CARITAS CASTRENSE

MANUAL DE SEGURIDAD EN INTERNET Y REDES SOCIALES

MADRID, octubre de 2020

SUMARIO

Introducción

En los últimos años hemos asistido a una fuerte evolución tecnológica. Este extraordinario avance técnico se basa en las llamadas "TIC,s," *Tecnologías de la Información y las Comunicaciones.*

El Siglo XXI se caracteriza por una evolución continua de estas tecnologías y, en la actualidad, son conocidas como las *Nuevas Tecnologías de la Información y las Comunicaciones*, que hacen referencia a las técnicas que han surgido en los últimos años dentro de los campos de la informática y la comunicación. Instrumentos y herramientas que hacen más fácil la vida del hombre en algunos aspectos y que le ayudan a entender mejor, esta era de cambios y velocidad en la que vive.

Podemos citar algunos ejemplos de estas nuevas tecnologías, como los ordenadores y su capacidad de comunicación; el desarrollo informático; la aparición del video (grabar imágenes, escucharlas y reproducirlas): el desarrollo de la fibra óptica; la televisión digital; la informatización de la educación, los libros electrónicos, el material online, etc.

En definitiva, una tecnología basada en algoritmos, imágenes e iconos, que permite a los niños familiarizarse con su manejo y significado, mucho antes de comenzar a hablar correctamente

Es cierto pues que estas nuevas tecnologías están muy presentes en nuestras vidas; forman parte de nuestro trabajo, actividades de ocio, cultura y entretenimiento.

En consecuencia, interactuamos continuamente con amigos y familiares, revisando y activando desde los teléfonos móviles, los ordenadores o las Tablet, todo lo que sucede en el mundo, a través de todas las redes, sin percatarnos, la mayoría de las veces, de los potenciales riesgos que conllevan su mal uso, ni tampoco, ponemos los medios adecuados para evitarlos.

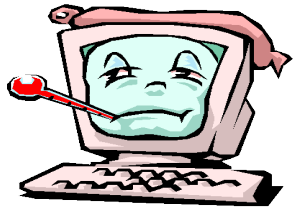
Por lo tanto, se puede afirmar que, el correo electrónico, las páginas webs, las redes sociales como *Facebook, Twitter, Instagram, YouTube*, etc. hace mucho tiempo que forman parte de la vida social y de comunicación de las personas.

No obstante, debido al gran número de personas conectadas, así como la ausencia de medidas de prevención, éstas se convierten en un blanco fácil para los delincuentes y personas mal intencionadas, para atacar a sus víctimas y ocasionarles un gran perjuicio.

Principales riesgos y amenazas en Internet y RRSS.

A modo de introducción sobre los riesgos y amenazas que asolan el mundo de la información y las telecomunicaciones, veamos los más populares y más agresivas:

Virus: Son códigos maliciosos, gusanos y troyanos usados para acceder al equipo de la víctima y robar información confidencial o claves. Se propagan a través de mensajes populares, principalmente en Facebook, que llevan a enlaces falsos o por medio del lenguaje de programación que insta a descargar e instalar archivos maliciosos en el equipo.



Phishing: Esta modalidad consiste en el robo de información a través de la suplantación de identidad. Aunque esta acción fraudulenta es más común en mensajes de correo electrónicos, en redes sociales, algunos delincuentes pueden crear cuentas en Twitter o páginas en Facebook de entidades bancarias falsas para hacerle creer a la persona que es la real y así invitarlo a actualizar datos o a acceder al sitio web (falso) de la entidad para atacarlo.

Acoso: Al tener información, fotos o videos visibles para todo el mundo en las redes sociales, se puede caer en el ojo de un acosador. Si no se configura la privacidad en las redes sociales, cualquiera puede acceder a todo lo que publicamos y convertirse en un riesgo para la integridad de nosotros mismos.

Robo de información: En nuestras redes sociales compartimos mucha información: dónde vivimos, con quién estamos, dónde estamos, qué compramos, qué comemos, etc. Quizás no sea un riesgo mayúsculo como una contraseña o el número de la tarjeta de crédito, pero con estos datos muchos cibercriminales crean perfiles falsos para acceder a personas cercanas y atacarlas.

