MARCELO ROMERO - DIEGO MIGLIORISI

PATITO AZUL

HISTORIA DEL FRAUDE INFORMATICO

1770 Argentina | DFM 2022

Romero Marcelo / Diego Migliorisi

Patito azul: historia del fraude informático / Diego Migliorisi; Marcelo Romero. - 1a edición especial - Ciudad Autónoma de Buenos Aires: Diego Fernando Migliorisi, 2022.

Libro digital, PDF
Archivo Digital: descarga ISBN 978-987-88-3159-6

1. Derecho Penal. 2. Nuevas Tecnologías. I. Romero, Marcelo. II. Título.
CDD 345.009

Migliorisi, Diego
Patito azul: historia del fraude informático / Diego Migliorisi; Marcelo Romero. - 1a edición especial - Ciudad Autónoma de Buenos Aires: Diego Fernando Migliorisi, 2022.
Libro digital, PDF

Archivo Digital: descarga ISBN 978-987-88-3159-6

1. Derecho Penal. 2. Nuevas Tecnologías. I. Romero, Marcelo. II. Título.
CDD 345.009

Edición: Diego F Migliorisi
Diseño de tapa: Gustavo Nanno // Marcelo Romero
Edición: Juan Ignacio Fernández Mugica

Reservados todos los derechos. Hecho el depósito que marca la ley 11.723 Publicación electrónica hecha en la Argentina. Se autoriza a republicar en forma total o parcial esta obra siempre que se mencione la fuente y el link oficial.

Prólogo

Nos sumergimos en un mundo cuasi digital, donde esto cambiará para siempre la forma de entablar relaciones, o comunicarnos, traerá la cuarta revolución, o simplemente ya está, pero no la aceptamos.

La tecnología nos entretiene, nos permite automatizar datos, acortar las fronteras o hacerlas desaparecer. Transformó el mercado tal cual lo conocemos, desafiando las leyes y la manera de ver el mundo, esto nos lleva a volver a empezar a entender cómo funcionan las cosas.

La tecnología es hermosa, pero suele quedar en un lugar de arma de doble filo, donde la falta de un faro, o moral terminan jugando una mala pasada a las personas, perdiendo el acto de las relaciones sociales; el contacto que nos hizo evolucionar hace millones de años, aunque parezca irónico, la tecnología, se muestra como un puente entre las personas, termina siendo usada para atacar a las mismas, y despojarlas de toda humanidad, y sus bienes.

En la pandemia que vivió el mundo, la tecnología fue clave para seguir avanzando ante el parate mundial, pero esto también fue aprovechado por los delincuentes, que siguen migrando a nuevos mundos digitales para hacerse con los activos de las personas. Este trabajo pretende dar un pantallazo a todas las personas interesadas en analizar estas estafas realizadas en el mundo virtual.

Así como un docente hoy le empieza a dar valor a una pizarra blanca virtual para enseñar, el delincuente le empieza a dar valor a los NFT token no fungible, como activo de valor que puede ser despojado de su dueño, al

igual que una cuenta de cualquier plataforma de comunicación, que representa al usuario en el mundo vertiginoso de internet. Comúnmente conocido como su AVATAR.

Hace poco, tuve la posibilidad de crear un simulador de tiro virtual, el cual sumerge al tirador en un mundo virtual, llevando a este a sucesos controlados para evaluar su destreza en un mundo manejado digitalmente, esto fue puesto en marcha en la sede UAE (Unidad Académica extracurricular) Moreno. Claramente utilizando la tecnología para fines profesionales y éticos no tiene límite, pero si la misma es factible de usarse para dañar a personas, estaremos ante una nueva rama de lo ético y no ético en cuanto al avance de la tecnología y la inteligencia artificial.

