

Muchas gracias por tu interés en esta actividad, empezaremos en unos instantes

Recuerda apagar tu cámara y silenciar tu micrófono.

Durante la sesión para cualquier pregunta puedes usar el chat interno de la plataforma o bien preguntarnos activando tu micrófono.

La sesión será grabada y podrá ser publicada posteriormente en los canales del proyecto Digicom; puedes abandonarla en cualquier momento.

Correo para consultas **digicom@comercioasturias.com**

Web del proyecto <https://comerciodigitalgijon.es>



DIGICOM
PLAN DE DIGITALIZACIÓN
DEL COMERCIO DE GIJÓN

CIBERSEGURIDAD

Ingeniería social – El factor humano



El 46% de los comerciantes online ha sido víctima de un ciberataque

Seguridad 24 OCT 2022

El 53% de los comerciantes en España tuvo que hacer frente a varios tipos de ataques, siendo los bots maliciosos, los ataques a servidores DNS y los ataques de ransomware los más comunes. El 51% contrató un proveedor de servicios externo para resolver el ataque, el 39% instaló parches de seguridad y el 25% instaló una copia de seguridad.

PrestaShop ha dado a conocer los resultados de su última encuesta realizada entre las tiendas Million Club, que reúne a los clientes que generan más de un millón de ventas al año, y que revela que el 46% de los comerciantes ha sido víctima de un ciberataque. En el caso de España, las cifras superan la media mundial, ya que el 53% de los comerciantes afectados tuvo que hacer frente a varios tipos de ataques. Un 60% de los encuestados considera que el número de ataques está creciendo.

[El 46% de los comerciantes online ha sido víctima de un ciberataque](#) | Seguridad | IT Reseller

FORMACIÓN >

Carme Artigas: “Los ciberdelitos son el primer crimen organizado a escala internacional, por delante del narcotráfico y de la trata de personas”

La secretaria de Estado de Digitalización e Inteligencia Artificial habla de la creciente importancia del cibercrimen y de cómo protegerse adecuadamente

mismo. En España, por ejemplo, lo abonaron un 50 % de las mismas. Solo en 2021, el [Instituto Nacional de Ciberseguridad](#) (INCIBE) atendió 109.126 incidentes, de los cuales más de 90.000 correspondieron a ciudadanos y empresas. Con ocasión del [mes](#)


[Carme Artigas: “Los ciberdelitos son el primer crimen organizado a escala internacional, por delante del narcotráfico y de la trata de personas”](#) | [Formación](#) | [Economía](#) | [EL PAÍS](#) ([elpais.com](#))



¿Qué es la ingeniería social?

52.086 visualizaciones...

 871

 NO ME GUSTA

 COMPARTIR

 GUARDAR ...

¿Qué es la ingeniería social? - YouTube

“Una cadena es tan fuerte como su eslabón más débil”

“El eslabón más débil de la ciberseguridad es el usuario”

¿QUÉ ES LA INGENIERÍA SOCIAL?

La ingeniería social es “cualquier acto que influencia una persona para que realice acciones que puede o no estar entre sus intereses”

(Christopher Hadnagy – 2018)

¿QUÉ ES LA INGENIERÍA SOCIAL?

La ingeniería social no es algo nuevo ni exclusivo de los ciberdelincuentes

En el ámbito de la ciberseguridad el método consiste en el empleo de técnicas psicológicas y habilidades sociales para conseguir información de interés o el acceso a los sistemas informáticos

Los ataques basados en éstas técnicas son muy efectivos, sencillos, baratos y pueden ocasionar un alto impacto en la víctima u organización afectada

¿QUÉ ES LA INGENIERÍA SOCIAL?

Kevin Mitnick – “*The Art of Deception*”

“La ingeniería social utiliza la influencia y la persuasión para engañar a las personas, convenciéndolas, mediante la manipulación, de que el ingeniero social es alguien que no es. Como resultado, el ingeniero social es capaz de aprovechar a las personas para obtener información con o sin el uso de la tecnología”

Su éxito radica en que:

- ✓ Todos queremos ayudar
- ✓ No nos gusta decir que no
- ✓ La primera actitud suele ser de confianza hacia otra persona
- ✓ Nos gusta que nos alaben

LOS 6 PRINCIPIOS DE PERSUASIÓN E INFLUENCIA (Robert Cialdini)

1 - RECIPROCIDAD

Las personas tratan a los demás como perciben que los demás les tratan a ellos

Esto puede llevar a que cuando damos (ej: información) algo esperamos recibir algo a cambio (ej: recomensa)

