DERECHO INFORMÁTICO

Delitos informáticos (PARTE II)

DELITOS INFORMÁTICOS

TIPOS:

- Contra Sistemas: Ransomware, Criptojacking.
- Contra Personas: Grooming, Sextorsión.
- Contra la Economía: Fraude bancario, estafas cripto, phishing.
- Contra la Propiedad Intelectual: Pirateria.

DELITOS INFORMÁTICOS

BIEN JURIDICO PROTEGIDO:

- Delitos contra el honor y la privacidad (acceso, difusión y desviación de comunicaciones electrónicas, acceso y manipulación de datos personales)
- Delitos contra la integridad sexual (pornografía infantil, sexting, grooming, sextorsión)
- Delitos contra la propiedad (defraudación , phishing, sabotaje informático, malware, ransomware)
- Delitos contra la propiedad intelectual (plagio, piratería, creaciones con IA)

DELITOS INFORMÁTICOS

Ley 26.388

Incorporó al Código Penal Argentino diversos delitos informáticos

DELITOS INFORMÁTICOS

ACCESO ILEGITIMO A SISTEMAS INFORMÁTICOS

(*HACKING*)

ART 153 BIS:

"Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros (AGRAVANTE)"

DELITOS INFORMÁTICOS

SABOTAJE INFORMÁTICO

ART 183 1° PÁRRAFO:

"Será reprimido con prisión de 15 días a 1año el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

DAÑO INFORMÁTICO Y DISTRIBUCIÓN DE VIRUS

ART 183 2° PÁRRAFO:

En la misma pena incurrirá el que alterare, destruyere o inutilizare datos,documentos, programas o sistemas informáticos (daño o sabotaje informático) ; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños."

Esta segunda parte corresponde al delito de "virus maker" y pune la conducta de todo aquel que elabora un malware y lo hace circular por cualquier forma (vende, distribuye o introduce).

DELITOS INFORMÁTICOS

GROOMING

DELITOS INFORMÁTICOS

GROOMING

Ley 26.904 incorporó esta figura al Código Penal Argentino en el año 2013

ART 131:

"Será penado con prisión de 6 meses a 4 años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

DELITOS INFORMÁTICOS

CONCEPTO

Acción deliberada que lleva a un adulto a ganarse la confianza de un menor con el propósito de contactarlo, y posteriormente tomar el control emocional de la víctima, rompiendo sus débiles barreras por razones de inmadurez biológica, facilitando su propósito sexual.

La conducta tiene una intención determinada que se divide en etapas que pueden durar semanas o meses.

DELITOS INFORMÁTICOS

"*Grooming*"

Campaña sobre Grooming junto a Movistar

https://youtu.be/LxfcvzgKmUs?si=smMtEMFTgp4qeMtx

DELITOS INFORMÁTICOS

Este delito presenta 3 fases:

- Fase inicial o de "relación": acercarse al menor "suplantando identidad", hablando de gustos, amigos, etc.
- Fase intermedia o de "amistad": ganada la confianza, se va obteniendo datos personales de la víctima, y comienza un intercambio de confidencias y secretos, llegando la primer petición muy sutil con el propósito de obtener imágenes o videos de contenido sexual.
- Fase final o de "actuación": hay una intención sexual, implícita o explícita, que mediante engaño logra concretar una cita real destinada a lograr un fin sexual (una salida tentadora: "te llevo al río a andar en moto de agua").

DELITOS INFORMÁTICOS

DISTRIBUCIÓN Y TENENCIA DE PORNOGRAFÍA INFANTIL

DELITOS INFORMÁTICOS

"Distribución de pornografía infantil" Art. 128 Código Penal

Será reprimido con prisión de 3 a 6 años el que:

produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales; organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Por cualquier medio: comprende la red de Internet y toda aplicación y/o dispositivo móvil o electrónico

Victima: Menor de 18 años.

Lo que se protege es la integridad sexual del menor.

DELITOS INFORMÁTICOS

"Distribución de pornografía infantil" Art. 128 Código Penal

¿Qué se entiende por "pornografía infantil"?

"Toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales".

Esto es:

Un menor adoptando un comportamiento sexualmente explícito.

Una persona que parezca un menor adoptando un comportamiento sexualmente explícito.

Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

Todo ello en: fotos, imágenes, diapositivas o videos.

Lo que se protege es la integridad sexual del menor.

DELITOS INFORMÁTICOS

"Distribución de pornografía infantil" Art. 128 Código Penal

Las representaciones No comprenden:

Caricaturas ni Animaciones.

Representación Auditiva: grabaciones de audio, con voces simuladas o reales, o conversaciones telefónicas, de menores de edad.

Representación Escrita: todo tipo de textos, cuentos, cartas que relaten las experiencias de la vida real del autor, describiendo escenas pornográficas con menores.

DELITOS INFORMÁTICOS

"Tenencia de Pornografía Infantil y Tenencia con Fines de Distribución" Art. 128 Código Penal

Será reprimido con prisión de 4 meses a 1 año el que a sabiendas tuviere en su poder representaciones de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales (Ley 27.436).

"Será reprimido con prisión de 6 meses a 2 años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización"

"Acceso a Espectáculos Pornográficos" Art. 128 Código Penal

Todas las escalas penales previstas en este artículo se elevarán cuando la víctima fuere menor de 13 años.

Será reprimido con prisión de 1 mes a 3 años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de 14 años.

Lo que se protege es la integridad sexual del menor.