Sobre **Marcelo Romero**

Técnico superior en Seguridad Publica, especialista en Informática Forense, Investigador Digital, especializado en escena del hecho digital. Instructor de Informática Forense. Funcionario en el Ministerio Público De la Ciudad de Buenos Aires. Co Autor de dos libros sobre Grooming (El abuso silencioso) y Ciberbullying (La sociedad acosada) y Libertad de expresión en internet. Director Nacional de capacitación de la ONG Asociación Argentina de Lucha Contra el Cibercrimen. Expositor en gran cantidad de eventos, charlas, mesas redondas, Jornadas y Congresos. Miembro de la subcomisión de informática forense de IRAM. Investigador en el proyecto de desarrollo tecnológico social "Desarrollo de una Suite de Análisis y Visualización de la información extraída de dispositivos

móviles" de la UFASTA. Docente universitario en la Diplomatura de Cibercrimen y evidencia digital de la UAI, Docente universitario de la Diplomatura en Cibercrimen de la UNAM México, y Profesor en la escuela de policía Juan Vucetich sede Moreno.

Sobre Diego Migliorisi

Belgraniano. Abogado de la Universidad católica de salta, Master en gestión de la comunicación política y electoral de la Universidad autónoma de Barcelona, corredor inmobiliario, fundador de la ONG Asociación Argentina de Lucha Contra el Cibercrimen, Escritor, especialista en Seguridad Pública, vivienda y altas tecnologías. Fundador de 1770Argentina.org Manuel Belgrano. Representante de AALCC en la en la sección de sociedades civiles de la organización de Estados Americanos. Coordinador del sitio www.libertadeninternet.com, Vicepresidente del comité de tecnología y comunicaciones de la Federación Interamericana de Abogados. Participo en la International Law Association (Itechlaw) y en la American Society of Comparative Law . autor y coautor de más de obras y artículos de opinión sobre diferentes temáticas

“Sin educación No hay adelantamiento “

“Un pueblo culto jamás podrá ser esclavizado”

Manuel Belgrano

Índice:

CAPITULO I

¿Qué es el fraude informático?

Para hablar de esto nos basaremos en la ley 26.388 Ley Nacional de Delitos Informáticos sancionada en el 2008 en Argentina.

El Código Penal sanciona la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.[1]

Pero como siempre, esa definición no me alcanza para comprender a fondo este mundo, así que manos a la obra y empezaremos a ir de a poco, para interpretar la letra chica.

Definiremos primeramente la palabra **Fraude** según la RAE (Real Academia Española) "Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete" que, sin dudas, dependiendo de quién lo escuche, es sinónimo a mentir. Ahora si tomamos una definición popular que dice "Engaño económico con la intención de conseguir un beneficio, y con el cual alguien queda perjudicado." Nos damos cuenta de que hay diferencias sustanciales, ya que esta última incorpora la palabra económico dentro de su definición. Por cuestiones de prácticas esta última es la más utilizada entre las personas.

[1] https://www.argentina.gob.ar/justicia/derechofacil/leysimple/delitos-informaticos#titulo-7

La siguiente pregunta, que debemos respondernos es cuantos tipos de fraudes existen:

1. El fraude **cometido por funcionario público**
2. **Laboral o empresarial**
3. **Electoral**
4. **Fiscal o tributario**
5. **Bancario**
6. **Informático o virtual**

Se nombraron algunos para usarlos de referencia, pero observamos que en último lugar se encuentra el Fraude Informático o Fraude Virtual, este último es el que analizaremos a fondo.

Si observamos un poco la historia veremos que el Cibercrimen como tal, toma relevancia nacional cuando los delincuentes informáticos comienzan a meterse en el patrimonio de las personas, o más conocido como estafas informáticas. Es ahí cuando toma una connotación nacional, estos robos asociados a las transferencias electrónicas bancarias, tomando esta metodología el primer lugar por el impacto que causa en las víctimas y la sociedad en sí. Lejos estamos viendo la primera definición de FRAUDE INFORMATICO donde hacía referencia a una acción contraria a la verdad, para tomar una definición popular; Como la acción por internet que intenta realizar un perjuicio patrimonial.