LOS 6 PRINCIPIOS DE PERSUASIÓN E INFLUENCIA (Robert Cialdini)

2 - COMPROMISO Y COHERENCIA

Las personas realizan acciones que son coherentes con lo que ya han realizado y tienden a ser consecuentes con las decisiones tomadas

Esto puede llevar a que cuando damos algo esperamos recibir algo a cambio

Cuando alguien nos pide ayuda lo hacemos. Tras ayudarle con cuestiones sencillas nos resultará más difícil decir que no

LOS 6 PRINCIPIOS DE PERSUASIÓN E INFLUENCIA (Robert Cialdini)

3 - APROBACIÓN SOCIAL

Las personas tienden a sumarse a la opinión mayoritaria

No dará menos reparo hacer algo si previamente lo realizó el grupo

LOS 6 PRINCIPIOS DE PERSUASIÓN E INFLUENCIA (Robert Cialdini)

4 - AUTORIDAD

Las personas con cierto liderazgo tienen mayor credibilidad

La suplantación de entidades reconocidas o personas de prestigio/poder (jefe) dará más opciones de obtener la información de manos de un empleado

LOS 6 PRINCIPIOS DE PERSUASIÓN E INFLUENCIA (Robert Cialdini)

5 - SIMPATÍA

Las personas simpáticas y/o atractivas tienen mayor grado de persuasión

El llamado “Efecto Halo” hace que atribuyamos más cualidades positivas a personas que nos parecen atractivas y por ello facilitar la creación de vínculos de confianza

LOS 6 PRINCIPIOS DE PERSUASIÓN E INFLUENCIA (Robert Cialdini)

6 - ESCASEZ

Tendemos a dar más valor a aquello que percibimos como escaso o exclusivo

Por ello en este tipo de ataques se juega con la urgencia transmitiendo a la víctima la necesidad de actuar de forma inmediata para aprovechar la oportunidad

El objetivo es que actúe sin pensarlo dos veces

FASES DE LA INGENIERÍA SOCIAL

RECOLECCIÓN DE INFORMACIÓN

En esta fase el objetivo es obtener la mayor información posible de la víctima para conocer sus debilidades y elegir el vector de ataque

RELACIÓN DE CONFIANZA

En base a la información obtenida se prepara el anzuelo para atraer a la víctima y establecer la confianza

FASES DE LA INGENIERÍA SOCIAL

MANIPULACIÓN

En esta fase se realiza la ejecución del ataque con el objetivo que se desee conseguir

SALIDA

Una vez realizada la extorsión se corta la interacción con la víctima y se intentan borrar las huellas



Diario de Sevilla

SEVILLA

SEVILLA PROVINCIA ANDALUCÍA ESPAÑA ECONOMÍA SOCIEDAD DEPORTES CULTURA COFRADÍAS OPINIÓN ☰ TODAS LAS SECCIONES

SEVILLA VIVIR JUZGADO DE GUARDIA RUTAS DE SENDERISMO

SEMANA SANTA El nuevo orden del Domingo de Ramos

SEVILLA

El ataque del intermediario, la estafa en la que ha caído el Ayuntamiento de Sevilla

- Unos ciberdelincuentes lograron interceptar las comunicaciones entre Urbanismo y una empresa adjudicataria, a la que luego suplantaron
- Este tipo de timo, conocido en inglés como 'Man in the Middle', ha afectado ya a decenas de entidades en España



Las luces de Navidad, contrato en el que se ha detectado la estafa. / JUAN CARLOS MUÑOZ

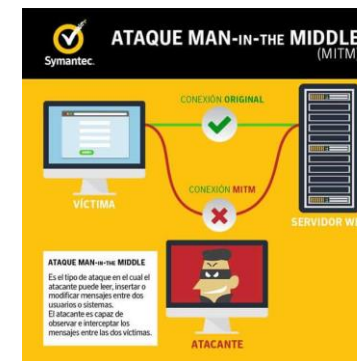
REDACCIÓN

21 Septiembre, 2021 - 13:13h



En el caso que está investigando la Policía Nacional, todo apunta a que los ciberdelincuentes interceptaron las comunicaciones del Ayuntamiento de Sevilla y la empresa adjudicataria del contrato de la iluminación navideña. Lo hicieron probablemente mediante la introducción de un virus informático.

Luego suplantaron la identidad de la empresa y lograron que el Ayuntamiento abonara el contrato no a la cuenta de la empresa real, sino a otra controlada por ellos. Para poder cobrar o mover luego este dinero, generalmente hace falta una mula económica, un hombre de paja que, a cambio de un beneficio económico, ponga su nombre a la cuenta a la que se hace el pago. La cantidad estafada es de 962.797 euros.





