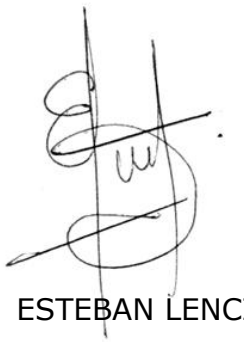
PROYECTO DE COMUNICACIÓN

La Cámara de Diputados de la Provincia de Santa Fe, vería con agrado que el Poder Ejecutivo Provincial, a través del organismo que estime pertinente, realice las gestiones al efecto de establecer con carácter de Fiesta Nacional del Helado Artesanal, la festividad que se celebra en la ciudad de Rosario, durante el mes de noviembre de cada año, incluyéndose la misma en el calendario turístico nacional y lugares de difusión que disponga el Ministerio de Turismo de la Nación.



ESTEBAN LENCI
Diputado Provincial

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

FUNDAMENTOS

Señor presidente:

El desarrollo del helado artesanal en Rosario tomó impulso en gran parte por iniciativa de inmigrantes italianos que arribaron a estas tierras buscando nuevos horizontes tras la Segunda Guerra Mundial.

Heladerías ya desaparecidas como La Turinesa, Polito, La Uruguaya o Piamonte configuraron parte de la historia de mediados del siglo pasado, junto a otras pioneras que hoy continúan una tradición en plena vigencia como Catania (desde 1952), Esther (1957), Bajo Cero (1968), Smart (1972), Río Helados (1972), Yomo (1974) y muchas otras.

Entre las familias italianas que trajeron y difundieron la producción artesanal de helados hubo varias provenientes de Sicilia. No casualmente Don Giuseppe Capitano, fundador de Catania (hoy la heladería más antigua), provenía del pequeño pueblo siciliano de Alessandria Della Rocca).

De Italia era también Don Mario Nicoletti, que dio el nombre de su hija, Esther, a la heladería que inauguró en el garaje de su casa en 1957 (curiosamente 957 es la altura de Ov. Lagos donde hoy funciona la sede principal de esta marca).

En la Rosario del siglo pasado las heladerías se convirtieron en un punto de encuentro habitual para las y los rosarinos. La clientela terminaba siendo parte de la familia.

Recetas exclusivas, tradiciones llenas de historia, sabores que no se consiguen en el resto del país. Desde heladerías históricas con sus sabores

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

tradicionales a las nuevas apuestas gourmets con especialidades que sorprenden. Desde las barriales a las ubicadas en centros comerciales. Hay 190 heladerías de las cuales 150 son artesanales.

Lo que más se pide es el cucurucho tradicional o el recipiente térmico de ¼ kg, pero también hay tradicionales bandejas con topping y, las preferidas de los más chicos, las paletas con sorprendentes formas y sabores.

El gusto preferido siempre es el dulce de leche, pero lo siguen en orden de los más pedidos frutilla a la crema, chocolate, sambayón y gustos exóticos que se ponen de moda cada temporada.

Además, cada vez en más heladerías se encuentran helados veganos, sin contenido lácteo, y para personas celiacas.

El consumo de helado en Rosario duplica al del resto del país.

En el año 1999, el Poder Ejecutivo Nacional dictó el Decreto 86 por el que designa a Rosario como "Capital Nacional del Helado Artesanal".

La importancia de la producción de helados, motivó que desde el año 2012, se celebre en la ciudad de Rosario la fiesta del helado artesanal, impulsado por el Ejecutivo Municipal y el ETUR. La Fiesta del helado artesanal transcurre durante una semana. La Cámara Industrial y Comercial del Helado Artesanal de Rosario conjuntamente con la Municipalidad de Rosario llevan adelante distintas iniciativas y actividades y por ser una fiesta popular, se desarrolla frente al Monumento Nacional a la Bandera, lugar público y emblemático de la ciudad, de acceso libre y gratuito en la que, con el fin de promocionar y difundir la elaboración y consumo del helado artesanal

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

rosarino, se desarrollan exhibiciones y degustaciones de los helados artesanales.

A instancias del entonces Senador Miguel Lifschitz, en el año 2012 esta fiesta se declaró de interés provincial.

A nivel provincial se han celebrado varias ediciones de la Fiesta Provincial del Helado Artesanal. La 5ta. edición tuvo lugar durante la gestión del Gobernador Miguel Lifschitz, que impulsó esta fiesta considerando que representa toda una cadena productiva integrada, desde la calidad de la leche que se produce en los tambos santafesinos hasta la forma de comercialización, con las pequeñas heladerías y los métodos artesanales que cuidan mucho la excelencia de sus productos y del servicio a los clientes.