Spam o correo basura: Son mensajes no deseados o correo basura. Si un correo electrónico se clasifique como spam, es porque este tipo de mensajes se envían de forma masiva a un gran número de destinatarios. A veces, el spam es publicidad que nadie pidió, pero también puede incluir malware, el cual permite la descarga de un virus que posiblemente dañe nuestro sistema operativo.

Información nociva: Mucha información en Internet contiene pornografía, crímenes, actos terroristas y suicidas, etc. Aunque los adultos podemos optar por mantener una postura analítica ante estos hechos, los niños y adolescentes son más vulnerables ante tal información.

Anuncios falsos: ¿Alguna vez has entrado a una página web y visto la leyenda: "Felicidades has ganado 1 millón de euros"? Internet es una forma muy sencilla de llegar a mucha gente, algunas personas utilizan estos anuncios para robar información de cuentas bancarias. Millones de personas en el mundo han sido víctimas de estos estafadores que utilizan anuncios falsos para obtener datos verdaderos de gente ingenua que se deja sorprender.

Hackeo: Este es uno de los mayores peligros de Internet, ya que mucha gente pierde el acceso a sus cuentas de correo y redes sociales. Esto sucede porque los piratas cibernéticos roban la información de nuestras cuentas, cambian los

accesos e ingresan a nuestros correos y roban la información más personal y laboral que tenemos.

Estafas económicas: Las tiendas online suelen ofrecer la posibilidad de pagar con tarjeta o PayPal, pero siempre tenemos que saber a quién estamos comprando. Por ejemplo, si al comprar, el vendedor nos solicita los datos por email o quiere que se los demos de manera particular sin tener que hacerlo por su web como suele hacerse habitualmente, debemos desconfiar. También es importante saber si la tienda online es conocida o tiene buena reputación, ya que muchas se crean como intermediarias de la compra sin que se sepa y después de pagar puede no llegar el producto.

2.1 Modalidades de estafas/ fraudes, detectadas en Cáritas: la clonación o suplantación de identidad, y la estafa carta nigeriana, "la herencia"

a. La primera, la suplantación de identidad, clonación o phishing:

"Modus operandi"
Consiste en suplantar la identidad de una empresa o entidad**.** Lo básico es elegir una marca en la que los usuarios confíen y copiarla lo mejor posible. Algunas de las fórmulas que utilizan los ciberdelincuentes para suplantar a empresas o entidades financieras y engañar a sus víctimas, suelen ser: copiar los contenidos y los dominios de marcas registradas o información de contacto con teléfonos y cuentas de Skype.

En la mayor parte de las veces los ataques comienzan con un simple correo electrónico. "*Tu banco solicita tus datos para mantener activa la cuenta o una marca de referencia te pide rellenar una sencilla encuesta: reclamos simples en los que cualquiera pudiera caer*. El email puede contener textos originales, imágenes oficiales y enlaces que, en un principio, nos pueden parecer confiables.

Lo mismo ocurre con las webs a las que nos dirigen: *el formato y los contenidos son idénticos.* Todos estos mecanismos pueden darse a la vez o por separado. Se puede encontrar desde sitios totalmente clonados hasta aquellos que solo copian los contenidos y el logotipo o utilizan un nombre diferente.
Por tanto, siempre es importante fijarse en el nombre del dominio de la página web para detectar si es falso. Por ejemplo, podrían crear www.amezon.com en vez de www.amazon.com y no darnos cuenta de la "e" que es un nombre diferente y falso.

Dos **ejemplos** claros de estos ciberataques son los sufridos por la propia Agencia Tributaria y Cáritas Española

- En el primero de los casos, se hace referencia a falsos reembolsos de impuestos para los que el usuario, si quiere recibirlos, tendrá que acceder a una web maliciosa y rellenar un formulario con sus datos de cuentas bancarias y tarjetas de crédito. Además, se invita a

descargar una supuesta nueva aplicación que, bajo el nombre de **TAPE**, no es más que un dañino *malware*.

- En el segundo caso, el de la clonación de la página web de Cáritas, mediante este procedimiento, querían redirigir las entregas de los donantes, a una cuenta diferente, propiedad de los delincuentes.