En los últimos años el incremento de las personas que se conectan al ciberespacio hace que el delincuente vea con otros ojos este espacio virtual, donde su atención es captada por la cantidad de personas, futuras víctimas, que

se agolpan en ese espacio no tangible. Por tal motivo este oscuro personaje, comienza el entrenamiento.

Tipos de fraudes

Podríamos estar todo el día nombrando diferentes tipos de fraudes que aparecieron, sobre todo estos dos últimos años, pero nos centraremos en dos tipos que son los más comunes, el phishing y el ransomware.

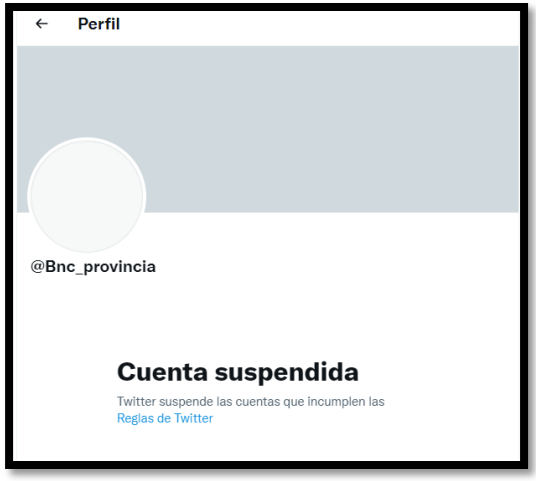
Phishing: es un delito informático **que** tiene como objetivo robar información confidencial. Los estafadores se hacen pasar por grandes empresas u otras entidades de confianza para **que** les facilite voluntariamente sus datos de acceso a un sitio web o incluso el número de su tarjeta de crédito, pero en estos últimos tiempos se vio un incremento del uso del Phishing para robar las credenciales de whatsapp y utilizar esta última como herramienta de estafa. Generalmente estos se lanzaban por correos electrónicos, pero un aumento del uso de las plataformas de mensajerías como whatsapp y telegram, hicieron que el delincuente, mutara y busque herramientas nuevas. Esto llevo a que utilicen cuentas de whatsapp suplantando a empresas, y poder robar datos que luego le sirvan de intercambio.

Como el viejo arte de la pesca, un pescador analiza la carnada que utilizará dependiendo de qué tipo de pez quiere pescar, un delincuente viendo que todo el mundo empezó a operar sus cuentas bancarias, y cambio monetario por internet, vio la oportunidad de poder utilizar las identidades de empresas, casas de cambios y hasta

incluso identidades digitales de personas ofreciendo tentadores negocios en línea.

Preparando el cebo, dependiendo que tipo de víctima se busque, el Phishing está destinado al robo de datos, independientemente de para qué se utilice luego. Por ese motivo, y netamente educativo, analizaremos un Phishing bancario. Para esto el delincuente, sabiendo que el banco con la pandemia, dejó de atender al público en sus oficinas y necesitaban sacar turno vía web, el cebo perfecto fue suplantar la identidad de estas entidades en las famosas redes sociales.

Uno de los últimos casos que viene a mi cabeza es la cuenta en la red social de twitter del Banco Provincia https://twitter.com/Bnc_provincia donde utilizaron los delincuentes el nombre Bnc_provincia para impersonar al banco y como una araña estar en la red social monitorizando los reclamos de los usuarios, y poder responder las preguntas que tenían sus estos, y así llevarlos a una conversación privada, y lograr pedirles las credenciales sin que se enteren, prometiendo mejoras u respuestas a sus problemas.



Cuenta suspendida, que crearon los delincuentes, para interactuar con los usuarios.

Unos de los usuarios, exponiendo y arrobando al Banco Provincia, sabiendo que, al realizar un reclamo público, alguno de los delincuentes levantará ese reclamo y lo contactará, para intentar estafarlo. El usuario expone que esta cuenta llevaba 7 horas realizando este tipo de maniobras.