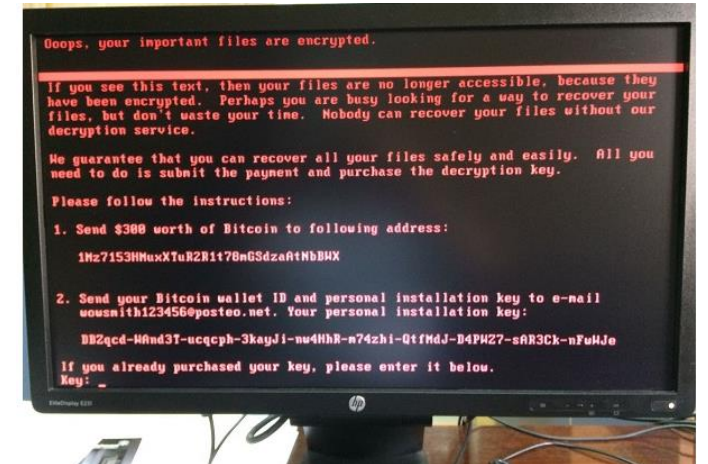
Publicado el
12/05/2017

Importancia : Alta

Malware

Ransomware

Importante oleada de ransomware afecta a multitud de equipos



[Importante oleada de ransomware afecta a multitud de equipos | Oficina de Seguridad del Internauta \(osi.es\)](https://www.osi.es)



Sala de prensa

SALA DE PRENSA ACTUALIDAD POLICIAL

Comunicación / Sala de prensa / Noticia

El fraude detectado asciende a más de 20.000 euros

La Policía Nacional desarticula un grupo criminal especializado en la comisión de estafas románticas

Los miembros del entramado operaban a nivel nacional e internacional haciendo creer a sus víctimas que mantenían una relación sentimental a distancia, a razón de la cual se hacían necesarias varias transacciones económicas para sufragar gastos que posibilitarían el encuentro entre ambos

Hacían creer a sus víctimas que mantenían una relación sentimental y les pedían dinero con cualquier excusa para posibilitar su encuentro

Fraude superior a 20.000 euros y víctimas de avanzada edad

Portal web de la Policía Nacional



[Detalle nota de prensa. Policía Nacional España. \(policia.es\)](#)

Publicado el
17/02/2021

Importancia : Media

Ingeniería social

Redes sociales

Suplantación de ident...

Oleada de casos de suplantación de identidad en cuentas de Instagram y Onlyfans con fraudes dirigidos hacia sus seguidores



[Oleada de casos de suplantación de identidad en cuentas de Instagram y Onlyfans con fraudes dirigidos hacia sus seguidores | Oficina de Seguridad del Internauta \(osi.es\)](https://www.osi.es)



Perfil real




Perfil falso

CASOS REALES



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) : [haga clic aquí.](#)

Gracias por su cooperación,
Agencia Tributaria.

Enlace a la página web fraudulenta


Redacción extraña

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

Redacción extraña

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



Dirección de remitente que no corresponde con el dominio real.

Necesitamos que verifique su cuenta introduciendo sus credenciales y SMS verificación .

Solicitud que no se ajusta a la forma habitual de proceder

URL de destino sospechosa en el botón de acceso

Redacción extraña



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

Archivo Mensaje

Expiracion del correo electrónico [redacted]@[redacted].es
Arsys Servidor de Correo (webmail_admin@[redacted].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

Cuando 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



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

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.

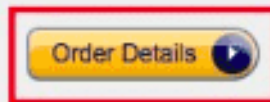
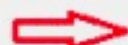
Order Confirmation
Order #154-1238066-0002647

Hello ,

Thank you for shopping with us. We confirm 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

