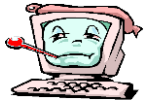
Principales riesgos y amenazas en Internet y RRSS.

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, casi todos Se propagan a través de mensajes populares, principalmente en Facebook,

Virus: Son códigos maliciosos, gusanos y troyanos usados para acceder al equipo de la víctima y robar información



Phishing: Esta modalidad consiste en el robo de información a través de la suplantación de identidad, en redes sociales, 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 en las redes sociales, se puede caer en el ojo de un acosador se puede acceder a todo lo que publicamos y convertirse en un riesgo para la integridad de nosotros mismos**.**

Robo de Informacion En RRSS compartimos información: dónde vivimos, con quién estamos, dónde estamos, qué compramos, no es gran riesgo mayúsculo, pero con estos datos muchos cibercriminales acceden a personas cercanas y atacarlas

Spam o correo basura Son mensajes no deseados. A veces, el spam es publicidad que nadie pidió, pero también puede incluir **malware**, malicioso

Dic 2020

Cáritas Castrense

TRIPTICO DE SEGURIDAD EN INTERNET Y REDES SOCIALES

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*

www.caritas.es/castrense

Informacion nociva Internet contiene mucha 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: "Felicidades has ganado 1 millón de euros" Internet es una forma muy sencilla de llegar a mucha gente, utilizan anuncios para robar información de cuentas bancarias. Millones de personas en el mundo han sido víctimas

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. los piratas cibernéticos roban la información de nuestras cuentas, cambian los accesos, 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

Modalidades de estafas/ fraudes, detectadas en Cáritas:

La suplantación de identidad, clonación o phishing: Consiste en s**uplantar la identidad de una empresa o entidad. Lo básico** es elegir **una**

marca en la que los usuarios confíen y copiarla lo mejor posible.

mismo ocurre En la mayor parte de las veces los ataques **comienzan con un simple correo electrónico**. "*Tu banco solicita tus datos para……*. El email puede contener **textos originales, imágenes oficiales y enlaces** que, en un principio, nos pueden parecer confiables.

Lo 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.

Caso real 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.

La estafa conocida como carta nigeriana, la herencia fraude que busca captar usuarios, a través de un mensaje inicial en el que se ofrece una herencia u otro tipo de ardid y ofrece al destinatario la "oportunidad" de compartir 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.

Medidas en ambos casos

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.

evitar el acceso a cualquier web a través de un enlace, en especial si lo hemos recibido por alguna de las vías antes dichas. I**ntroducir la URL original directamente en la barra de direcciones** del navegador.

Navega 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

lo mejor que puedes hacer cuando has sido estafado es recopilar toda la información posible (capturas de pantalla, enlaces, direcciones de correo, mensajes…) y 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

No desestimar las medidas de seguridad al elegir "la pregunta secreta",

Actualizar siempre el sistema operativo.

Utilizar siempre que sea posible el sistema de doble factor de autenticación. Esto evitará que si te roban las claves puedan entrar.

Adquirir un buen producto antivirus y actualizarlo con regularidad.

No ofrecer datos personales por Internet

No introducir el número de tarjeta en páginas de contenido desconocido

Para evitar los fraudes telefónicos, controlar las facturas, **No descargar información dudosa** ni **facilitar los números de teléfono**, y **Nunca envíe dinero. Evita cualquier acuerdo** con un extraño que solicite **el pago por adelantado** mediante giro postal, transferencia bancaria.

No facilite datos confidenciales. Cuidado con las llamadas que no has solicitado o perdidas desde el extranjero.

No proporciones nombres de usuarios o contraseñas. NO aceptes transferir dinero el blanqueo de capitales es un delito.

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

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

Estafas de compras online

Ofertas de trabajo falsas o Estafas en ofertas de trabajo desde casa y oportunidades de negocio Donaciones o ayudas falsas

Estafas amorosas, sentimentales, Estafas por extorsiones y amenazas, Timos con pisos de alquiler o de las cartas nigerianas

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.

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 el anuncio que tenía puesto el estafador, así como todas las actuaciones que has realizado.

En todo caso, lo importante, 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