DELITOS INFORMÁTICOS

En la actualidad:

Proyecto de ley en cuanto a Ciberdelitos e inteligencia artificial

La creación un capítulo completo de delitos informáticos que incluye la creación de imágenes falsas de contenido sexual mediante IA, el fraude digital y los ciberataques complejos. Se ordena la eliminación inmediata de estas reproducciones. Actualmente, existen algunos delitos informáticos dispersos, pero sin un tratamiento integral ni contemplación específica de la IA.

DELITOS INFORMÁTICOS

MODALIDADES DE FRAUDE INFORMÁTICO

DELITOS INFORMÁTICOS

FRAUDE INFORMÁTICO

(DEFRAUDACIÓN)

ART 173 inc 16

"Será reprimido con prisión de un mes a seis años, el que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Los ataques informáticos suelen basarse en *ingeniería social*: trucos para convencer a las víctimas de la necesidad de abrir un archivo (darle doble clic a un adjunto que es malicioso), instalar un programa en la computadora o una app en el smartphone, clickear el link de un sitio, copiar y pegar un fragmento de código".

DELITOS INFORMÁTICOS

PHISHING

Es una técnica de ingeniería social donde se suplanta la identidad de una persona o entidad y se busca mediante engaños obtener información confidencial o datos financieros.

Es decir, hay un robo de información personal y/o financiera del usuario a través de la falsificación de un ente de confianza (la víctima cree ingresar los datos en un sitio de confianza, que en realidad son enviados directamente al atacante).

Los cibercriminales emplean emails y sitios web muy similares a los de alguna institución financiera o plataforma en línea, para lograr que el usuario ingrese sus credenciales de acceso.

Se valen del miedo para cegar a sus víctimas, enviando un mensaje fraudulento que indica la existencia de algún problema con la cuenta del usuario.

DELITOS INFORMÁTICOS

TIPOS DE PHISHING

DELITOS INFORMÁTICOS

I- SPEAR PHISHING

Es un ataque dirigido a una persona en particular o a una organización. En este caso se investiga la información de la víctima y no son correos masivos. Suelen solicitar información confidencial, enviar archivos adjuntos y enlaces maliciosos.

II- PHISHING POR CLONACIÓN

Este tipo de phishing copia y utiliza correos de empresas o proveedores oficiales para robar información personal de los usuarios. Modifican los correos oficiales con enlaces maliciosos.

III- QR PHISHING

Simula un código QR de una marca o de un negocio y luego de escanearlo redirige a un sitio falso de la empresa víctima para obtener información y robar los datos personales.

IV-ANGLER PHISHING

Este tipo de ataques ocurre en las redes sociales o servicios de mensajería donde los atacantes se hacen pasar por el servicio al cliente de la plataforma y de esta manera robar las credenciales de acceso a las redes o información personal.

DELITOS INFORMÁTICOS

SMISHING

Es un ataque dirigido que puede ser dirigido o enviado de manera masiva a través de mensajes de texto. Pueden enviar enlaces, solicitar información o también interactuar con la víctima.

DELITOS INFORMÁTICOS

WHISHING

Es un ataque similar al de smishing pero donde los mensajes son enviados a servicios de mensajería instantánea como Whatsapp y Telegram entre otros.

DELITOS INFORMÁTICOS

VISHING

Engaño que se realiza vía telefónica, donde el ciberdelincuente llama a la víctima haciéndose pasar por una persona allegada o alguien de la organización para obtener información personal.

DELITOS INFORMÁTICOS

PHARMING

Pharming+Phishing, es un método para redirigir a la víctima a un sitio falso. De esta manera, mediante ataques como DNS Poisoning redirige a la víctima a un sitio potencialmente peligroso.

Es una amenaza más sofisticada. No hay engaño a una persona sino manipulación de un sistema informático de las direcciones DNS (es el sistema de nombres de Internet que traduce nombres de dominio a direcciones IP) que utiliza el usuario.

Llega un email vacío y con solo abrirlo se instala en la computadora un programa que reescribe el archivo “hosts”. Al reescribirse esas direcciones, el usuario entrará a páginas webs falsas sin darse cuenta.

DELITOS INFORMÁTICOS

KEYLOGGER

Es un hardware o software malicioso que registra los tipeos que se realizan en el teclado como objetivo robar toda esa información.

Este tipo de malware puede recopilar información confidencial como contraseñas, datos de tarjetas de crédito y correos electrónicos, lo que pone en riesgo la seguridad del usuario. También puede robar la información a través de capturas de pantalla.

DELITOS INFORMÁTICOS

RANSOMWARE

Es un malware que cifra toda la información de la víctima impidiendo que se pueda acceder a ellos. “Secuestra” los archivos que, para recuperar los mismos se debe pagar un “rescate”. Una vez que se paga, el ciberdelincuente envía el software o un código de desbloqueo que permite volver a acceder a los datos “secuestrados ”.

DELITOS INFORMÁTICOS

SKIMMING

Consiste en sustraer información de las bandas magnéticas de las tarjetas de débito para luego extraer dinero de los cajeros automáticos.

Combina un moderno dispositivo electrónico, con microcámaras de video o *keyloggers* colocados en cajeros automáticos.

Se instala un falso lector en la puerta de una sucursal, que copia los datos de la tarjeta cada vez que alguien pasa la banda magnética por el lector.

Asimismo se instala una microcámara camuflada cuyo lente apunta al teclado, para grabar el momento en que un cliente teclea su clave de seguridad.

Luego se clona la tarjeta y se usan los datos para extraer dinero de los cajeros automáticos