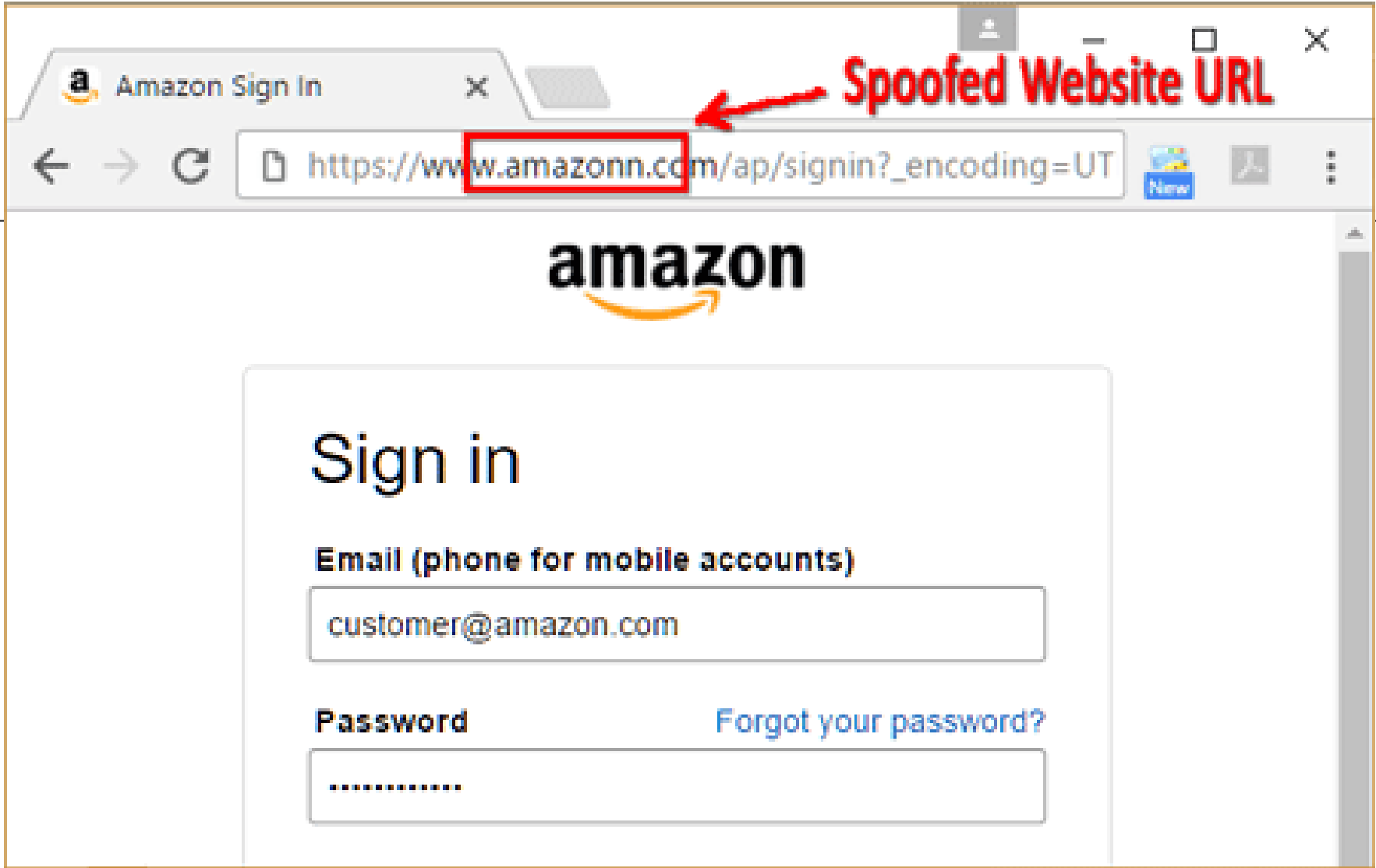


Payment Summary

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







Publicado el
06/07/2022

Fraude

Suplantación

Coca-Cola no está haciendo regalos por el 130 aniversario



Oficina
de Seguridad
del Internauta

[Coca-Cola no está haciendo regalos por el 130 aniversario | Oficina de Seguridad del Internauta \(osi.es\)](https://www.osi.es)



Regalos por el 130 aniversario de Coca-cola
5.000 productos exclusivos gratis.
cocacola.com

13:18 ✓



Hola,

Bienvenidos al Concurso por el 130 aniversario de Coca-cola.

Responde al cuestionario, encuentra el premio oculto y gana una mini nevera exclusiva Coca-Cola.

Quedan 246 regalos.

Pregunta 1 de 4: ¿Conoces a Coca-Cola?

SI

NO

Team Support Service@account.com via [redacted] hostgator.com 7:45 AM (15 hours ago) ☆



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

Dirección de remitente que no corresponde con el dominio real.

Enlace fraudulento, a URL que no corresponde a PayPal



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.

