



GUÍA DELITOS TELEMÁTICOS



2018



FUENTES CONSULTADAS:

OEDI (Observatorio Español de Delitos Informáticos).

EDITADO: GUARDIA CIVIL M.A. (SALAMANCA)



GUÍA DELITOS TELEMÁTICOS 2018.

- **¿QUE ES EL CIBERDELITO?**

Delitos cometidos a través de cualquier medio tecnológico.

- **¿QUE ES EL ENGAÑO O CEBO?**

Señuelo para atraer, tentar, seducir, persuadir con mañas, hacer caer en una trampa... Se usa en el entorno de los pederastas en Internet para hablar de su forma de convencer a los niños de que se encuentren con ellos fuera de la Red.



TÉRMINOS EMPLEADOS:

GUSANO:

Es un programa que se trasmite a sí mismo activamente por una red (se dice que es "autorreplicante"). No requiere ninguna intervención del usuario para extenderse ni "escondarse" en ningún programa. Tienen en como con los virus que su principal función es reproducirse, pero los gusanos en lugar de meterse dentro de otros archivos, crean copias de sí mismos. Pueden realizar acciones adicionales malignas.

HACKER:

La denominación HACKER es utilizada de forma errónea para asociarla con los piratas informáticos o ciberdelincuentes. Los HACKERS son personas inquietas con habilidades, ganas de aprender cosas nuevas para superar un reto o barrera, normalmente son expertos en sistemas informáticos con o sin estudios universitarios.

MALWARE:

Cualquier tipo de software dañino o con malas intenciones.

GUERRAS DE AVISOS:

Batallas entre usuarios de Internet a base de provocaciones que dan lugar a advertencias de los proveedores de acceso por violar las condiciones de utilización, normalmente utilizado por gente que busca reventar un espacio ya sea un foro, como un diario de noticias, etc... hay de muchos tipos de perfiles detrás de cada persona desde los simples TROLLS, hasta grupos organizados para sabotear a la competencia previo pago del servicio, Debunkers que cobran por desinformar o cambiar opiniones políticas o de otro ámbito a través de internet.



GUÍA DELITOS TELEMÁTICOS 2018.

ADWARE:

Componente de un programa que instalamos, en el cual va escondido, que muestra anuncios publicitarios, en ocasiones puede recabar datos acerca de nuestra actividad.

ANONIMIZADOR:

Servicio proxy que permite navegar sin que se sepa la IP del cliente.

CIBER BULO:

Es un mensaje de correo electrónico que alerta sobre un virus inexistente. También se conocen como hoaxes o falsas alarmas, y no son más que bromas y/o intentos de causar pánico entre usuarios inexpertos.

CRAWLER:

Programa que recorre Internet a la caza de direcciones de correo electrónico, normalmente para luego convertirlas en objetivo del spam.

CRAKER:

Aquel que rompe la seguridad de un sistema.

SNIFFER:

Programa que espía las comunicaciones de Internet, por ejemplo, para encontrar números de tarjetas de crédito. Las agencias de seguridad también los utilizan con fines de espionaje, contraterrorismo, etc.

FLAME O FLAMING:

Mensaje incendiario enviado a un foro, lista de correo o tablón de mensajes para provocar y obtener una respuesta indignada de cualquiera de los participantes o de alguno/a en particular. En general, mensaje insultante u ofensivo. Muy empleado por los TROLLS de internet.

PHISING:

Prácticas utilizadas para obtener información confidencial (como números de cuentas, de tarjetas de crédito, contraseñas, etc.).



GUÍA DELITOS TELEMÁTICOS 2018.



DELITOS TELEMÁTICOS SEGÚN CÓDIGO PENAL

ACCESO E INTERCEPTACIÓN ILÍCITA

CÓDIGO PENAL:

Art. 197 a 201. Delito de descubrimiento y revelación de secretos a través del acceso y difusión sin consentimiento de sus respectivos titulares de datos registrados en ficheros o soportes informáticos.

Art. 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial).

TIPO DE HECHO

DESCUBRIMIENTO/REVELACIÓN DE SECRETOS

ACCESO ILEGAL INFORMÁTICO

INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA

CÓDIGO PENAL:

Arts. 264 (Daños informáticos).

TIPO DE HECHO

ATAQUES INFORMÁTICOS

FALSIFICACIÓN INFORMÁTICA

CÓDIGO PENAL:

Arts. 386 y sucesivos, 401

TIPO DE HECHO

FALSIFICACIÓN DE MONEDA, SELLOS Y EFECTOS TIMBRADOS

USURPACIÓN DEL ESTADO CIVIL



GUÍA DELITOS TELEMÁTICOS 2018.

FRAUDE INFORMÁTICO

CÓDIGO PENAL:

Arts. 248 a 251.