Luego de varias horas de actividad, la entidad bancaria, y pasados muchos reclamos, se contacta con el creador del contenido y solicita que REPORTEN a la cuenta fraudulenta. A esta altura quisiera realizar un comentario adicional, ya que no habla la entidad bancaria de una tentativa de delito, una denuncia, ni nada parecido. A qué se refiere la entidad bancaria al hablar de REPORTAR?.

Las redes sociales son empresas privadas, y si bien hablaremos de Twitter, esto lo hacemos extensivo al resto, al encontrarse fuera de nuestro país, lo correcto es hablar de un reporte y no una denuncia, pero por la traducción al español cuando Twitter habla de Report, en nuestro país, es traducido como denuncia y no reporte.

Según el portal de Twitter, Cualquiera puede denunciar comportamientos abusivos directamente desde un Tweet, perfil o Mensaje Directo.

Para denunciar un Tweet:

Dirígete al Tweet que deseas denunciar en twitter.com o en la aplicación de Twitter para iOS o Android.

Pulsa o haz clic en el ícono.

Selecciona Denunciar.

Selecciona Es abusivo o perjudicial.

“A continuación, te pediremos que nos proporciones más información sobre el asunto que quieres denunciar. Además, tal vez te pidamos que selecciones otros Tweets de la misma cuenta a fin de que podamos disponer de más contexto para evaluar tu denuncia”.

Incluiremos el texto de los Tweets que denunciaste en los correos electrónicos y las notificaciones de seguimiento que te enviamos. Si quieres dejar de recibir esta información, quita la marca de la casilla junto a la opción “Las actualizaciones acerca de esta denuncia pueden mostrar estos Tweets”.

“Una vez que envíes la denuncia, te recomendaremos otras medidas que puedes tomar para mejorar tu experiencia en Twitter”.

Para denunciar una cuenta:

Ve al perfil de la cuenta y pulsa o haz clic en el ícono de contenido adicional

Selecciona Denunciar.

Selecciona Es abusivo o perjudicial.

“A continuación, te pediremos que nos proporciones información adicional acerca del asunto que quieres denunciar. Además, tal vez te pidamos que selecciones otros Tweets de la misma cuenta a fin de que podamos disponer de más contexto para evaluar tu denuncia”.

Incluiremos el texto de los Tweets que denunciaste en los correos electrónicos y las notificaciones de seguimiento que te enviamos. Si quieres dejar de recibir esta información, quita la marca de la casilla junto a la opción “Las actualizaciones acerca de esta denuncia pueden mostrar estos Tweets”.

Una vez que envíes la denuncia, te recomendaremos otras medidas que puedes tomar para mejorar tu experiencia en Twitter.

Nota: Puedes denunciar una cuenta que bloqueaste o que te ha bloqueado. Ve al perfil de la cuenta, pulsa o haz clic en el ícono de contenido adicional y selecciona Denunciar.[2]

Al no darse a conocer esta práctica por parte de los delincuentes a la justicia argentina, no son investigados, y esto es aprovechado por parte de estos, para lograr realizar ciento o miles de intentos de estafas y salirse con la suya. Por este motivo, es rentable el método de Phishing, ya que un delincuente puede intentar tantas veces como necesite hasta que caiga la primera víctima y recién ahí se informaría a la justicia la concreción de la estafa. Claramente ahora podemos observar que hubo muchos intentos anteriormente. A esto le debemos sumar,

[2] https://help.twitter.com/es/safety-and-security/report-abusive-behavior

que los pedidos de información a las empresas en el extranjero, suelen ser tardíos, como así también desconocido por muchos de los operadores de la justicia, esto da el combo perfecto para que la estafa llegue a las últimas instancias buscadas.

Haciendo un poco de futurología, como diría un viejo profesor mío, intentaremos ver qué hubiera pasado si los delincuentes en este caso expuesto hubieran logrado tener éxito en la concreción de la maniobra delictiva.