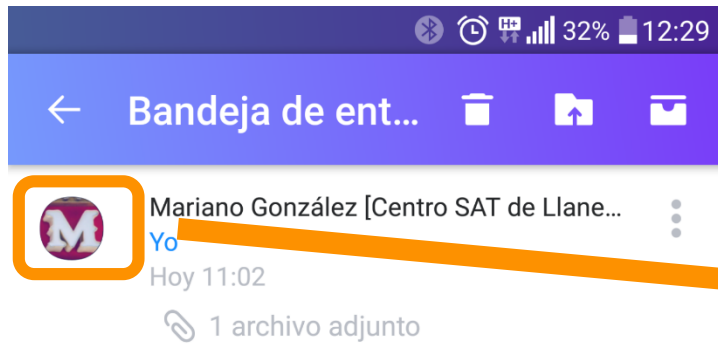
Documento disponibile qui:

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

Cordiali saluti.

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

Solicitud que llega
directamente en otro
idioma



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



Estimado cliente:

No hemos recibido el pago de esta factura.

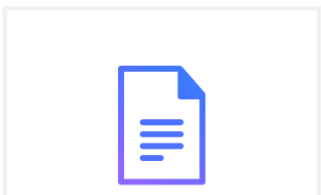
Atentamente,

Mariano González [Centro SAT de Llanera |
CTIC Centro Tecnológico

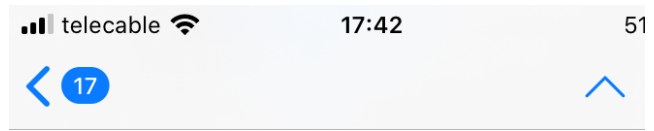
Teléfono 95 877 58 30 Extensión 4990

Datos de contacto
falsos

1 archivo adjunto | 251 KB



Adjunto
sospechoso



Factura P-4388

Hola,

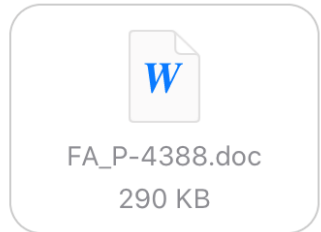
Adjunto envío la factura
correspondiente al mes.

Salutacions,

Mariano González [Centro SAT de
Llanera | CTIC Centro Tecnológico

Te. +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.

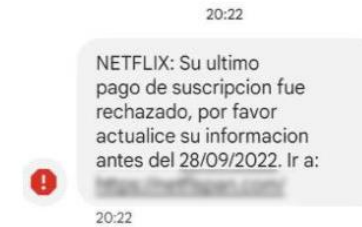
Atentamente.

- 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

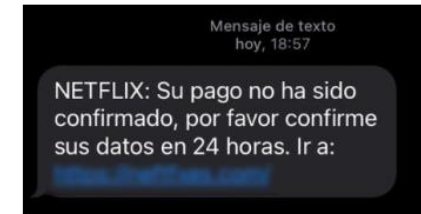




Ejemplo 1 de SMS:



Ejemplo 1 de SMS:



Publicado el
24/10/2022

Importancia : Media

Netflix

Smishing

SMS

No renueves tu suscripción de Netflix sin antes ver este aviso



[No renueves tu suscripción de Netflix sin antes ver este aviso | Oficina de Seguridad del Internauta \(osi.es\)](https://www.osi.es)

CASOS REALES



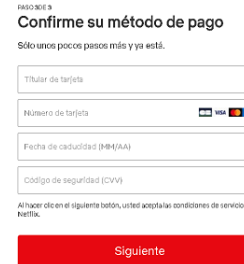
NETFLIX



NETFLIX



NETFLIX

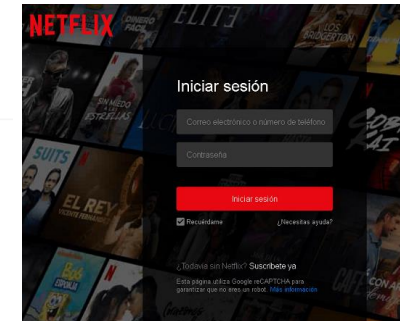


NETFLIX



[No renueves tu suscripción de Netflix sin antes ver este aviso | Oficina de Seguridad del Internauta \(osi.es\)](https://www.osi.es)

NETFLIX





¡Atención! Se han detectado varias campañas de smishing que suplantan a entidades bancarias

Publicado el 10/10/2022

Smishing SMS

Importancia : Alta

Nuevo dispositivo conectado a su banca online, si no reconoce dicha accion verifique inmediatamente: [redacted]

Nuevo dispositivo conectado a su banca online, si no reconoce dicha accion verifique inmediatamente: [redacted]

Leido [redacted]

Su tarjeta ha sido limitada temporalmente por razones de seguridad, para reactivarla, actualice su informacion [redacted]

CAIXABANK INFORMA
Acción requerida en tu tarjeta, se han detectado movimientos inusuales, activa el nuevo sistema de seguridad antes del 03/09/2022 a través del siguiente enlace para evitar el bloqueo de tus cuentas y tarjetas [redacted]

Hemos detectado movimientos inusuales en su aplicacion, por prevencion si no ha sido usted confirmelo en nuestra web: [redacted]

Ibercaja Banco [servicio al cliente] :
Apartir del 23/09/2022 No puedes utilizar su Tarjeta. Tienes que activar el nuevo sistema de seguridad: [redacted]

Openbank: Codigo de confirmacion [redacted] para confirmar el acceso a Openbank.