TIPO DE HECHO

ESTAFA BANCARIA

ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQUES DE VIAJE

OTRAS ESTAFAS

DELITOS SEXUALES

CÓDIGO PENAL:

Arts. 183.ter y sucesivos

TIPO DE HECHO

PROVOCACIÓN SEXUAL

CORRUPCIÓN DE MENORES/INCAPACITADOS

PORNOGRAFÍA DE MENORES

DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 16 AÑOS CON FINES SEXUALES

CONTRA LA PROPIEDAD INDUSTRIAL E INTELECTUAL

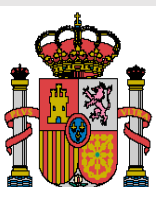
CÓDIGO PENAL:

Arts. 270 a 277 (Contra la propiedad intelectual y contra la propiedad industrial)

TIPO DE HECHO

DELITOS CONTRA LA PROPIEDAD INDUSTRIAL

DELITOS CONTRA LA PROPIEDAD INTELECTUAL



GUÍA DELITOS TELEMÁTICOS 2018.

CONTRA EL HONOR

CÓDIGO PENAL:

Arts. 205 y sucesivos.

TIPO DE HECHO

CALUMNIAS

INJURIAS

AMENAZAS Y COACCIONES

CÓDIGO PENAL:

Arts. 169 a 172

TIPO DE HECHO

AMENAZAS

COACCIONES

ENLACES DE INTERES:

OBSERVATORIO ESPAÑOL DE DELITOS INFORMÁTICOS:

<http://oedi.es>

GDT UCO (GRUPO DE DELITOS TELEMÁTICOS):

https://www.gdt.guardiacivil.es/webgdt/home_alerta.php





GUIA SOBRE DELITOS DE ACOSO: SEXTING, STALKING, CHILD GROOMING Y BULLYING.

SEXTING

Artículo 197.7 del Código Penal.-

Es el envío de imágenes, vídeos de contenido sexual, erótico e íntimo a través de cualquier medio (Mensajes, Facebook, Whatsapp etc...). Este delito se comete aunque medie consentimiento de la víctima en la obtención de las fotografías o vídeos.

EJEMPLO:

- 1- Persona que mantiene una relación sexual esporádica con otra, lo graba en vídeo con el consentimiento de la otra persona y luego lo difunde por Whatsapp.
- 2- Persona que manda fotografías de contenido sexual propio a otra y ésta las difunde a terceras personas.

Cosas a tener en cuenta:

Para que exista este Delito, las imágenes o grabaciones audiovisuales se tienen que difundir, revelar o ceder a terceras personas, tiene que ser **SIN AUTORIZACIÓN** de la persona afectada, las imágenes o vídeos tienen que ser obtenidos en un ámbito privado, fuera de la mirada de terceras personas. Tienen que menoscabar gravemente la intimidad de la persona.



STALKING (sólo perseguible mediante denuncia).-

Artículo 172 Ter del Código Penal.-

Consiste en acosar o acechar de forma insistente y reiterada a otra persona mayor de edad. Si se tratara de una persona menor de edad, estaríamos ante un delito de BULLYING.

EJEMPLO:

- 1- Persona que llama 20 veces al día a otra, sin que medie consentimiento por su parte.
- 2- Persona que sigue continuamente a otra (lugares públicos, lugar de trabajo, domicilio, lugares de ocio).

Cosas a tener en cuenta:

Para que exista este Delito, tiene que existir hacia la persona perjudicada:

Vigilancia, intentar la cercanía física, persecución, establecer contacto mediante medios de comunicación o terceras personas, que mediante el uso indebido de sus datos personales se adquieran productos o mercancías, o se contraten servicios, que haga que terceras personas se pongan en contacto con ella, o bien, que se atente contra el patrimonio, su libertad o de personas cercanas a la víctima.



CHILD GROOMING

Artículo 183 Ter del Código Penal.-

Es el engaño o embaucamiento a personas menores de **16 años**, a través del teléfono, internet o cualquier tecnología de la información, para conseguir que el menor participe en un fin sexual u obtener material pornográfico.

EJEMPLO:

- 1- Una persona de 30 años que a través de las redes sociales embauca a un/a menor de 15 años para mantener relaciones sexuales.
- 2- Persona mayor de edad que contacta con menor de 16 años mediante Facebook, haciéndose pasar por otro menor, lo embauca para conseguir datos personales o íntimos del mismo, los cuales usa para chantajearle y conseguir material sexual (fotografías, vídeos).

Cosas a tener en cuenta:

Para que exista este Delito, se tienen que tratar de menores de **16 AÑOS**, tiene que tener un fin exclusivamente sexual, o la finalidad de recabar material pornográfico, tiene que proponer al menor, mediante contacto por cualquier medio, un encuentro con fines sexuales y que este se acompañe de actos encaminados al acercamiento, o bien para conseguir material erótico o sexual del menor.



BULLYING (ACOSO ESCOLAR) - CIBERBULLYING.

Artículo 172 Ter del Código Penal

Es toda forma de maltrato físico, verbal o psicológico que se produce entre menores de una forma reiterada en el ámbito escolar.

El CIBERBULLYING es el acoso efectuado a través de internet o telefonía móvil.

EJEMPLO:

- 1- BULLYING VERBAL: Un/a menor que en su centro educativo, recibe adjetivos descalificativos por un grupo de menores debido a su exceso de peso.

- 2- BULLYING FÍSICO: Un/a menor que recibe una bofetada de cada componente de un grupo de 4 compañeros de clase, con cierta frecuencia.

- 3- CIBERBULLYING: Un/a menor que recibe mensaje ofensivos e insultantes a través de Facebook, Twitter o cualquier red social.