Como primera medida, le hubieran pedido al usuario, el usuario y contraseña de su Home Banking, esto para poder identificarlo, siendo esto sus credenciales de identificación ante la entidad. Lo segundo es nombre completo y D.N.I. datos que tradicionalmente las entidades nos solicitan para poder identificarnos. Al entregar estos datos, les estamos dando acceso total a nuestra plataforma digital del banco en el cual estamos operando, para completar la maniobra, el delincuente con total habilidad nos expondrá que debe reiniciar todo para no tener ningún problema más y que en 20 minutos podemos volver a operar digitalmente en nuestra banca. Esto dará el tiempo necesario al delincuente para poder entrar a la plataforma y vaciar las cuentas, y una de las maniobras que estuvieron en auge este último tiempo, es solicitar en nuestro nombre, un crédito preaprobado o adelanto de sueldo. Con la finalidad de poder hacerse con más dinero, esto será trasladado a otra cuenta digital, sea de cualquier plataforma o banco que previamente se encuentra en manos del delincuente.

Una vez que el usuario se da cuenta que fue víctima de una estafa, realizará la denuncia, ante la justicia, y una denuncia y desconocimiento ante la entidad bancaria. Esto hará que empiece nuestra victima una procesión de pasos para lograr que el banco revierta esta estafa y nos devuelva el dinero, y cancele el crédito que fue otorgado en nombre de la víctima, pero al cual nunca tuvo acceso.

Hay dando vueltas en lugares destinados a jurisprudencia sobre estos temas, algunos que llamaron la atención, y quisiera compartir, con ustedes.

La Plata, 29 de Julio de 2020.

AUTOS Y VISTOS:

Proveyendo a la presentación electrónica de fs. 4:

Por devueltos de la Sra. Agente Fiscal, tiénese a la misma por presentada en el carácter invocado de conformidad con lo establecido por los arts. 52 de la ley 24.240, 27 de la ley 13.133 y 29 inc. 4° de la ley 14.442.

Tiénese presente lo dictaminado en el escrito en vista y háceselo saber a sus efectos. Consecuentemente, señálase que estas actuaciones que se encuentran en estado de resolver y de las que;

***RESULTA**:*

Que a fs. 1 se presenta el actor H. G. M. con el patrocinio letrado del Dr. M. D. F. e interpone demanda de medida cautelar de no innovar, contra el B. P. de B. A. (sucursal …), requiriendo en el punto I OBJETO, que se ordene la inmediata suspensión en la afectación de su cuenta

sueldo de cuotas correspondientes a "Préstamo Personal", ello hasta el resultado de la acción penal que se encuentra tramitando en sede penal en IPP. . . que tramita ante la UFI N° 9, Juzgado de Garantías N° 1, caratulada "ESTAFA - Art.172 C.P-. Ello así, toda vez que manifiesta haber sido estafado a través de una secuencia o acción llevada a cabo vía telefónica por autor que a la fecha se desconoce su paradero, pero que conforme la investigación en curso podría identificarse. Relata asimismo que, habiendo obtenido los datos necesarios, se ha solicitado con ellos un préstamo bancario mediante la modalidad "Home Banking" y no ha sido con el consentimiento del titular de la cuenta aquí actor, para luego esos mismos fondos ser transferidos a cuentas particulares, conforme datos y hechos detallados y surgente de la documental adjunta en PDF. Que por fs. 2 se da intervención al Ministerio Público Fiscal por los fundamentos allí brindados, quién asume por fs. 4 dictaminando en sentido favorable en relación a la medida cautelar requerida y;

