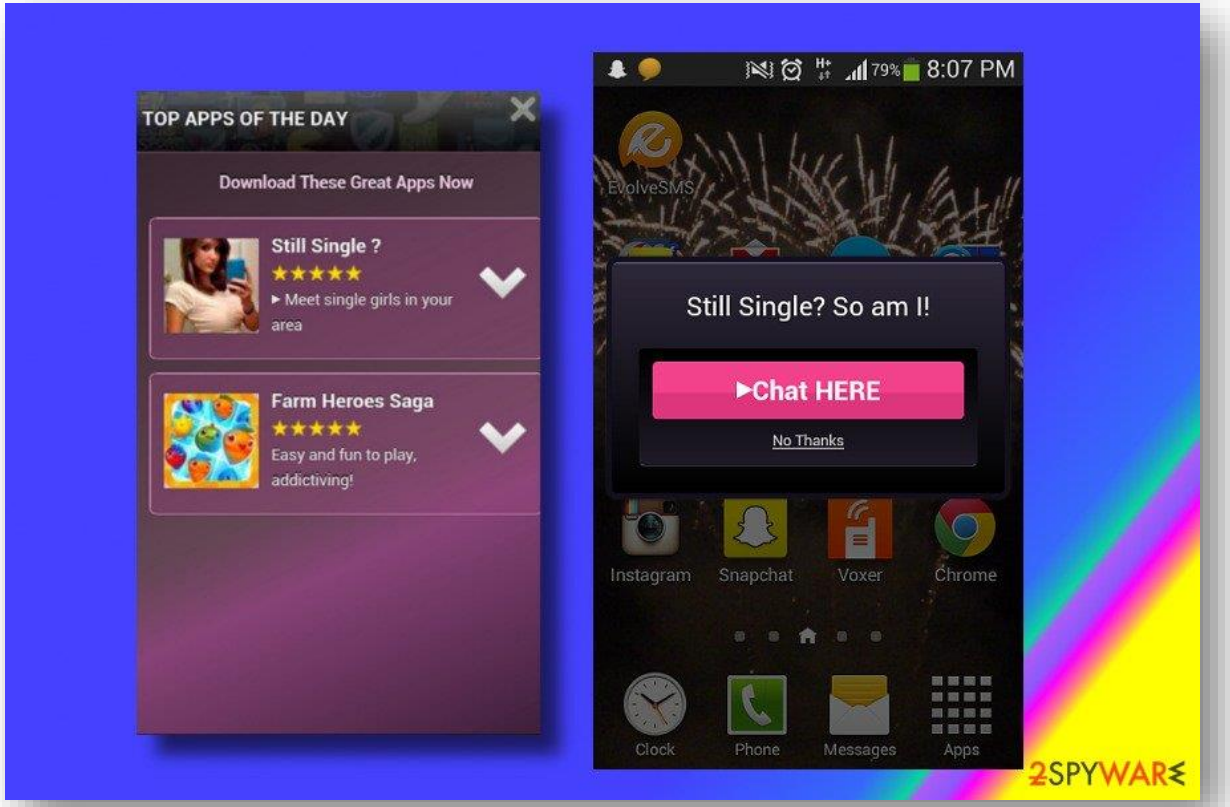
Aumentan los casos de mensajes en los que se suplanta la identidad de otra persona

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.



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-ðŸ"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 ...

DIGICOM
PLAN DE DIGITALIZACIÓN DEL COMERCIO DE GIJÓN

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

DIGICOM

PLAN DE DIGITALIZACIÓN
DEL COMERCIO DE GIJÓN

unión de comerciantes
Principado de Asturias

gijón reinicia
2020/2021

Gijón | impulsa