Medidas

- Evitar ser estafado es **no responder jamás a una solicitud de información personal** a través del correo electrónico, llamada de teléfono o SMS. Tenemos que recordar que, por *tarjeta de crédito o cualquier i*nformación personal por estos medios. Si recibes una petición así, lo más probable es que se trate de un suplantador.
- Se recomienda **evitar el acceso a cualquier web a través de un enlace**, en especial si lo hemos recibido por alguna de las vías antes dichas. Es mucho mejor **introducir la URL original directamente en la barra de direcciones** del navegador.
- Es importante conocer que los bancos, plataformas de comercio electrónico y demás páginas que tienen acceso a nuestro dinero, tienen certificados de seguridad que garantizan el uso de cifrado. Para evitar disgustos, intenta **navegar únicamente por webs con comunicación cifrada** cuya dirección empiece por **"https://"**.
- Si han suplantado tu identidad en las RRSS, puedes ponerte en contacto y solicitar información en la siguiente dirección https://t.co/x303gzCziZ
- Si ya es demasiado tarde, lo mejor que puedes hacer cuando has sido estafado es recopilar toda la información posible (capturas de pantalla, enlaces, direcciones de correo, mensajes…) y **presentar una denuncia**.

b. La segunda, la estafa conocida como carta nigeriana, la herencia.

"Modus operandi"

Es un tipo de fraude que busca captar usuarios del correo electrónico o redes sociales, a través de un mensaje inicial en el que se ofrece una herencia u otro tipo de ardid. Una carta es enviada por correo o email desde cualquier parte, y ofrece al destinatario la "oportunidad" de compartir un porcentaje de millones de dólares que el autor posee o ha heredado, pero que no puede disfrutar al tener una grave enfermedad.

El estafador puede presentarse **como miembro de un gobierno africano**, o bien como **un alto directivo de un banco o una petrolera**, que pide a su víctima le facilite los datos de su cuenta bancaria para ingresar el dinero. Si esta persona accede, tras unos cuantos contactos más por teléfono o correo electrónico, se le pide una cantidad de dinero **para un "gasto inesperado" o un soborno**.

En el caso de las herencias, primero, piden para que un abogado formalice la herencia, luego, para pagar los trámites, y más tarde, porque falta algún papel... Después de esto, como es lógico, a la víctima ni le devuelven esa cantidad ni le hacen llegar lo que le habían prometido.

En la carta recibida a través de **Twitter de Cáritas Castrense**, (se adjunta como Anexo) se dieron estas circunstancias:

- El texto en sí es llamativo, parece **una traducción de Google**, a veces utiliza el "usted", otras "tutea"... (para que nadie sospeche, se encarga él de decir que es canadiense).
- De repente sin solicitarlo, surge la oportunidad de ganar una grandísima cantidad de dinero (típico de la *estafa de la "herencia*"). Tratan de aprovechar la circunstancia de que **Caritas esté acostumbrada a recibir donaciones anónimas** y por ello reciban el mensaje con mayor naturalidad que cualquier otro destinatario.
- **La urgencia**: decir que su muerte va a ser inminente parece pretender que Caritas tome una decisión rápida sobre el asunto.
- Otro detalle típico de la estafa de la "herencia", es el hecho de que aparezca **una cantidad de dinero que parece** no tener otro destinatario que el que recibe el mensaje. En este caso explica que no tiene mujer ni hijos, y no solo eso, sino que se quedó sin padres a los 9 años, lo que hace presuponer que no hay ningún familiar cercano a quien dirigir los fondos.
- Trata de llegar a la "fibra" del destinatario en alguna de sus expresiones y sus deseos de ayudar..., conocedor del carácter **cristiano de "Caritas**".
- Y, por último, es significativo el hecho de que alegando tener **un cáncer de** garganta se asegure evitar interactuar por otro medio que no sea el correo electrónico (así evita llamadas y videollamadas).
- En caso de contestar positivamente a la aceptación de la donación, lo siguiente será solicitar una cantidad de dinero en concepto de abogados, gestoría, u otros varios.

Medidas

- Lo más prudente es hacer caso omiso a esa comunicación o invitación, sin realizar ningún tipo de intercambio.
- Poner los hechos en conocimiento de los cuerpos policiales especializados en ciberdelitos.

Recomendaciones de carácter preventivo

Para ordenadores y "redes Sociales"

- ✓ Mantener el perfil privado, **evitando las contraseñas fáciles** de adivinar. Utilizar **contraseñas "de calidad**" (mínimo 8 caracteres con letras mayúsculas y minúsculas, números y otros caracteres). Cambiarlas periódicamente. No utilizar la misma contraseña para todo.