***CONSIDERANDO**:*

PRIMERO) Que en los procesos cautelares, como el que anida en la pretensión descripta en las Resultas, es factible solicitar el anticipo jurisdiccional de no innovar cuando medien o se encuentren acreditados -prima facie- los presupuestos de procedencia de la misma, sin que ello implique emitir opinión sobre el fondo de la cuestión, ello en razón que el juicio de verosimilitud debe carecer de repercusión en lo que hace a la sentencia final, la que se dictará una vez investigado el fondo y previo ejercicio del

debido derecho de defensa en juicio (arts. 16, 18 y concs. de la Const. Nac.), aditándose que estas requieren como presupuesto a) la existencia de un derecho que debe ser acreditado prima facie, b) un interés jurídico que justifique el anticipo de la garantía jurisdiccional, o sea, peligro en la demora, y c) el otorgamiento de una contracautela que asegure a la contraparte el resarcimiento que pudiere ocasionar la medida para el supuesto que se hubiere pedido sin derecho (Podetti, " Tratado de las Medidas Cautelares", p. 51, Morello-Sosa-Berizonce, "Códigos..."), al respecto y teniendo presente la lamentable situación en la que nos encontramos inmersos como sociedad en virtud de la pandemia declarada por la O.M.S., que conllevó el ASPO - aislamiento social preventivo y obligatorio- decretado por el P.E.N. por Dec. 297/2020 prorrogado hasta el 02 de agosto de 2020 inclusive por el Poder Ejecutivo Nacional mediante Decs. 325/2020, 355/2020, 408/2020, 459/2020, 493/2020, 520/2020, 576/2020 y 605/2020; la realidad económica agravada, por la situación descripta en el escrito introductorio de litis y que el peticionante de la cautelar recibe un ATP, (PDF relativa a los extractos de la cuenta bancaria) el que se otorga teniendo en cuenta el diferente grado de vulnerabilidad de los trabajadores formales cubriendo el 100% a quienes ganan menos de un salario minino vital y móvil, en los términos del Decreto 332/2020, dictado en uso de las atribuciones conferidas por los artículos 1°, 2° y 58 de la Ley N° 27.541 y el artículo 99 incisos 1, 2 y 3 de la Constitución Nacional (https://www.argentina.gob.ar/atp/empresas/en-que-consiste-el-beneficio#) y los múltiples informes de

entidades oficiales, locales e internacionales, que dan cuenta de ello.

Sólo a modo de referencia puede citarse el muy completo análisis que las Naciones Unidas (ONU) elaboró para nuestro país, donde básicamente dice que "...La epidemia causada por el virus COVID-19 tendrá en la Argentina un impacto multidimensional. Afectará al total de la ciudadanía, a los distintos sectores de la economía y actores de la vida del país, al ambiente y los recursos naturales...".

La crisis de COVID-19 ha exacerbado la vulnerabilidad y la discriminación hacia los y las menos protegidos/as de la sociedad, destacando profundas desigualdades económicas y sociales que requieren atención urgente...".

En especial los consumidores o usuarios, los que resultan ser sujetos pasibles de aprovechamientos y/o estafas como la denunciada en autos, situación ésta que resulta de público y notorio en la realidad diaria y cotidiana, con dicho piso en el estrecho marco cautelar en despacho y con criterio de buena fe es posible adoptar coherente y razonablemente (arts. 1, 2, 3 Código Civil y Comercial) la medida cautelar, ya que es preferible el exceso en acordarlas que la parquedad en desestimarlas, pues con ello se satisface el ideal de brindar seguridades para la hipótesis de triunfo, claro que ello con un límite temporal en el que se analizara su prorroga de conformidad al grado de avance de los autos que tramitan ante el fuero penal descripto en las Resultas y/o la acción civil que promueva y su carácter provisorio (art. 202 CPCC), ello se motiva en que la vigencia de la medida cautelar no puede

quedar librada al hiato temporal del proceso cognitivo, cuya excesiva prolongación puede convertirla en los hechos en definitiva. Es en este campo, precisamente, donde las medidas cautelares deberían ser cuidadosamente limitadas en el tiempo, mediante plazos razonables, adecuados a las características particulares de cada supuesto, atendiendo en especial al gravamen que la medida pueda causar a su sujeto pasivo, a la naturaleza del proceso o acción en que se la impetra, al alcance de la prolongación excesiva del proceso en comparación con la pretensión de fondo (CSJN Fallos 327:2490, 330:4076).