Centro de ayuda Banco Santander.
A partir del 31/08/2022 no podra utilizar su tarjeta debido a cambios en la politica de seguridad. Acceda al link para proceder con la activacion [redacted]

AVISO: Se ha conectado un nuevo dispositivo. Si no reconoce este acceso verifique mediante: [redacted]



[¡Atención! Se han detectado varias campañas de smishing que suplantan a entidades bancarias | Oficina de Seguridad del Internauta \(osi.es\)](https://www.osi.es)



Publicado el
06/09/2022

Importancia : Media

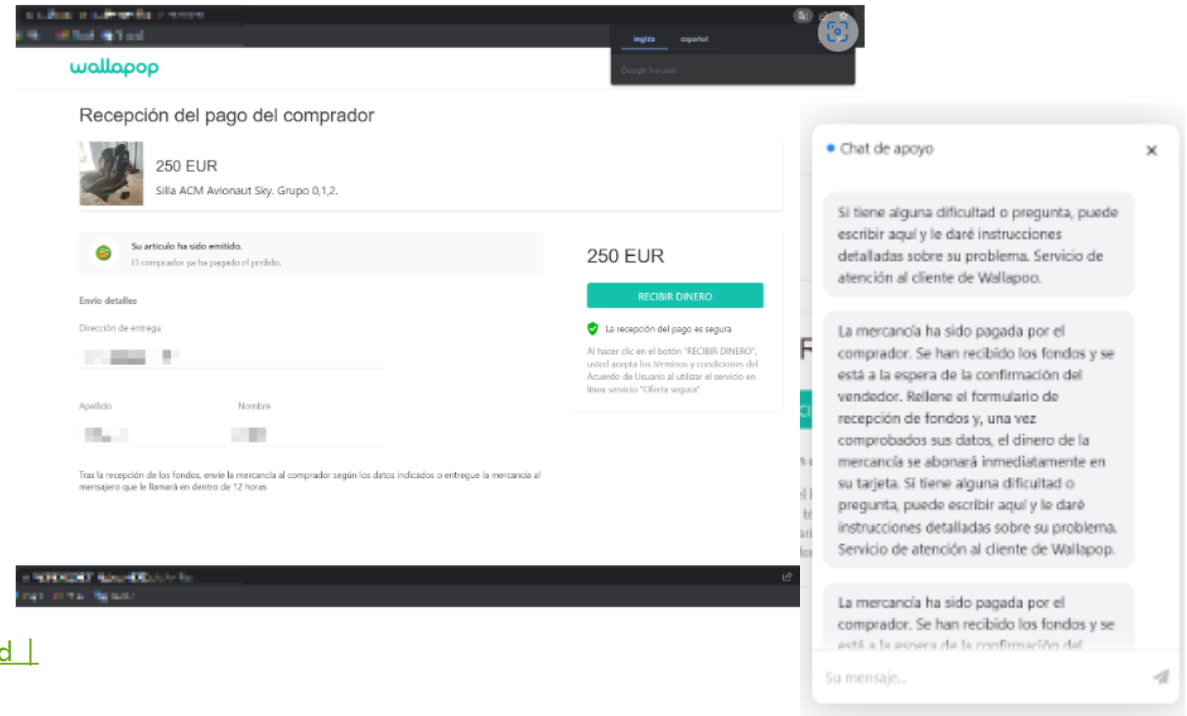
Aviso

Comprar

Fraude

Smishing

Detectado nuevo método de fraude en tiendas de compraventa como Wallapop y Vinted