En lo que a la economía local concierne, sin duda alguna la industria del helado es generadora de empleo y contribuye al crecimiento económico de nuestra Provincia.

Entendemos que la promoción de la Fiesta Nacional del Helado Artesanal de Rosario tendrá por objeto la difusión de la elaboración y consumo del helado artesanal, a nivel local como nacional.

Es por todo lo expuesto que solicito a mis pares la aprobación del presente proyecto.

ESTEBAN LENCI
Diputado Provincial

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

FUNDAMENTOS

Señor presidente:

ESTAFAS VIRTUALES

PISHING

La Ley 25.326 de Protección de los Datos Personales consigna específicamente en el Artículo 9 que “El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado”. Casualmente, **todo lo que el Estado no está haciendo**.

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

Más allá de la naturaleza delictiva de estos hechos y de la propensión de las víctimas a proporcionar información confidencial a través de la manipulación verbal, **existe un componente fundamental en la cadena de seguridad que sigue fallando en su rol de custodia y administración de nuestros datos: el Estado**.

Según la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), las estafas bancarias crecieron un 3000% interanual en el país[1]. Y no debe sorprendernos, es lógica consecuencia de la extrema digitalización a la que nos sometimos desde el inicio de la pandemia y su cuarentena.

De la noche a la mañana, quisimos realizar todas nuestras tareas telemáticamente, pero "salteándonos" la educación, la prevención y el desarrollo de herramientas confiables. Los resultados están a la vista.

Kaspersky, la reconocida empresa de seguridad informática, informó recientemente que -desde 2020- el objetivo preferido de los ciberdelincuentes es la asistencia económica que la mayoría de los gobiernos le entrega a sus ciudadanos para subsanar los daños de la pandemia, y que la modalidad más elegida es el correo electrónico que simula ser de un banco. La compañía detectó, con su sistema "Anti-Phishing", sólo en el primer trimestre de 2021, 79 millones de intentos de visita a páginas fraudulentas (casi el 6% de sus clientes ya se enfrentó a algún ataque de "phishing")[2].

Incluso ESET, también referente en el rubro, destacó que "este año se alcanzó un pico histórico" de sitios de "phishing" detectados en un mismo mes[3], y que el sector más apuntado por los maleantes sigue siendo la industria financiera (24.9%), seguido por las redes sociales (23.6%) y los servicios de correo electrónico (19.6%).

¿Qué es "phishing"?

Al introducir la palabra "phishing", el traductor de Google nos devuelve automáticamente la fórmula "suplantación de identidad", y esto no es correcto. Si bien estamos hablando de dos técnicas de ingeniería social que confluirán en la mayoría de los casos, es importante destacar que no son lo mismo.

Por fonética, es innegable su semejanza con el verbo en inglés "fishing" (que significa pescar), pero el término que nos convoca se escribe con PH en lugar de la F y esto sí tiene que ver con su procedencia. Si bien hay varias teorías al respecto, la más aceptada es que viene de "phreaking", que también se escribe con PH y es la contracción de las palabras "phone" y "freak"[4].

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

Estos “locos por los teléfonos” fueron una especie de tribu urbana -surgida entre los 60 y los 70 en los Estados Unidos- que, como su nombre lo indica, dedicaban su tiempo a la búsqueda de fallas en el circuito telefónico. Entre otras cuestiones, estos grupos de “hackers” (quizá los primeros) lograron engañar a compañías telefónicas para evitar que les cobren las llamadas de larga distancia que realizaban.

En esta lógica, “phishing” no sería más que la explotación de ciertas técnicas de ingeniería social[5]con el objeto de manipular a una persona para que entregue cierta información. Aquí el ciberdelincuente detecta y ataca al eslabón más débil de toda la cadena (normalmente, el usuario final) para luego inducirlo a realizar determinada acción.

Hay un “anzuelo”, que podrá tener forma de aviso urgente, oferta de último minuto o emplazamiento, y una “pesca”, que se perfecciona cuando alguna de las víctimas (genéricas o individualizadas) completa el formulario, realiza la compra, solicita el préstamo, descarga el archivo, entrega el código, etc.

Y debemos destacar que no siempre habrá “suplantación de identidad”. Muchos casos (conocidos popularmente como “spray and pray”) simplemente consisten en cadenas masivas de correo electrónico o mensajes de texto con “felicitaciones” por haber obtenido determinado premio, por ejemplo, y la condición de responder por la misma vía con ciertos datos personales. Es que la sofisticación del ataque dependerá, en primer término, de las capacidades técnicas del atacante y de los objetivos que éste se proponga; ergo, no siempre necesitará de una capa adicional de identidad.