Que la documental adjunta en PDF relativa a los extractos de la cuenta bancaria del peticionante, denuncia penal efectuada, permiten tener por acreditados -prima facie- y conforme los postulados citados precedentemente y lo que infra se dispone, la verosimilitud del derecho invocado.

SEGUNDO) La pretensión cautelar, la ubicaríamos en un supuesto de phishing, aunque no refiere a ello el escrito de fs. 1, el que constituye un término informático que denomina a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

Para realizar el engaño, habitualmente hacen uso de la ingeniería social explotando los instintos sociales de la gente, como es de ayudar o ser eficiente. A veces también

se hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar información, pero otras veces es instalar malware, sabotear sistemas, o robar dinero a través de fraudes.

Una de las innumerables formas de phishing lo constituye el Vishing, es similar al phishing tradicional pero el engaño se produce a través de una llamada telefónica, prima facie constituiría el supuesto objeto de la exposición de los hechos de la cautelar (fs. 1 pto II y III Objeto y Hechos).

Los daños causados por el phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales.

Hay varios programas informáticos anti-phishing disponibles. La mayoría de estos programas trabajan identificando contenidos phishing en sitios web y correos electrónicos; algunos softwares anti-phishing pueden, por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con los phishing recibidos por el usuario.

Muchas organizaciones han introducido la característica denominada «pregunta secreta», en la que se pregunta información que sólo debe ser conocida por el usuario y la organización. Las páginas de Internet también han añadido herramientas de verificación que permite a los usuarios ver imágenes secretas que los usuarios

seleccionan por adelantado; sí estas imágenes no aparecen, entonces el sitio no es legítimo.

También han surgido soluciones que utilizan el teléfono móvil (smartphone) como un segundo canal de verificación y autorización de transacciones bancarias (phishing y pharming: nuevas modalidades de estafas on line, por DANIEL MONASTERSKY, CLARA M. COSTAMAGNA, 2005, www.saij.jus.gov.ar, ARTÍCULO INÉDITO, Id SAIJ: DACC050104, CSJN, 11.5.1993, Fernández, Alba O. c/ Ballejo, Julio A. y otra, LA LEY, 1993-E, 472).

Es fundamental en este estado de situación, es decir en el marco de la declaración de la pandemia, que los consumidores y usuarios sean objeto de protección por su condición de débiles jurídicos, tutela que debe darse en forma extendida, tanto en lo atinente a la protección de su vida, de su salud, de su dignidad, de sus intereses económicos, información adecuada, educación de sus derechos y del acceso en condiciones continuas a bienes y servicios necesarios para satisfacer sus derechos e intereses (arts. 42 C.N., 38 CPBA. 1, 2, 3, 5, 10 10bis y concds Ley 24240, t.o. Ley 26361, 100 Reglas de Brasilia, Secciones 1, 2, 3 y sigts).

En el caso de la prestación remota de servicios, enfocado, en la red de cajeros automáticos por la cual presuntivamente se obtuvo por terceras personas un crédito e inmediata transferencia a terceros, lo que refleja la documental de fs. 1, en formato PDF, referidos a los movimientos bancarios (Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos Aires, SENTENCIA 15 de mayo de 2008, CAMARA NACIONAL DE APELACIONES EN LO

COMERCIAL. CAPITAL FEDERAL, CIUDAD AUTÓNOMA DE BUENOS AIRES, Magistrados: Gerardo G. Vassallo - Juan J. Dieuzeide - Pablo D. Heredia, Id SAIJ: FA08971926), prima facie acredita el cumplimiento de los recaudos propios del marco cautelar.

En rigor, una de las obligaciones primordiales del Banco, que constituye el presupuesto básico de los servicios que ofrece, es que éstos sean brindados, tanto cuando se lo haga en forma personal como cuando lo sea por medio de elementos mecánicos o electrónicos, con total seguridad para el cliente. No está de más recordar que los servicios ofrecidos por cualquier Banco inciden directamente sobre el patrimonio del usuario, tanto en sus operaciones pasivas como en las activas (ver clasificación de las operaciones bancarias a Garrigues J., "Curso de Derecho Mercantil", T. IV, página 165). La garantía de inocuidad prevista en el art. 5 de la Ley 24.240 supone la presencia de un producto seguro, que no genere daños en condiciones de utilización normales o razonablemente previsibles.

