

¿POR QUÉ ES TAN IMPORTANTE LA CIBERSEGURIDAD?

Las tecnologías de la información y las comunicaciones (TIC) y, en particular, el uso de Internet nos han facilitado mucho la vida, pero debemos ser muy prudentes con el uso de la información que depositamos en la red, puesto que si no adoptamos las medidas de seguridad apropiadas, seremos vulnerables, y podremos ser atacados por los ciberdelincuentes.

Los ciberdelincuentes, que son conocedores de esta situación de vulnerabilidad, aprovechan la falta de concienciación o de conocimiento en ciberseguridad de la población para tratar de descubrir nuevas vías de acceso a nuestros dispositivos y materializar sus ataques. Solo si sabemos actuar frente a estas amenazas, podremos estar más seguros y protegidos.

Un aspecto que adquiere especial relevancia en el ámbito de la ciberseguridad son las estafas, ya que suponen aproximadamente el 90 % de los delitos informáticos que se cometen en la actualidad. También existen otros delitos informáticos, como las injurias y las calumnias, las amenazas, el acoso o, incluso, la distribución de pornografía infantil, que utilizan las TIC como elemento facilitador de su comisión.

En el caso de sufrir un delito debemos DENUNCIAR.



¿CÓMO PODEMOS DENUNCIAR?

Informar: si observas la comisión de alguna acción irregular que pudiera ser sospechosa de una infracción administrativa o penal.

colabora@guardiacivil.org

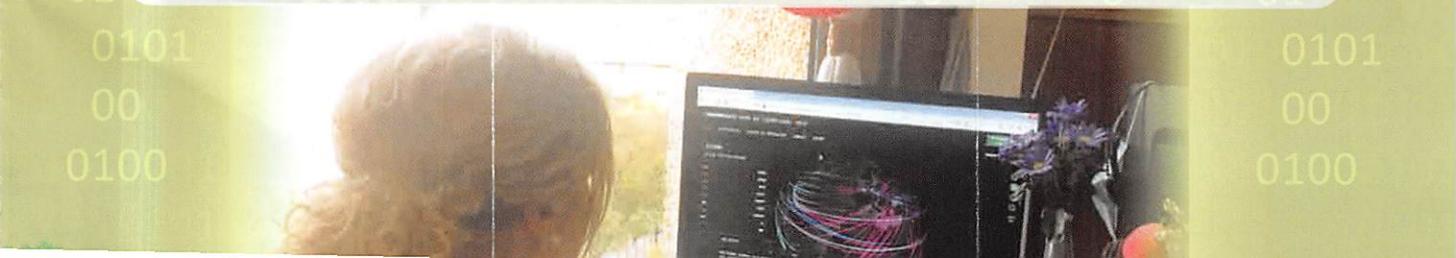
Denunciar: si deseas presentar una denuncia formal, teniendo la posibilidad de certificar los contenidos que deseas adjuntar a la misma, puedes hacerlo de forma presencial en los diferentes Puestos de la Guardia Civil o través de la página web oficial.



CREACION DE LOS EQUIPOS @

La Guardia Civil ha creado los Equipos @. Estos equipos se encargan de asesorar, de prevenir y de proporcionar una respuesta ante la ciberdelincuencia, en particular, ante las estafas en la red, que, como se ha dicho, constituyen uno de los principales problemas en este ámbito.

Se encuentran en todas las provincias, y una de sus funciones es asesorar y proporcionar atención presencial y a distancia a los ciudadanos y empresas, por lo que se puede acudir a ellos ante cualquier duda o cuestión.





GUARDIA CIVIL

CULTURA CIBERS

ATAQUE DE DENEGACIÓN DE SERVICIO (DOS O DDOS)

Una de las principales utilidades de las botnets son los ataques de denegación de servicio o DoS, por su acrónimo del inglés (Denial of Service). Los servidores que ofrecen servicios en internet están dimensionados por un número determinado de usuarios clientes. Imaginemos un periódico digital. Tendrá un estudio de audiencia y sabrá que sus clientes diarios pueden ser, imaginemos 10.000. Para ello, el servidor al que se conectan los clientes debe estar dimensionado para recibir peticiones de un mínimo de 10.000. Portales de comercio electrónico como Amazon deberá estar dimensionado para muchísimos más clientes. Pero si en un momento determinado, se supera el límite de clientes que acceden a un servidor, este no puede responder a todos y se bloquea, produciéndose una denegación de servicio.

BOTNET

Como se explica en los troyanos, éstos tienen un auge espectacular con el fraude en banca electrónica, llegándose a hablar de troyanos bancarios. Lo que hacían estos programas maliciosos era entrar en el equipo de la víctima para robar las claves de acceso a banca electrónica. Pero una vez dentro, las posibilidades eran muchas. El delincuente podía controlar remotamente el equipo informático de la víctima, que se convertía en un robot o zombi a merced del delincuente. Y eran tantos los ordenadores que un delincuente infectaba que disponía de legiones de equipos zombi o robots a su antojo para ordenarles remotamente, a la vez, realizar cualquier cosa, mandar un email, atacar a un tercero, conectarse a una página web, etc. Son redes de robots (BOT NET en inglés) a merced de un delincuente. Se han llegado a descubrir botnets de millones de equipos infectados.