Una cadena por WhatsApp, por tanto, podría consistir en la simple recolección de números telefónicos; una aplicación de filtros fotográficos podría pretender el acopio de rostros; un juego en línea para niños podría tener por objeto la medición de gustos, usos y costumbres. A nuestro criterio, todos ellos son también casos de “phishing”. Criterio que se fortalece a su vez sobre ciertas ocasiones en las cuales la suplantación de identidad será simplemente el medio para la comisión de otros delitos, como el grooming.

El caso típico

Aclarado esto, conviene abocarnos ya al caso típico. Es que, si bien existen ataques dirigidos y personalizados (como el “spear phishing”[6]) y mucho más sofisticados (como el “pharming”[7]), lo cotidiano será la campaña masiva y al voleo que solo respeta algunas consignas básicas (ej. usuarios de tal servicio, clientes de cierto banco o simplemente consumidores interesados en cuestiones estacionales, como el Cyber Monday, el Black Friday, etc.).

Como ya dijimos, el ciberatacante busca engañar a su víctima para que ella misma le entregue sus datos personales, bancarios u otra información confidencial. El “anzuelo” puede ser la caída de un servicio, el bloqueo de una clave, una oferta de último minuto, un premio, e incluso una multa o castigo. Y en la década del 90, el correo electrónico era el canal idóneo para llevar a cabo este tipo de conductas, pero con la proliferación de las redes sociales y los servicios de

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

mensajería instantánea, y la propia creatividad de los criminales, el “phishing” fue tomando infinitas formas.

No dejaron de existir las campañas tradicionales al estilo “Príncipe Nigeriano”[8] o “cuento del tío” (algunas con variantes simples como la herencia vacante, la cuenta bancaria abandonada, el moribundo que quiere compartir su fortuna, etc. y otras con historias más inverosímiles como aquella del astronauta sin nación que se encuentra varado en el espacio y necesita recaudar fondos para volver), pero vemos ya casos “pasivos”, en donde el atacante simplemente crea un usuario en Instagram del “@BancoSaantander” o “@BncoGalicia”, con publicaciones, logos y fotos oficiales, y se sienta a esperar que sus víctimas tengan una necesidad operativa por la cual se contacten con ese supuesto banco.

De hecho, en los últimos meses, observamos que los delincuentes están atentos también a cada nuevo “seguidor” de las cuentas oficiales, con quien -en cuestión de segundos- se ponen en contacto, haciéndose pasar por un empleado de la empresa, para solicitarle el “token”. Con ese código (que se obtiene de un cajero automático), el atacante “blanquea” las claves y se apodera del “homebanking” de la víctima, en donde solicita préstamos y realiza transferencias hasta donde los límites bancarios y la propia víctima le permitan.

Lo cierto es que -como ya dijimos- todos estos ataques tienen en común su objetivo, el eslabón más débil de toda la cadena de seguridad de la información, que no es otro más que el propio ser humano. Apelan al error, a la falta de atención, a la falta de conocimiento e incluso a la avaricia, por lo cual es muy importante conocer los riesgos, las medidas preventivas que podemos tomar y lo que debemos hacer ante un ataque.

¿Qué hacer?

Lo primero que debemos tener en mente es que ninguna empresa puede (ni necesita) requerirnos nuestras credenciales de ingreso. La contraseña, el código de activación, el segundo factor de autenticación, el token, etc. son información que solo nosotros debemos conocer. Son datos de validación, en su mayoría de un solo uso, que hacen a la exclusividad del usuario dentro de un servicio o plataforma digital, por lo cual es importante no compartirlos ni utilizarlos en otros sitios.

Sin perjuicio de ello, es fundamental que una vez detectada cualquier anomalía informemos de inmediato al banco, en este caso, para que éste bloquee preventivamente al usuario de homebanking, las cuentas y las tarjetas, y evite cualquier tipo de operación posterior (una vez recuperadas las claves, se podrán utilizar nuevamente todos los servicios).

Ahora bien, si el atacante llegó a realizar alguna transacción, como solicitar un préstamo o transferir dinero, tendremos que desconocer el movimiento frente al mismo banco para que éste reclame el dinero y lo reintegre a la cuenta o bien cancele la deuda que se haya generado a través del homebanking (hasta que no se resuelva este desconocimiento, el banco no puede cobrar nada; normalmente, en 30 días se obtiene una respuesta).

Lamentablemente, y sin perjuicio de las nuevas exigencias que presentó hace pocos días el Banco Central[9] (y de las recomendaciones que les brindó esta Defensoría), tanto los bancos públicos como los privados están aportando respuestas negativas a estos trámites. Por lo cual, ante el rechazo, la única vía es el reclamo extrajudicial y luego judicial (aquí es dable destacar de todas maneras que existen ya, a lo largo y a lo ancho del país, diversos antecedentes jurisprudenciales que ordenan la restitución del dinero a las víctimas).