The screenshot shows a Wallapop transaction page for a 'Silla ACM Avionaut Sky, Grupo 0,1,2' priced at 250 EUR. A green notification states 'Su artículo ha sido emitido. El comprador se ha pagado el pedido.' Below this, there is a 'RECEPCIÓN DE DINERO' section with instructions: 'La recepción del pago es segura. Al hacer clic en el botón "RECIBIR DINERO", usted acepta los términos y condiciones del Acuerdo de Usuario al utilizar el servicio en línea "Oferta segura".' To the right, a chat window titled 'Chat de apoyo' contains the following text: 'Si tiene alguna dificultad o pregunta, puede escribir aquí y le daré instrucciones detalladas sobre su problema. Servicio de atención al cliente de Wallapop.' and 'La mercancía ha sido pagada por el comprador. Se han recibido los fondos y se está a la espera de la confirmación del vendedor. Rellene el formulario de recepción de fondos y, una vez comprobados sus datos, el dinero de la mercancía se abonará inmediatamente en su tarjeta. Si tiene alguna dificultad o pregunta, puede escribir aquí y le daré instrucciones detalladas sobre su problema. Servicio de atención al cliente de Wallapop.'



[Detectado nuevo método de fraude en tiendas de compraventa como Wallapop y Vinted | Oficina de Seguridad del Internauta \(osi.es\)](https://www.osi.es)

CASOS REALES



18:59

< EndesaES Eliminar

martes, 28 de enero de 2020

 Notamos que pago la factura dos veces al mismo tiempo. Cantidad: 159,99 € Para confirmar su reembolso Haga clic en el enlace <https://area-clients.com> 19:21

Banca Online: Santander a las 19:33 se ha recibido una transferencia. Por favor, accede tu linea Santander por firmarlo, en nuestro sitio web: www.msantander.es





 Toca para cargar la vista previa

6 minutos

CASOS REALES



 Ejemplo de fraude telefónico Compartir

 "Debemos estar alerta frente a peticiones extrañas. No debemos proporcionar información si no estamos absolutamente seguros de la persona que está al otro lado, y nunca dar credenciales de acceso. Como podemos oír en el audio, el usuario que recibe la llamada proporciona su clave y acceso remoto a su equipo a una desconocida que aunque dice ser del departamento de Informática, no lo demuestra en ningún momento."


MÁS VÍDEOS

0:02 / 2:23

YouTube

Ejemplo de fraude telefónico

16.178 visualizaciones... 77 NO ME GUSTA COMPARTIR GUARDAR ...

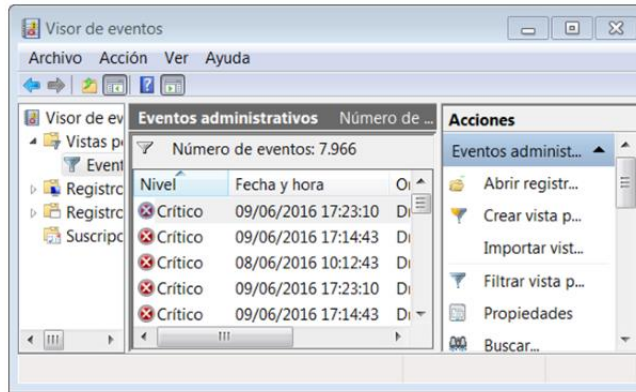
 **INCIBE**
39.900 suscriptores SUSCRIBIRME

La ingeniería social es el elemento más utilizado por los ciberdelincuentes. Habitualmente sus ataques nos suelen llegar a través del correo electrónico pero también usan otros canales como el telefónico. En este audio podemos comprobar cómo una ciberdelincuente es capaz de conseguir información crítica de un empleado de una empresa.



Publicado el
27/12/2016

Servicio técnico falso, pero estafa real



Microsoft | Centro de noticias Inicio Nuestra empresa ▾ Nuestros productos ▾ Blogs y comunidad

Microsoft alerta sobre un aumento de estafas de soporte técnico, donde se utiliza ilegalmente su marca, e insta a reforzar la seguridad a los usuarios

junio 26, 2020 | Microsoft Prensa



[Servicio técnico falso, pero estafa real | Oficina de Seguridad del Internauta \(osi.es\)](#)

[Microsoft alerta sobre un aumento de estafas de soporte técnico, donde se utiliza ilegalmente su marca, e insta a reforzar la seguridad a los usuarios – Centro de noticias](#)



Publicado el
08/09/2022

Importancia : Media

Extorsión

Detectados correos que engañan a los usuarios con un supuesto pirateo de sus dispositivos



[Detectados correos que engañan a los usuarios con un supuesto pirateo de sus dispositivos | Oficina de Seguridad del Internauta](#)

Evidencia 4

De [Redacted] ☆
Asunto: **A la espera del pago.**
A [Redacted] ☆

iHola!
¿Ha notado hace poco que ha recibido un correo electrónico desde su propia cuenta?
Eso es simplemente porque tengo total acceso a su dispositivo.

