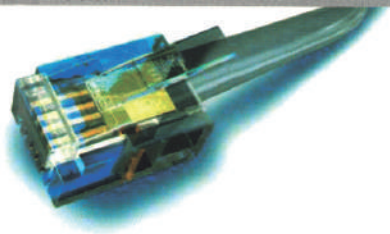
DELINFO.

GUÍA DE SEGURIDAD PARA PREVENIR Y CONTROLAR DELITOS INFORMÁTICOS



Autor :
MAGISTER LUÍS CARLOS REVELO TOVAR

Co Autores:
ING.DAVID ANDRES CALVACHE DIAZ
ING.JOSE VICENTE MAYAG RODRIGUEZ
ING.VICTOR HUGO ORTEGA MARTINEZ

INSTITUCIÓN UNIVERSITARIA DIOS CIENCIA Y SERVICIO CESMAG

NARIÑO Gobernación

GUIA DE SEGURIDAD PARA PREVENIR Y CONTROLAR DELITOS INFORMATICOS

LUIS CARLOS REVELO TOVAR
DAVID ANDRES CALVACHE DIAZ
JOSE VICENTE MAYAG RODRIGUEZ
VICTOR HUGO ORTEGA MARTINEZ

GUÍA DE SEGURIDAD PARA PREVENIR Y CONTROLAR DELITOS INFORMÁTICOS EN APLICACIONES WEB

Primera Edición, 2011

ISBN:

978-958-8439-19-8

Diseño de Caratula:

I.S. David Calvache
3172498777
david.calvache@hotmail.com

Diagramación e impresión:

TecnoGrafic
Calle 18-Nº 28-28 Ed. INSUCA Primer Piso.
Tel. 7291648

El pensamiento que se expresa en esta obra es
exclusiva responsabilidad
de los autores y no compromete
la ideología de la
Institución Universitaria CESMAG

GUÍA DE SEGURIDAD PARA PREVENIR Y CONTROLAR DELITOS INFORMÁTICOS EN APLICACIONES WEB

Presentación

El objetivo de esta guía es generar procesos tendientes a fortalecer la capacidad de las organizaciones sociales, gubernamentales, comunidad infantil, adolescente, padres de familia y en si la comunidad en general; en temas y aspectos que son relevantes en la seguridad de la información, además de la seguridad de las personas.

Por lo que se presenta esta guía de seguridad que aborda una tendencia temática como lo es la seguridad de la información en las redes de computadores.

A través de esta guía se podrá conocer un enfoque práctico de aplicación básica de seguridad en la búsqueda de prevenir y controlar los delitos informáticos en el procesamiento de la información diariamente utilizada por la comunidad en general.

Contenido.

LISTA DE ANEXOS

GUÍA DE SEGURIDAD PARA PREVENIR Y CONTROLAR DELITOS INFORMÁTICOS EN APLICACIONES WEB

1. PRÓLOGO

Esta guía nació como el resultado de la investigación realizada a la seguridad en las aplicaciones web y el uso cotidiano y frecuente de las mismas.

Este documento pretende aportar información sobre los delitos informáticos más frecuentes y de mayor impacto que se presentan en las aplicaciones web o a través de este medio; además de plasmar conceptos básicos metodologías y medios por los cuales se pueda aumentar el nivel de seguridad de los usuarios al momento de interactuar en internet. Así también dar tratamiento efectivo de todos los aspectos de este creciente problema.

2. OBJETIVOS

Como resultado de una investigación realizada para esta guía se presenta como objetivos los siguientes:

Promover la seguridad en la información para la comunidad en general.

Establecer una cultura de acceso a redes informáticas.

Establecer y promover formas de prevención y control para los delitos informáticos.

3. DELITOS A TRATAR:

De acuerdo al estudio realizado en este proyecto de investigación se estableció dos categorías para la clasificación de los delitos informáticos y se obtuvieron los siguientes resultados:

3.1 DELITOS INFORMÁTICOS POR IMPACTO:

1. GROOOMING
2. PORNOGRAFIA INFANTIL
3. CIBERBULLYING

3.2 DELITOS INFORMÁTICOS POR FRECUENCIA:

4. MALWARE
5. SPYWARE (espionaje)
6. ESTAFA ELECTRONICA (comercio electrónico)

4. DELITO INFORMÁTICO GROOMING

4.1 En qué consiste:

El grooming de niños por Internet, es un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones efectuadas por parte de un adulto en búsqueda a establecer lazos de amistad con un niño o niña a través de internet, con el objetivo de obtener una satisfacción sexual mediante el contenido de imágenes o videos cuyo contenido sea de índole pornográfico del menor o incluso como un delito preparatorio para un posible encuentro sexual, posiblemente por medio de abusos y chantajes.