___

Recomendaciones mínimas

SIEMPRE…

- Revisá que la cuenta esté verificada (la reconocés por su tilde celeste).
- Confirmá la identidad del que se comunicó con vos por otro medio.

NUNCA…

- Entregues datos personales ni códigos.
- Ingreses datos ni operes en sitios desconocidos.

Si tenés la más mínima duda o sospecha, abandoná de inmediato la comunicación.

___

CHRISTIAN H. MILLER. Abogado (UCA). Especialista en Derecho de la Alta Tecnología (UCA) con formación en Cibercrimen y evidencia digital (UBA) y en Protección de datos personales, privacidad y compliance (UP). Asesor Jurídico en el Centro de Protección de Datos Personales (CPDP) de la Defensoría del Pueblo de la Ciudad.

Ministerio de Seguridad, advierte sobre posibles estafas relacionadas con el censo 2022. En este sentido, el jefe de la sección Cibercrimen de la Agencia de Investigación Criminal (AIC),

Noticia de: El Litoral (www.ellitoral.com) [Link:https://www.ellitoral.com/index.php/id_um/193949-cibercrimen-si-no-hay-denuncia-no-hay-delito-como-actua-la-policia-frente-a-los-casos-de-grooming-y-sextorsion-politica.html]

Convenio sobre Ciberdelincuencia de Budapest. Crédito: Pablo Aguirre

¿Qué dice el Convenio de Budapest?

Consiste en el único acuerdo internacional sobre delitos informáticos **que**, fundamentalmente, hace hincapié en las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red.
¿Cuándo entró en vigor el Convenio de Budapest?

1 de julio de 2004

El **convenio** y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001. El 23 de noviembre de 2001 se abrió a la firma en **Budapest** y **entró en vigor** el 1 de julio de 2004.
¿Qué países están en el Convenio de Budapest?

En junio 2021, 66 Estados ya **forman** Parte del **Convenio** (**países** europeos, Argentina, Australia, Canadá, Cabo Verde, Chile, Colombia, Costa Rica, Estados Unidos de América (EUA), Filipinas, Ghana, Israel, Japón, Mauricio, Marruecos, Panamá, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal y Tonga, otros 2 Page 2 ...4 jun 2021
Que por la Ley N° 27.411, la REPÚBLICA **ARGENTINA** adhirió al **CONVENIO** SOBRE CIBERDELITO del CONSEJO DE EUROPA

General López 3055 – (S3000DCO) – Santa Fe – República Argentina

(ETS N0 185), adoptado en Ciudad de **BUDAPEST**, REPÚBLICA DE HUNGRÍA, el 23 de noviembre de 2001, que contiene CUARENTA Y OCHO (48) artículos.27 nov 2019

¿Qué establece la Estrategia Nacional de Seguridad Cibernética?

Estrategia Nacional de Seguridad Cibernética es la incorporación del ciberespacio en los ámbitos de **seguridad** planteados en el Sistema **Nacional de Seguridad**, de tal manera **que** se generen espacios de articulación estratégicos para formular acciones encaminadas a la protección de los ciudadanos, su patrimonio y sus datos ...

El Convenio de Budapest desde una perspectiva de derechos humanos

El Convenio de Budapest es un instrumento internacional que busca homogeneizar la manera en que los diversos países contratantes abordan y definen la “cibercriminalidad”. Pero, ¿qué pasa cuando son los mismos Estados los responsables de la comisión de este tipo de delitos?

POR: R3D

El Convenio sobre Ciberdelincuencia, mejor conocido como el Convenio de Budapest, es un tratado internacional vinculante en materia penal, que establece herramientas legales para perseguir penalmente aquellos delitos cometidos ya sea en contra de

sistemas o medios informáticos, o mediante el uso de los mismos. El Convenio nació, como señala su preámbulo, en vista de la necesidad prioritaria de aplicar "una política penal común" entre sus miembros, así como de mejorar la cooperación internacional entre ellos con el fin de "proteger a la sociedad frente a la ciberdelincuencia".

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Resolución 1291/2019

RESOL-2019-1291-APN-MJ

Ciudad de Buenos Aires, 25/11/2019

VISTO el Expediente Nº EX-2018-50942023- -APN-DGDYD#MJ, la Ley N° 27.411, y

CONSIDERANDO:

Que con fecha 23 de noviembre de 2001, durante la celebración de la Conferencia

Internacional sobre la Ciberdelincuencia celebrada en la Ciudad de Budapest, Hungría, se abrió a la firma el Convenio sobre Ciberdelito, el cual fue aprobado por el Comité de Ministros del Consejo de Europa en su 109ª reunión el 8 de noviembre de 2001.