CARTAS NIGERIANAS

Una de las estafas informáticas más habituales son las cartas nigerianas. Suelen ser email no deseados en que nos informan de una oportunidad, a veces no legal, de obtener grandes beneficios. Una herencia millonaria de un fallecido sin herencia, una bolsa de dinero extraviada en algún conflicto armado. Otras veces son mensajes con alta carga emocional que nos inducen a pagar, como ayudar a personas que están pasando una situación grave y desesperada, o hacerse cargo de un cachorro o mascota por el que luego nos irán solicitando aportaciones económicas para supuestos trámites aduaneros. La casuística es muy amplia. Adquieren el nombre de cartas nigerianas porque, inicialmente, grupos de delincuentes nigerianos se especializaron en esta modalidad de fraude, estafando a multitud de víctimas a lo largo de todo el mundo. En ocasiones también se conoce a este fraude como el "scam del 419" (timo del 419), en alusión al artículo del código penal nigeriano que tipifica las estafas, el 419.

CIBERACOSO SEXUAL

Por ciberacoso entendemos el conjunto de acciones que buscan acosar sexualmente a terceros a través de mensajes de correo electrónico, mensajes en redes sociales, llamadas telefónicas, mensajes de telefonía, o cualquier medio similar. El objetivo del acoso es obtener el favor sexual, ya sea para envío de imágenes de contenido sexual o para encuentros reales. Normalmente el ciberacosador elige a la víctima acercándose a ella a través de las redes sociales, y mediante estrategias de engaño bien elaboradas, obtienen información para obligar a la víctima a ofrecerle imágenes de contenido sexual. Cuando hablamos de menores, a estas conductas se las conoce como grooming. Si nos referimos a adultos, se conoce como stalking, y la mayoría de las veces tienen su origen en relaciones de parejas rotas.

CIBERDELITOS

No hay un criterio claro para identificar cuáles son los ciberdelitos. El Consejo de Europa, en su Convenio sobre ciberdelincuencia, del año 2001, y sus correcciones, establece que los delitos informáticos son los siguientes:

- Delitos contra los derechos de propiedad intelectual e industrial, cometidos a través de internet, es decir, la piratería.
- Los delitos de falsificación y fraudes en la red, las estafas.

CIBERBULLYING

El ciberbullying consiste en acosar, insultar o ridiculizar a menores mediante el envío de correos electrónicos, llamadas telefónicas, sms, mensajes en redes sociales, o cualquier otro medio tecnológico similar, y que atormentan, humillan, amenazan o molestan a la víctima, generándole estrés psicológico que puede inducirle a males mayores.

DARK WEB

Existe el error de asociar la Deep Web a contenidos delictivos, pero no es así. El no estar indexado para poder acceder a ellos a través de los navegadores convencionales no significa que sea delictivo o ilícito. Solo una parte de la Deep Web es de contenidos delictivos o ilícitos, es la que conocemos como Dark Web, la web oscura. Contenidos de pornografía infantil, markets de venta de tarjetas, de datos bancarios y personales, ofertas de servicios ilegales, sicarios, tráfico de órganos, venta de droga, etc son contenidos propios de la dark web.

DEEP WEB

El concepto Deep Web hace referencia a toda aquella información que existe en la red de redes, internet, que no es accesible a través de los navegadores convencionales. Es la información que no está indexada. Desde la parte privada de nuestras redes sociales hasta los contenidos de la red TOR forman parte de la Deep Web. Se calcula que aproximadamente el 90 % de todo lo que está en internet, si bien es tan grande que es imposible determinar con exactitud cuál es su alcance. Se suele utilizar el símil de iceberg, que oculta bajo el agua más parte de hielo del que se ve en la superficie.

FRAUDE EN BANCA ELECTRÓNICA

Es habitual confundir el phishing con el fraude en banca electrónica. El fraude en banca electrónica es la suplantación de nuestra identidad para ordenar transferencias no consentidas a terceros, es decir, sacar el dinero de nuestra cuenta. Normalmente se manda a terceros conocidos por mulas, cuya única misión es estar atentos a la recepción del dinero en su cuenta, sacarlo y remitirlo por otro canal a los autores del fraude, que, lo más habitual es que estén en el extranjero. El phishing es el primer paso. A través del phishing roban nuestra identidad electrónica para luego suplantarlos y realizar el fraude en banca electrónica.

HACKER

El concepto de hacker se acuñó en los albores de internet, cuando el acceso ésta se realizaba mediante conexión telefónica y por la que se pagaba por consumo realizado. Hacía referencia a aquellos que atraídos por la red, y con dificultades por el consumo telefónico, accedían a través de terceros, defraudando a terceros. Desde que se abarató el acceso, esto ya no existe.

El desconocimiento generalizado de las TIC y una imagen idealizada del personaje que, desde su garaje desarrolla programas informáticos que luego vende y se hace millonario, o accede desde su ordenador a cualquier lugar de la red, superando las barreras de seguridad, han llevado a una concepción romántica del hacker, visto como una persona sin intenciones maliciosas. Y cuando empiezan los fraudes en la red y el robo de datos personales, ya no se habla de hackers, sino de piratas informáticos.

La realidad es que existen personas con habilidades especiales para el mundo de las TIC, muchos de los cuales, con inquietud y ganas de aprender, buscan superarse en la red encontrando los errores de los sistemas informáticos, para mejorarlos. Y estos se proclaman hackers.

Pero también es una realidad que otros, con las mismas habilidades y potencial, sus acciones las orientan con fines delictivos. Y ellos también se proclaman hackers.

Lo que está claro es que hay expertos informáticos que ayudan a mejorar y perfeccionar el escenario de las TIC y que hay otros expertos informáticos que se dedican a delinquir en la red, que son ciberdelincuentes. Ambos se autoproclaman hackers. Digamos pues que hay hackers buenos y malos.