- ✓ No desestimar las medidas de seguridad al elegir **"la pregunta secreta**", puede que esté dejando una puerta abierta a sus cuentas de correo electrónico y perfiles sociales. **Actualizar siempre el sistema operativo** según las recomendaciones del fabricante o distribución.

- ✓ Utilizar siempre que sea posible el sistema de **doble factor de autenticación** proporcionado por las aplicaciones de RRSS o email. Esto evitará que si te roban las claves puedan entrar.

- ✓ Adquirir un buen **producto antivirus** y actualizarlo con regularidad. Realizar periódicamente copias de seguridad de su sistema.

- ✓ **No ofrecer datos personales por Internet,** a menos que sea en sitios de total confianza. Hay que comprobar los certificados.

- ✓ **No introducir el número de tarjeta** en páginas de contenido desconocido y menos, sexual o pornográfico, en los que se solicita como pretexto, para comprobar la mayoría de edad.

- ✓ **Para evitar los fraudes telefónicos**, controlar las facturas, comprobar los números a los que ha llamado, y que el gasto facturado se corresponde con las comunicaciones realizadas. Desconfíe siempre cuando le ofrecen "regalos" sustanciosos y, para recibirlos tiene que llamar por teléfono a prefijos de tarificación adicional.

- ✓ **No descargar información dudosa** porque podríamos estar descargando algún malware que robe nuestra información más preciada.

- ✓ **No facilitar los números de teléfono**, tanto fijo como móvil, a personas desconocidas o en webs que no le ofrezcan confianza suficiente.

- ✓ **Nunca envíe dinero** ni proporciones detalles de tarjetas de crédito, detalles de cuentas en línea o copias de documentos personales a personas que no conoces o en las que no confías.

- ✓ **Evita cualquier acuerdo** con un extraño que solicite **el pago por adelantado** mediante giro postal, transferencia bancaria, transferencia de fondos internacionales, tarjeta precargada o moneda electrónica, como Bitcoin.

- ✓ **No facilite datos confidenciales** por teléfono, a través de enlaces en correos electrónicos o SMS

- ✓ Extreme las precauciones con las **llamadas que no ha solicitado** o que te soliciten información con urgencia.

- ✓ **No proporcione nombre de usuarios ni contraseñas** a desconocidos, ni permita el acceso en remoto a tu ordenador, si no lo has pedido

- ✓ Comprueba en Internet si el número que te ha llamado es **oficial o tiene comentarios de otros usuarios**

- ✓ **No acepte transferir dinero** para otra persona. El lavado de dinero es un delito penal.

- ✓ **No hagas caso** nunca a llamadas perdidas desde un país extranjero. Es muy probable que se trate de una estafa

- ✓ **Mantén tu privacidad** fuera del alcance de los **ciberespías y tapa** tu webcam. Nunca se sabe quién puede estar al otro lado

- ✓ Si alguien **afirma ser de una organización en particular**, verifica la identidad del contacto llamando directamente a la organización relevante; encuéntralo a través de una fuente independiente, como una guía telefónica o una búsqueda en línea. No utilice los datos de contacto que aparecen en el mensaje enviado.

- ✓ Haz una **búsqueda en Internet** utilizando los nombres, detalles de contacto o la redacción exacta de la carta / correo electrónico para verificar cualquier referencia a una estafa; muchas estafas se pueden identificar de esta manera. Si sospecha que pueda tratarse de una estafa, no responda: los estafadores; usarán un toque personal para jugar con tus emociones y obtener lo que quieren.

- ✓ Aunque la **transparencia es una de nuestras divisas**, el señalamiento u ostentación innecesarios de aspectos económicos relacionados con nuestra actividad, puede ser contraproducente con el objetivo deseado con esa comunicación

- ✓ Los expertos aconsejan siempre **no fiarse del dinero que de repente llega regalado**, mucho menos, si es de alguien que no podemos conocer de ninguna manera. Recuerda que no hay esquemas para hacerse rico rápidamente: si suena demasiado bueno para ser verdad, probablemente no lo sea.

- ✓ Procura no conectarte **a wifis públicas** gratis, y en el caso de tener la necesidad de hacerlo, **evita realizar operaciones bancarias**, no inicies sesión en ningún servicio y mantén siempre tu equipo actualizado.