Que por la Ley N° 27.411, la REPÚBLICA ARGENTINA adhirió al CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA (ETS N0 185), adoptado en Ciudad de BUDAPEST, REPÚBLICA DE HUNGRÍA, el 23 de noviembre de 2001, que contiene CUARENTA Y OCHO (48) artículos.

Que por la Decisión Administrativa N° 308 del 13 de marzo de 2018 el MINISTERIO DE RELACIONES EXTERIORES Y CULTO ha sido designado como autoridad central de aplicación del Convenio sobre Ciberdelito de Budapest, siendo dicha función desempeñada por la DIRECCIÓN DE ASISTENCIA JURÍDICA INTERNACIONAL de la DIRECCIÓN GENERAL DE CONSEJERÍA LEGAL.

Que la adhesión al Convenio sobre Ciberdelito de Budapest por parte de la REPÚBLICA ARGENTINA constituye un hito fundamental para la mejora del sistema penal, tanto en la persecución de los delitos informáticos como en la investigación de cualquier delito para el que se requiera de obtención de pruebas en formato digital. Asimismo, resulta un avance importante en cooperación internacional en materia penal ya que ubica a la REPÚBLICA ARGENTINA en un sistema de cooperación especializado junto a los países más importantes de nuestro entorno cultural, con los que la REPÚBLICA ARGENTINA tiene tradicionales vínculos de cooperación.

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

Que el artículo 35 del CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA prevé que las Partes designarán un punto de contacto localizable, las VEINTICUATRO (24) horas del día, SIETE (7) días a la semana, denominado Red 24/7, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recolección de pruebas electrónicas de una infracción penal. Esta asistencia, de acuerdo con el Convenio comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas: a. aportación de consejos técnicos; b. conservación de datos según lo dispuesto en los artículos 29 y 30 del Convenio; y, c. recolección de pruebas, aportación de información de carácter jurídico y localización de sospechosos. Ambos aspectos exigen una rápida respuesta para, de esta forma, asegurar la asistencia inmediata en las investigaciones y en la recolección de pruebas electrónicas; máxime si se consideran los efectos transfronterizos de los delitos relacionados con la tecnología y la volatilidad e intangibilidad de la evidencia digital.

Que entre las funciones a desarrollar, la Red 24/7 deberá prestar asesoramiento técnico en las investigaciones penales en las que un Estado Parte del Convenio requiera asistencia, especialmente colaborar en los pedidos de conservación de datos informáticos y facilitar los mecanismos necesarios para la obtención de pruebas informáticas respetando el marco normativo vigente, así como facilitar los mecanismos de comunicación con la autoridad central encargada de la tramitación de solicitudes de cooperación internacional cuando se solicite asesoramiento respecto de cualquier requisito legal necesario para prestar la cooperación, ya sea de manera formal o informal, y asistir en la localización de sospechosos. Asimismo, el punto de contacto deberá asistir a los funcionarios del sistema penal de nuestro país, tanto a nivel federal como provincial, en todo lo atinente a la investigación de delitos

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

informáticos o la obtención de evidencia digital cuando se requiera de cooperación internacional de Estados Partes del Convenio.

Que debido a la volatilidad de los elementos que conforman la evidencia digital, dicha unidad tiene además como función proveer y requerir a las contrapartes extranjeras asistencia internacional idónea durante el proceso de investigación inicial, en donde se busca preservar la evidencia digital relevante, de modo que ésta, se encuentre disponible en un momento posterior de tiempo cuando sea requerida mediante los canales de cooperación internacional vigentes.

Que otro de los propósitos del establecimiento de dicha Red 24/7 es que, además de la intervención de autoridades locales, los delitos relacionados con la tecnología requieren en muchos supuestos asistencia urgente de autoridades extranjeras, para de esta forma agilizar los contactos entre los Estados, ya que muchas veces es importante que los investigadores trabajen a velocidades sin precedentes para preservar los datos electrónicos y localizar a los sospechosos, solicitando incluso a los Proveedores de Servicios de Internet ubicados en diferentes jurisdicciones su colaboración para la preservación de los datos.

Que es de extrema importancia para la eficiencia del sistema penal de nuestro país integrar la Red 24/7 no sólo para la implementación del CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, sino también para lograr la máxima efectividad de las investigaciones penales de todo tipo (mucho más en casos de delincuencia transnacional o compleja) en las que la necesidad de estas novedosas herramientas de cooperación internacional resulta cada vez más evidente. Especialmente en un mundo en el que la ubicación física de la información

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

en formato digital resulta cada vez más transnacional y en muchos casos, incierta.