El perfil psicológico de un abusador sexual o un pedófilo como también es conocido es el siguiente:

Una persona de buena educación además de tener amplios conocimientos informáticos en cuanto a internet, el pedófilo tiene la capacidad para seducir a sus víctimas; se permite aclarar el frecuente uso de las aplicaciones como Messenger o también las redes sociales más comunes como facebook, twitter entre otras, siendo los medios más utilizados por los menores en internet también son los medios más utilizados por este tipo de personas denotando de esta manera que el atacante estudia a su víctima mediante los perfiles que ellos tengan en sus cuentas ya sea en los servicios de mensajería instantánea así como también en las redes sociales.

La realidad virtual no es tan virtual e irreal como se cree, muchas personas tienen la idea de que el mundo virtual o el internet no es tierra de nadie y que nadie está ahí por lo contrario es de establecer que el mundo virtual se asemeja bastante a la realidad; por consiguiente también en ella existen delincuentes victimas y peligros.

Es preciso tener en cuenta la falta de cultura de autoprotección por parte de los niños así como también por parte de los padres ante los peligros que trae el inadecuado uso del internet, al parecer no existen una real conciencia sobre los riesgos a los que se está expuesto en internet.

En inglés, para diferenciarlo del significado original relativo al acicalado de animales se suelen utilizar los términos *child grooming* o *internet grooming.*

4.2 Cómo Sucede:

El grooming es un proceso que puede durar mucho tiempo es cuestión de semanas o incluso de meses, y suele pasar por las siguientes etapas, bajo diversas circunstancias:

1. El adulto procede a elaborar lazos emocionales (de amistad) con el menor, simulando ser otro niño o niña.

2. El adulto va obteniendo datos personales y de contacto del menor.

3. Utilizando tácticas como la seducción, la provocación, el envío de imágenes de contenido pornográfico, consigue finalmente que el menor se desnude o realice actos sexuales frente a la webcam o envíe fotografías de igual tipo.

4. Entonces se inicia el ciber-acoso, chantajeando a la víctima para obtener cada vez más material pornográfico o tener un encuentro físico con el menor para abusar sexualmente de él.

Cabe resaltar en esta parte que este problema o delito informático es una antesala a otro delito informático denominado *PORNOGRAFIA INFANTIL,* el cual se tratara posteriormente.

4.3 Cómo controlar y/o prevenir.

Hay que tener en cuenta varias medias tanto como para padres de familia así como también para los profesores, niños además de los administradores de sitios web o administradores de cibercafés.

Como medida principal para contrarrestar este problema sería que el menor debe dialogar con los padres acerca de las experiencias y vivencias que tiene en Internet. También debe hablar con sus profesores o tutores; el acercamiento con la familia seria el principal método de prevención y control de este delito informático.

Establecer lazos de confianza con el menor de edad tanto para profesores como para los mismos padres.

Como medida de seguridad tecnológica sería establecer horarios de acceso a internet además de lograr evitar al máximo el uso de cámaras web y sobretodo tener el computador o el acceso a internet en un lugar en el que los padres puedan tener control, en cambio de tener el computador en el cuarto del menor de edad.

La restricción de uso de celulares con cámara digital es otra forma de prevención de este delito.

Para las salas de internet o comúnmente llamados cibercafés se debe establecer horarios de atención para menores de edad o también el uso exclusivo de computadores para niños con configuraciones de seguridad en cuanto a Messenger o en las redes sociales

Para mayor información véase Cap. 10.1 *configuración de Messenger* y Cap. 10.7 Seguridad en facebook. Páginas 45 y 94 respectivamente

4.4. Herramientas de control utilizadas.

Existe software de tipo control para evitar el acceso a sitios web y también establecen control en el software que se instale en el computador.

Las medidas de control parental o control paterno es una medida tecnológica más confiable de los últimos tiempos

Para mayor información ver Cap. 10.3 *configuración del control parental.* Página 70.

4.5 Consecuencias.

Prepara el terreno al pedófilo para un posterior abuso sexual del menor.

Daño psicológico en el menor de edad o de la víctima.

Desprestigio y repudio hacia el menor de edad por parte de la sociedad.