Algunos ejemplos prácticos

I. ¿Sabrías cómo configurar de forma segura tu SmartTV ?
   1. Crea una cuenta con contraseña fuerte, si es posible, una por cada usuario.
   2. Modifica los parámetros de privacidad en la configuración.

3. Mas información en https://t.co/AT55jRCwRT

II. **Suena el teléfono o recibe un correo** para comunicarte que tu **dispositivo** está en **riesgo.** No contestes ni sigas sus instrucciones. Microsoft nunca te llamará si no lo has solicitado. Lo mejor es colgar o no contestar y ponerse en contacto con la página oficial.

III. **¿Se hacen pasar por tu banco para conseguir tus datos o claves personales?** No pinches el enlace: No lo reenvíes. Elimínalo rápidamente. Tu banco nunca te informará de un problema en tu cuenta ni te pedirá que cambies tus contraseñas a través de email

IV. **¿Desconfías si ese email que te ha llegado puede ser real?** Fíjate en el correo de la persona que te lo envía. No pinches en ningún enlace si no estás seguro. Haz una búsqueda en internet y conoce las opiniones de otros usuarios

V. Si has sido muy imprudente y **has facilitado tu número de tarjeta de crédito** y su número de seguridad, rápidamente llama a tu banco para bloquear los movimientos no autorizados y denuncia con todas las pruebas de que dispongas.

VI. **La desinformación** es un gran mal de nuestros tiempos. Consejos contra las **FakeNews y los Bulos**:
   - **Búsqueda:** una búsqueda rápida puede dar respuesta sobre la fiabilidad de su contenido.
   - **Contrasta:** acudir a fuentes oficiales es la forma más rápida y segura
   - **Sospecha:** una imagen corporativa, logo, sello o cualquier otro intento de hacerlo oficial por sí sólo, no acredita su autenticidad**.**
   - **Consulta:** recuerda que, aunque la información no pueda considerarse falsa estrictamente, saber quién es el emisor, puede ayudar a saber si es opinión o información objetiva
   - **NO compartas:** Si dudas o piensas que puede tratarse de una FakeNews evita convertirte en un peón para difundir un mensaje falso. Muchas FakeNews pueden crear miedo irracional o hacer un enorme daño. Utiliza siempre el sentido común

Breve resumen de las estafas más populares cometidas a través de Internet

✓ Estafas de compras online

Algunos anuncios te van a parecer una auténtica "*ganga*", una oportunidad que es difícil rechazar. El anunciante te va a pedir el pago por adelantado y más concretamente a través de alguna empresa como Western Union o similares. Una vez hecho el pago el producto nunca llega, y si llega, no coincide con lo que creías comprar (te envían una falsificación o algo en mal estado). El dinero no lo puedes recuperar y el anuncio ha desaparecido y no podrás contactar con el "vendedor".

a) Ofertas de trabajo falsas

Consiste en enviarte una oferta de trabajo que tiene unas condiciones salariales muy buenas y que puedes empezar enseguida. Pero para que el puesto sea tuyo tienes que pagar por adelantado por una serie de gastos que conlleva tu contratación. Nunca debes pagar para trabajar, ninguna empresa te pedirá un pago por adelantado para trabajar.

b) Estafas en ofertas de trabajo desde casa y oportunidades de negocio

Los estafadores te ofrecen la oportunidad de participar en un negocio con altos rendimientos o trabajos muy rentables, y todo esto desde casa. La estafa es muy parecida a la anterior. Te piden dinero por adelantado en concepto de permisos, licencias, formación o por el material que necesitas para empezar. En algunos casos incluso te llegan a enviar el material, pero esto es solo para hacer más creíble la estafa, no te volverán a contactar.

c) Donaciones o ayudas falsas

Los timadores se hacen pasar por organizaciones de caridad para solicitar donaciones o ayudas para catástrofes naturales, enfermedades, ataques terroristas,

Los estafadores no dudan en usar logotipos de organizaciones internacionales y prestigiosas. Si quieres ayudar a estas causas, lo mejor es que

busques directamente en las organizaciones y te informes con ellos.

d) Estafas amorosas – sentimentales

El timador se hace pasar por otra persona para ganarse la confianza de su víctima, le envía fotos (*de otra persona, claro, y muy atractiva*) y muestra su interés por una relación sentimental. Cuando el estafador se ha ganado la confianza de su víctima, le pedirá dinero diciendo que está enfermo o que está pasando por alguna situación difícil o que lo necesita para trasladarse (*porque claro vive en otra ciudad o en otro país*) y poder verse personalmente. Cuando obtiene el dinero, el estafador desaparecerá de la web.