Que, según el citado Convenio, cada Parte tiene la libertad de determinar la ubicación institucional del punto de contacto de la Red 24/7 conforme a su marco normativo. En este sentido, y a fin de mejorar la eficiencia de la Red e impulsar una mayor utilización de ésta por parte de las autoridades de persecución penal de todo el país, resulta propicio que el punto de contacto de la Red 24/7 funcione en el ámbito de la DIRECCIÓN NACIONAL DE ASUNTOS INTERNACIONALES dependiente de la UNIDAD DE COORDINACIÓN GENERAL de este Ministerio a través de la creación de la UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL, lo que contribuirá a aumentar la eficacia operativa y funcional de la Red, así como a facilitar los mecanismos de comunicación entre la autoridad central encargada de la tramitación de las solicitudes de cooperación internacional, los operadores del sistema penal federal y provinciales y la Red 24/7, así como la cooperación entre la Red 24/7 y los miembros de las redes de otros países. Dichos contactos permanentes son fundamentales para profundizar los efectos beneficiosos para nuestro país de formar parte de la Convención.

Que es indispensable, a los fines de la correcta aplicación del Convenio, y conforme exige el artículo 35 inciso 2.b. de éste, que el punto de contacto de la Red 24/7 funcione coordinadamente con la autoridad central designada por la REPÚBLICA ARGENTINA en el marco del Convenio para la tramitación de solicitudes de asistencia mutua, que es la DIRECCIÓN DE ASISTENCIA JURÍDICA INTERNACIONAL del MINISTERIO DE RELACIONES EXTERIORES Y CULTO.

Que corresponde que, una vez creada, la UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

EVIDENCIA DIGITAL, dicte su reglamento interno de funcionamiento, teniendo en consideración los recursos humanos y materiales actualmente a su disposición, a los efectos de asegurar una respuesta adecuada a los requerimientos que se le formulen.

Que, por último, resulta propicio otorgarle a la UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL que se crea en el presente acto, la facultad de invitar a representantes del MINISTERIO DE SEGURIDAD, por ser dicho Ministerio quien congloba a las Fuerzas de Seguridad de la Nación que han creado unidades especiales sobre la materia y mantiene los vínculos y coordinación con las fuerzas policiales provinciales, así como también a los Ministerios Públicos Fiscales de todo el país para articular el funcionamiento de ésta a nivel nacional, así como derivar con mayor rapidez los casos a cada jurisdicción y atender las necesidades de cooperación que requieran de países extranjeros.

Que ha tomado la intervención de su competencia la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de este Ministerio.

Que la presente medida se dicta en virtud de las facultades conferidas por el artículo 4°, inciso b), apartado 9 de la Ley de Ministerios (T.O.1992) y sus modificaciones.

Por ello,

EL MINISTRO DE JUSTICIA Y DERECHOS HUMANOS

RESUELVE:

ARTÍCULO 1°.- Créase la UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL que asumirá las funciones como punto de contacto de la Red 24/7 previstas en el artículo 35 del CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA.

ARTÍCULO 2°.- La UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL funcionará en la órbita de la DIRECCIÓN NACIONAL DE ASUNTOS INTERNACIONALES dependiente de la UNIDAD DE COORDINACIÓN GENERAL de este Ministerio y actuará en forma coordinada con el MINISTERIO DE RELACIONES EXTERIORES Y CULTO como órgano central de cooperación internacional en materia penal y autoridad central designada en el marco del Convenio para la tramitación de solicitudes de asistencia mutua.

ARTÍCULO 3°.- La UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL estará integrada por los funcionarios y el personal de este Ministerio que oportunamente se asignen.

ARTÍCULO 4°.- La UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL tendrá como funciones asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos y en la recolección de pruebas electrónicas de una infracción penal. Esta asistencia comprende, en la medida permitida por la normativa aplicable, facilitar la aplicación directa de las siguientes medidas: a. aportación de consejos técnicos; b. conservación de datos según lo dispuesto en los artículos 29 y 30 del Convenio de Budapest; y, c. recolección de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

ARTÍCULO 5°.- La UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL podrá convocar a los representantes, del MINISTERIO DE SEGURIDAD y de los Ministerios Públicos Fiscales de todo el país, a los fines de articular el funcionamiento de la Unidad a nivel nacional.