5. DELITO INFORMÁTICO PORNOGRAFIA INFANTIL.

5.1 En qué consiste:

Consiste en la representación visual o auditiva de una persona menor de edad para el placer sexual del atacante o también con fines lucrativos tanto para él; así como también para el intermediario; aquí se incluye la producción, distribución, la tenencia y el uso del material pornográfico.

Los impactos de la pornografía en el menor, en cuanto al aspecto social refiere, son bien comprendidos por los abusadores que la usan para preparar al menor.

La pornografía es una herramienta para inducir y socializar a niños y jóvenes para que sus conductas y comportamientos reflejen el contenido de materiales pornográficos.

A veces se considera que la experiencia de un niño o menor de edad de haber sido convertido en objeto de material abusivo es un daño secundario. Este punto de vista se pone de manifiesto cuando junto con la violación se cometen otros delitos contra el menor, tales como prostituirle o traficarle con fines sexuales y lucrativos.

5.2 Cómo sucede:

Son muchos los factores que influyen ante este fenómeno entre ellos se tiene:

La influencia que ejercen los medios de comunicación.

Particularmente esto se ve en la televisión al proyectar la imagen de la mujer como objeto sexual, y relacionarla con la niñez (forma de hablar, vestir, etc.), promoviendo lo atractivo de lo prohibido, en este caso el sexo con niñas y niños.

En Internet se ve demasiado material pornográfico sea en imágenes o videos de explotación de menores de edad. Además cabe denotar el tráfico excesivo y constante de imágenes o videos y la facilidad con que hoy en día se consigue dicho material.

Son muchos los sitios web con contenido pornográfico o que almacenen el mismo material; también se debe denotar la facilidad con que se proliferan los mensajes de correo electrónico con este tipo de contenido o la facilidad de obtener videos o fotografías mediante gestores de descarga o el uso indebido de las tecnologías P2P o de transferencia de archivos directa puesto que a través de ellas no se puede tener control de tráfico siendo también las mismas tecnologías portadoras o transmisoras de Malware o Spyware que posteriormente se hablara.

El mal uso de las cámaras de video, fotográficas o las mismas cámaras web.

Esto permite al pedófilo atacar induciendo al menor al chantaje para así poder tenerlo en sus manos. Con amenazas de publicar esas imágenes.

Falta de confianza con los padres.

La falta de confianza con los padres en temas de internet y de las personas que ahí se conocen, con quien habla el menor, con quien ha tenido contacto físico o que paginas a visitado entre mucho otros factores determinara el avance de este delito.
Al presentarse un distanciamiento del menor con sus padres ya sea por vergüenza o por evitar peleas, malos entendidos o por el mismo chantaje ejercido por el atacante, pueden ser lo más representativo en el momento de ejecutarse este delito.

5.3 Cómo controlar y/o prevenir:

Teniendo en cuenta que el delito informático *grooming* es la antesala al delito informático pornografía infantil, se tomaría las siguientes medidas de prevención y control a saber:

Como medida principal para contrarrestar este problema sería que el menor debe dialogar con los padres acerca de las experiencias y vivencias que tiene en Internet. También debe hablar con sus profesores o tutores; el acercamiento con la familia seria el principal método de prevención y control de este delito informático.

Establecer lazos de confianza con el menor de edad, tanto para profesores como para los mismos padres.

Como medida de seguridad tecnológica sería establecer horarios de acceso a Internet, además de lograr evitar al máximo el uso de cámaras web y, sobretodo, tener el computador o el acceso a internet en un lugar en el que los padres puedan tener control, en cambio de tener el computador en el cuarto del menor.

La restricción de uso de celulares con cámara digital es otra forma de prevención de este delito.

Tener en cuenta que si el menor tiene que ir a lugares públicos para entrar a Internet, se debe escoger un sitio de confianza.

En el caso de las salas de Internet o cibercafés, establecer horarios de atención a menores de edad, además de establecer espacios dentro del mismo recinto en el que el acceso sea por edades; es decir asignar computadores para niños y otros computadores solo para adultos, además tienen que tener instalados software de seguridad que a continuación se hablará.

5.4 Herramientas de control utilizadas:

Existe software de tipo control para evitar el acceso a sitios web con contenido pornográfico, además del acceso a salas de chat y también establecen control en el software que se instale en el computador como Messenger, juegos entre otros.

De la misma manera se sugiere el control parental o control paterno como medida tecnológica más confiable de los últimos tiempos

Para mayor información ver Cap. 10.3 *configuración control parental* Página. 70.

Taller de Caligrafía