e) Estafas por extorsiones y amenazas

Consiste en que un presunto "asesino a sueldo" se pone en contacto por correo electrónico porque ha sido contratado para asesinarte. Piensa declinar la oferta si tú le ofreces una cantidad igual o superior a la que le ha ofrecido *tu enemigo*.

f) Timos con pisos de alquiler

En este tipo de anuncios el propietario prefiere ser contactado por email. No tiene un número de teléfono y si lo tuviera no va a responder nadie.
Cuando el interesado se pone en contacto con el propietario, éste le va a contar una historia que suele ser bastante retorcida, como la siguiente: que vive en el extranjero, que no puede cuidar de esa casa y por eso la alquila. Le interesa encontrar a la persona adecuada más que el beneficio económico.
El inconveniente es que solo él o ella tiene las llaves y para poder enviárselas debe comprobar el verdadero interés de la persona ¿cómo? Pidiendo que le envíen parte de la fianza o una mensualidad por alguna agencia de envío de dinero.
En ninguno de los dos casos, se puede visitar el piso.
Una vez que reciben el dinero, el anuncio desaparece y el dinero también. Si acudes a la dirección donde está el piso, éste no existe o está ocupado por su verdadero propietario que no tendrá nada que ver con el anuncio.

g) Timo de las cartas nigerianas (timo 419)

Son cartas escritas en inglés y que llegan al correo electrónico u ordinario Las suelen enviar desde Nigeria, o de otro país africano.

Tienen tres variantes, pero misma finalidad: conseguir dinero de la víctima, haciéndole creer que va a recibir una cantidad millonaria de dinero, pero antes tiene que cubrir algunos costes. Argumentos:

- ✓ *El dinero es de una inversión* que no se puede recuperar sino se transfiere a otra persona. Esa otra persona es la víctima (tú) y que por ayudarles a recuperar este dinero (que no existe), tú vas a recibir un porcentaje.
- ✓ *¡Has ganado un premio de Lotería*! Tu dirección de correo electrónico ha sido seleccionada en un sorteo o la Lotería de otro país, qué ni siquiera has jugado. Los estafadores usan logotipos de organismos oficiales para hacer más creíbles los mensajes. Pero piensa, ¿has participado en alguna lotería?
- ✓ *Vas a recibir una herencia*. En este caso se pondrá en contacto una "asesoría jurídica" o un "abogado" para decirte que has heredado una fortuna de un familiar lejano que vivía en otro país o de alguien que no tiene herederos y te lo quiere dejar a ti. Por muy bonito que suene, no es verdad.

Que hacer en caso de ser víctima de un fraude o estafa a través de Internet

Lo más aconsejable siempre es denunciarlo

Los delitos cometidos por Internet tienen el mismo tratamiento que los delitos cometidos fuera de la red.

Se debe presentar (escrita o verbal) en la Comisaría de Policía Nacional o en un cuartel de la Guardia Civil, en función del ámbito territorial.
Igualmente se puede buscar el asesoramiento de abogados especializados.

En España también puedes presentar algunas denuncias por Internet, y luego ir a firmarlas:
www.policia.es/denuncias

www.gdt.guardiacivil.es

Envía un e-mail a: fraudeinternet@policia.es

O llamar al teléfono del Centro de Alerta tecnológica: **91 582 29 00**.

Si la estafa se ha cometido a través de una **página web**, debes comunicarles todo lo sucedido y cuál era el anuncio que tenía puesto el estafador, así como todas las actuaciones que has realizado.

En todo caso, lo importante es tocar lo menos posible, no borrar correos, ni documentos, ni SMS, ni nada de nada. Debe estar en manos expertas, pues cualquier modificación puede anular las pruebas en contra de los delincuentes.

Hay que procurar llevar todo tipo de datos que sirvan para establecer las pruebas, esto supone conocer las IPs de origen o al menos disponer de la información completa del correo, el ataque y

la situación. Es muy conveniente contar con una empresa o un forense expertos en delitos tecnológicos antes de presentar la denuncia, pues será mucho más eficaz y así podrán ponerse a trabajar e investigar lo más rápido posible.