ARTÍCULO 6°.- Facúltase a la DIRECCIÓN NACIONAL DE ASUNTOS INTERNACIONALES dependiente de la UNIDAD DE COORDINACIÓN de este Ministerio, para cursar las invitaciones al MINISTERIO DE SEGURIDAD DE LA NACIÓN y a los Ministerios Públicos Fiscales de todo el país para que designen los puntos de contacto necesarios para lograr el funcionamiento adecuado de la UNIDAD 24/7 DE DELITOS INFORMÁTICOS Y EVIDENCIA DIGITAL, así como otras comunicaciones que sean necesarias y emitir los actos de implementación que resulten necesarios para el cumplimiento de la presente Resolución.

ARTÍCULO 7°.- Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. Germán Carlos Garavano

Noticia de: El Litoral (www.ellitoral.com) [Link:https://www.ellitoral.com/index.php/id_um/193949-cibercrimen-si-no-hay-denuncia-no-hay-delito-como-actua-la-policia-frente-a-los-casos-de-grooming-y-sextorsion-politica.html]

Noticia de: El Litoral (www.ellitoral.com) [Link:https://www.ellitoral.com/index.php/id_um/193949-cibercrimen-si-no-hay-denuncia-no-hay-delito-como-actua-la-policia-frente-a-los-casos-de-grooming-y-sextorsion-politica.html]

>“Necesitamos que toda la comunidad se involucre un poco más y demande mayor capacitación”, manifestó la suboficial.Foto: Pablo Aguirre

—¿Qué indica la Ley?

—Frente al sexting, el Código Penal establece prisión de cinco a diez años a quien obligue a otra persona o a un tercero a entregar, enviar, depositar o poner a su disposición cosas, dinero o documentos que produzcan efectos jurídicos.

Con respecto al grooming, la legislación argentina incorporó con la ley 26.904 el artículo 131 al Código Penal. Allí se indica que las penas en prisión van de 6 meses a 4 años.

La ley de Grooming castiga a quien, por medio de comunicaciones que se establezca en tecnología de transmisión de datos, contacte a un menor con el objetivo de cometer un delito contra su integridad sexual.

La sanción de la norma data de 2013, pero la primer condena por este delito sucedió en 2017 con el caso de Micaela Ortega; una niña de doce años que fue encontrada muerta en un descampado, tras ser citada por Facebook por su asesino, Jonathan Luna, que fue condenado a prisión perpetua.

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

A esto hay que agregar que, desde marzo del año pasado, hubo un cambio respecto de la pornografía infantil que configura que la sola tenencia ya es delito, en vez de su divulgación como se establecía previamente.

Desempeño

—¿Cuáles son los pasos que se deben seguir si hay sospechas de un caso de este estilo?

—Primero es necesario decir que existen muchísimos más casos de los que se denuncian. Por este motivo instamos a que se produzcan las denuncias. Sin formalizar la denuncia, no se puede comprobar que haya delito. Para la elaboración de políticas públicas que protejan a la ciudadanía, necesitamos las estadísticas que nacen de los casos probados.

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

Dicho esto, el segundo paso es no borrar nada. Muchas veces, por miedo o vergüenza, los implicados -chicos y grandes- suelen eliminar las conversaciones o las cuentas. Esto es un error porque se elimina el material con el que luego se realiza el proceso de investigación.

Otro error común es intervenir en los chats para tener algún tipo de respuesta o producir un encuentro con la persona que está del otro lado del perfil. Esta situación suele derivar en que el delincuente se asuste y abandone el vínculo. Lo recomendable es mantener una comunicación dentro de los mismos términos y radicar la denuncia correspondiente.

—¿Con qué herramientas cuentan para realizar su trabajo?

—En el caso de la PDI, así como otros organismos certificados, podemos solicitar que los perfiles en las redes sean preservados para hacer un seguimiento del ID del perfil, una identificación electrónica que funciona como el DNI. De esta manera, nos aseguramos de tener un respaldo de cada uno de los movimientos.

Luego, por medio de oficios judiciales se puede solicitar información como el IP del dispositivo, para descifrar su dirección física.

Para poder actuar en estos casos, se vuelve importante el ingreso de Argentina al Convenio sobre Ciberdelincuencia de Budapest. Este acuerdo facilita los pasos legales de seguimiento de las IP, ya que los cibercriminales cambian el país de registro cada cierto período de tiempo para no ser rastreados con facilidad.

—¿Es posible detectar las cuentas falsas?

—En general, es notorio cuando los perfiles son falsos por ciertas incoherencias en las publicaciones y las fotos.

En casos como el de grooming, la situación es un poco más compleja. Allí, los victimarios suelen establecer un vínculo empático con los chicos. Por ejemplo, si un niño comenta que se peleó con su mamá, la respuesta será consintiendo ese comentario para generar ese sentimiento de confianza. Así, los intereses y los contactos de esos perfiles suelen estar en sintonía con los de los jóvenes.