Llevo un par de meses observándole.
¿No entiende cómo es posible? Bueno, ha sido infectado con un malware originario de un sitio web para adultos que visitó. Por si no está familiarizado con estos temas, intentaré explicárselo.

Con la ayuda de un virus troyano, puedo obtener total acceso a un PC o a cualquier otro dispositivo.
Eso significa que puedo ver siempre que quiera frente a la pantalla, con solo encender la cámara y el micrófono sin que usted se dé cuenta.
Además, también tengo acceso a su lista de contactos y a todos sus mensajes de correo.

Puede que se pregunte: "Pero mi PC tiene un antivirus activo, ¿cómo es posible? ¿Por qué no he recibido ninguna notificación?"
La respuesta es sencilla: mi malware utiliza controladores, lo que me permite actualizar las firmas cada cuatro horas y hacer que sea indetectable, y por eso el antivirus se mantiene en silencio.

Tengo un vídeo en el que sale masturbándose en el lado izquierdo, y en el derecho la película que estaba viendo mientras se masturbaba.
¿Se está preguntando en qué puede perjudicarle esto? Con un solo clic de ratón, puedo enviar el vídeo a todas sus redes sociales y contactos de correo electrónico.
También puedo compartir todos sus mensajes de correo electrónico y de messenger.

Lo único que debe hacer para evitar que esto suceda es transferir bitcoins por valor de 750\$ a mi dirección bitcoin (si no tiene ni idea de cómo hacerlo, puede abrir el navegador y simplemente buscar: "Comprar bitcoins").

Mi dirección bitcoin (monedero de bitcoin) es: 1C[Redacted]!R

Una vez que reciba la confirmación del pago, borraré el vídeo de inmediato, y se acabó, no volverá a saber de mí.
Tiene 2 días (48 horas) para completar esta transacción.
Cuando abra este mensaje de correo, recibiré una notificación y mi temporizador se pondrá en marcha.



Presentar una denuncia no le servirá de nada, ya que este correo electrónico no puede ser rastreado, al igual que mi identificador bitcoin.
Llevo mucho tiempo dedicándome a esto y nunca cometo errores.

Si descubro que ha compartido este mensaje con alguien más, distribuiré inmediatamente el vídeo, tal como le he advertido.

CASOS REALES



Redacción
extraña

De  ☆
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  ☆

¡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: 

Apela a la vergüenza
del usuario



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: 1JTwbvmM7ymByxPYCByVYCwasjH49J3Vj

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 ...

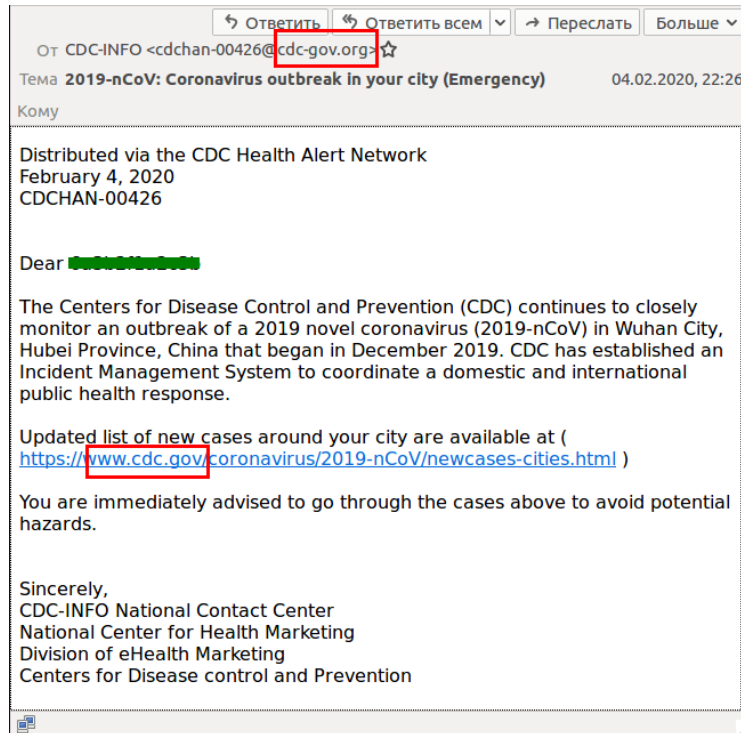
p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

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

CASOS REALES



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, cough, shortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE

AYUDA A EMPRESAS Y PYMES



INSTITUTO NACIONAL DE CIBERSEGURIDAD





DIGICOM
PLAN DE DIGITALIZACIÓN
DEL COMERCIO DE GIJÓN



¡Gracias!