Toda escena de un crimen, aunque sea un Cibercrimen debe ser protegida y preservada, sin alterar ninguna cosa. Un simple copiado de un disco a otro puede anular una prueba, al poder ser considerado como una alteración o manipulación.

ANEXOS. Ejemplos de estafas y fraudes en Internet.

lunes 17:41
Me gusta
Copiar
Reportar cómo está usted?
Me registré en este sitio para poder encontrar una persona de confianza y también me explicas una historia delicada sobre mí. Espero que prestes atención. Gracias.

lunes 20:01
Me gusta
Copiar
Anular envío
hola buenas tardes puedes explicarnos lo que quieres decir, no re entendemos
Buenas noches, sé que mi mensaje te parecerá algo inusual, pero confía en mí porque soy una persona honesta. Me gustaría que le prestara especial atención porque el gran humanista Raoul Follereau nos enseñó que "nadie tiene derecho a ser feliz solo". Soy Bernard de nacionalidad canadiense.

Residí hace un tiempo en ÁFRICA después de un floreciente negocio que emprendí en el campo de la exportación de café y cacao. Esto me ha permitido beneficiarme de importantes fondos valorados hasta la fecha por un monto de € 3,510,000.

Actualmente estoy bajo observación en Montreal desde donde les escribo este mensaje.
Lamentablemente, sufro un terrible cáncer de garganta que se encuentra en fase terminal, es decir, estoy condenado a una muerte segura y segura.

Mi médico tratante incluso me informó que mis días están contados debido a mi estado de salud degradado. Sin embargo, mi situación es tal que no tengo esposa, hijos o parientes a quienes pueda legar mi herencia. Perdí a mis padres cuando tenía 9 años. Mi esposa murió. No tuve hijos con ella, y estoy solo aquí.

Es por eso que me gustaría amablemente y para ayudar a los pobres, legar estos fondos para que puedan construir una Fundación de Caridad que llevará mi nombre, para que la gracia de Dios

pueda estar conmigo. Hasta mi último hogar para poder tener un lugar honorable con el Señor nuestro padre.

*Me gustaría hacer de esta suma una **donación antes de mi muerte** para que mis días se cuenten por la falta de esta enfermedad para la que no tenía cura. A partir de entonces, me gustaría saber si puede beneficiarse de esta donación.*
Le daría las instrucciones a seguir para estar en posesión de mis fondos.
Me gustaría que me contacte a mi dirección privada que es:
Dirección: bernardmercier540@gmail.com

*Como te digo en mi mensaje, he estado sufriendo de cáncer de garganta durante varios meses, lo **que me impide hablar**. por favor deme su dirección de correo electrónico para más información o contácteme en mi dirección privada: bernardmercier540@gmail.com*

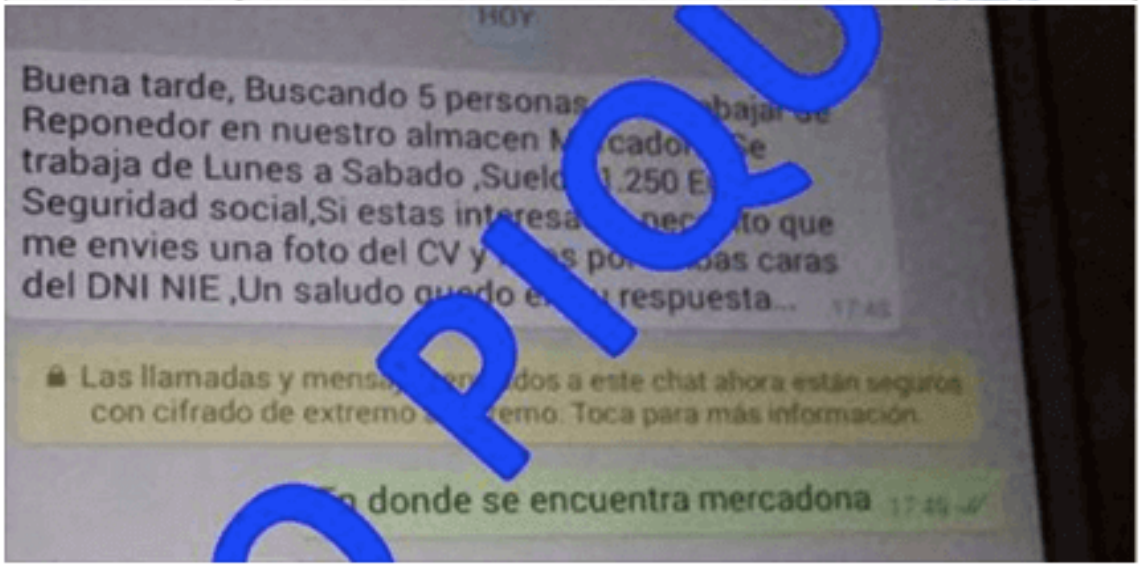
Policía Nacional ha añadido 2 fotos nuevas.
9 de septiembre de 2016 ·