Esto se ve agravado por la enorme cantidad de aplicaciones para tablet o celulares que existen y que están pensadas para los más chicos. La mayoría de ellas trae incorporado un chat donde se abre una posibilidad de que sean manipulados. Lo mismo pasa con los adolescentes por medio de los juegos en línea.

Prevención

—¿Qué actitud hay que tomar frente a estos casos?

—Los delitos no son una novedad, siempre existieron. La tecnología permite potenciarlo, lo hace masivo, anónimo e inmediato. Por eso, tenemos que priorizar la educación tecnológica y el uso responsable de internet.

Se trata de un cambio de paradigma respecto del cuidado de la niñez. Los adultos deben comenzar a investigar cuáles son las redes y aplicaciones más usadas por sus hijos. En cambio, en los niños, como son nativos digitales, es necesario hacer hincapié en la formación de criterios.

Existen muchas aplicaciones de mediación parental que sirven para administrar los dispositivos y que son muy buenas. De todas maneras, antes que el control, es fundamental poder hablar de estos temas tanto con los padres como en las escuelas.

Con respecto al rol docente es muy importante que, en la medida de lo posible, eviten los contactos por redes sociales con sus alumnos. Si bien es bastante común crear grupos de Facebook o Whatsapp educativos, no es recomendable este tipo de interacción porque vuelve muy delgada la línea que divide entre una relación académica y una personal.

—¿Cuál es el estado actual de capacitación en cibercrimen?

—En el último año, junto a la Defensoría del Pueblo, brindamos charlas y cursos en torno a protección de datos personales en distintas instituciones: escolares, judiciales, clubes de fútbol.

También existen organizaciones que trabajan mucho sobre estos temas y capacitan permanentemente. Algunas de ellas son Argentina Cibersegura y Grooming Argentina .

De todas maneras, sería importante que toda la comunidad se involucre un poco más y demande mayor capacitación para todos: alumnos, padres, docentes y directivos.

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

España es un caso modelo en este sentido. Cuentan con una gran cantidad de recursos para que la sociedad se pueda informar y, a la vez, materiales para abordar estas temáticas en clases.

Dónde denunciar

En Santa Fe, las denuncias se pueden realizar en los Centros Territoriales de Denuncia, en la Policía de Investigaciones, en el Ministerio Público de la Acusación o en cualquier comisaría.

Para aportar una solución, Grooming Argentina (http://groomingargentina.org/) creó una aplicación que puede ser descargada desde cualquier celular. También se pueden contactar mediante correo electrónico a: contacto@groomingargentina.org.

General López 3055 – (S3000DCO) – Santa Fe – República

Argentina

Cuidar nuestra información

Al día de hoy, es muy común que busquemos wifi en lugares públicos y que nos conectemos a cualquier red abierta que encontremos. Esa simple acción puede derivar en que el teléfono sea interceptado y toda la información que cargamos con nosotros (contraseñas, números de cuentas, fotos) sean secuestradas.

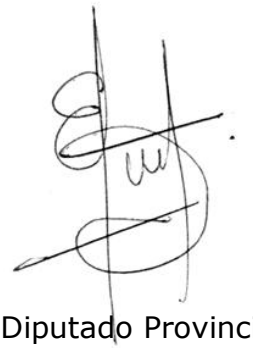
Como método de control sobre posibles estafas y extorsiones, Facebook habilitó una opción que permite descargar el registro completo de actividad en esa plataforma.

Este registro está compuesto por una lista que incluye todas las publicaciones, como las historias y fotos etiquetadas, así como las conexiones establecidas, por ejemplo, al indicar “me gusta” una página o al agregar a alguien como amigo.

Para conseguir la lista solo es necesario ingresar en el menú de perfil personal de Facebook, luego buscar “configuración y privacidad”, ingresar en “tu información en Facebook” y ahí se encuentra la opción “Registro de actividad”.

Noticia de: El Litoral (www.ellitoral.com) [Link:https://www.ellitoral.com/index.php/id_um/193949-cibercrimen-si-no-hay-denuncia-no-hay-delito-como-actua-la-policia-frente-a-los-casos-de-grooming-y-sextorsion-politica.html]

Es por todo lo expuesto, que solicito a mis pares la aprobación del presente proyecto.



Diputado Provincial
ESTEBAN LENCI

General López 3055 – (S3000DCO) – Santa Fe – República
Argentina

El jefe de la Sección Cibercrimen de la AIC explicó cómo protegernos de las ciberestafas. Aseguró además que el 90% de ellas se realizan desde la cárcel