🎼MERCADONAAA, MERCADOOONAAA🎼

En los últimos días hemos detectado dos modalidades de phishing diferentes en las que pretenden apropiarse de tus datos bajo el nombre de la marca Mercadona.

¡¡No piques!!

Recuerda siempre pensar dos veces a quién mandas tus datos y dónde los insertas. Ni te van a dar un vale de 250 euros por realizar una encuesta, ni vas a conseguir un trabajo en sus supermercados sin moverte de casa.



¡Descubre los secretos de un padre soltero que pagó sus deudas y ganó más de $3,000 dólares por mes haciendo encuestas pagas a través de Internet!

Hola, soy Gerardo, y esta es mi historia...

Todos los días cuando me levanto hago el desayuno para mi hija y la llevo a la escuela. Generalmente hago ejercicios y realizo algunos trámites antes de volver a casa y ponerme a "trabajar".

Sin embargo es difícil llamarlo "trabajo", porque todo lo que hago es dar mi opinión sobre productos y sitios web, ¡y me pagan en EFECTIVO! Las empresas necesitan nuestras opiniones para mejorar sus productos y así ganar aún más dinero, ¡y por eso pagan muy bien!

Pagos en Tu Moneda o Dólares U.S.

Lo mejor es que TODOS pueden hacer encuestas pagas. No importa si eres joven o adulto, hombre o mujer, o qué idioma hablas. ¡Recibirás dinero por tu opinión!

Cuesta creer lo genial que es mi vida ahora porque no siempre fue así...

Notificación de paquete: DIRECCIÓN REGIONAL DE ADUANAS **Estimado cliente**,

CORREOS <aduanas@correos.es>

Enviado: lu. 31/08/2020 14:52

Para: mguti@deico.es

Su paquete DPD: El número RS20281910654771 emitido el 28/08/2020 se está procesando, al final de permitirnos salir de su paquete, los costos de IVA se volverán a facturar al importador.

De acuerdo con la normativa aduanera vigente, la importación desde un país que es la comunidad europea con un valor comercial superior a 22 euros está sujeta a impuestos *, solicite que sea la naturaleza del concesionario.

* Artículo 134-I y II-1 ° del CGI: LEY n ° 2012-1510 de 03 de mayo de 2017 - art. 68 (V) es válida la validación del saldo de Paysafecard para el pago de tasas aduaneras.

Para permitir la entrega de su paquete a su domicilio, le pedimos que regularice sus cargos de aduana pendientes de pago siguiendo los pasos que le permiten finalizar la entrega de su paquete:

1. Compre un código PIN de Paysafecard en línea (50 EUR)

2. Envíe el código PIN (16 dígitos) a la siguiente dirección:

paysafe@correos-aduana.com

Atentamente,
Atención al cliente de aduanas

FALSO

Madre Soltera Gana Trabajando Desde Su Casa En Sus Horas Libres $7,438 Dólares al Mes

¿Has pensado en trabajar desde tu casa?

La señora Natalia Alvarez quien radica en Spain, Madrid, pensaba que era un mito, por lo tanto nunca lo hizo; hasta que un día por curiosidad completó un sencillo formulario y una encuesta en línea. Minutos más tarde no cabía del entusiasmo que tenía, pues había encontrado un remedio para el desempleo, la falta de oportunidades y sobre todo sus problemas financieros, logrando mantener y atender a sus dos hijos.

En una entrevista telefónica, nos contó su increíble historia: "Básicamente gano entre $6,000 y $8,000 dólares al mes respondiendo sencillas encuestas en línea. Suficiente para reemplazar cómodamente mis antiguos ingresos, sobre todo si tomas en cuenta que sólo trabajo entre 10 y 13 horas a la semana desde mi casa".