Por tal razón, el Banco Central de la República Argentina ha establecido y reiterado en su normativa, la imposición a los Bancos de contar con "mecanismos de seguridad informática" que garanticen la confiabilidad de la operatoria (Comunicación A 6878, 3.8.5), como también que en el marco de la emergencia sanitaria la Comunicación A 6942, prorrogada por la Comunicación A 6949 derivó la operatoria del sistema financiero a los canales electrónicos y de cajeros automáticos, principalmente.

A efectos de cumplir con el recaudo de contracautela, en razón que el peticionante reviste la condición de consumidor, y la gratuidad establecida por las normas para los reclamos que realizan los consumidores, estimo justo y razonable establecer la caución juratoria que considero rendida con el escrito inicial de demanda (art. 195, 199 CPPC; art. 53 Ley Nacional 24.240).

TERCERO) Atento todo ello y teniendo en cuenta asimismo el dictamen favorable emitido por el Ministerio Público Fiscal de fs. 4, corresponde decretar el anticipo jurisdiccional innovativo requerido inaudita parte, teniéndose por rendida la caución juratoria con la presentación del escrito de inicio, conforme el beneficio de gratuidad otorgado de pleno derecho precedentemente (Art. 53 Ley 24.240), a dichos fines se librará cédula a la accionada B. P. de B. A. C. M., con carácter de urgente y habilitación de días y horas inhábiles (art. 153 Cód. Procesal), para que en el plazo de CINCO DIAS, haga cesar los descuentos al actor H. G. M. DNI . . . . ., que se efectúen en su cuenta sueldo N° . . . . . originados por el préstamo obtenido por la suma de $153.000 el 29/4/2020 origen . . .. -datos éstos obtenidos del extracto de cuenta adjunto en PDF-, bajo apercibimiento de pasar estos obrados a la Fiscalía en Turno, ante la eventual y posible comisión de delito (arts. 106 y 239 del C. Penal), debiendo la parte demandada desplegar la actividad administrativa que estime corresponder a los efectos de cumplimentar la presente manda.

***POR TODO ELLO**, fundamentos legales y lo normado en los arts 34 inc. 3, 161, 195, 199, 232 y concs. del C.P.C.C.; 1, 2, 5, 52, 53, 65 y concdts. ley 24.240;*

***RESUELVO:** I) Hacer lugar a la medida cautelar INNOVATIVA requerida en el escrito en vista, por un término de NOVENTA DIAS CORRIDOS, que se cumplirían el 30 de octubre de 2020, de consuno al Considerando precedente en el que se analizara su prorroga de conformidad al grado de avance de los autos que tramitan ante el fuero penal descripto en las Resultas y/o la acción civil que promueva. II) En consecuencia, intimar al Banco P. de B. A. C. M., para que en el plazo de CINCO DIAS, haga cesar los descuentos al actor H. G. M. DNI. . .., que se efectúen en su cuenta sueldo N° . . . originados por el préstamo obtenido por la suma de $153.000 el 29/4/2020 origen . . ... -datos éstos obtenidos del extracto de cuenta adjunto en PDF-, bajo apercibimiento de pasar estos obrados a la Fiscalía en Turno, ante la eventual y posible comisión de delito (arts. 106 y 239 del C. Penal), debiendo la parte demandada desplegar la actividad administrativa que estime corresponder a los efectos de cumplimentar la presente manda. III) La cautelar se otorga con carácter provisional y la caución en atención al beneficio de gratuidad otorgado de pleno derecho se considera rendida con la presentación del escrito de inicio (art 53 ley 24.240; 195, 199 CPCC); IV) En el término de diez días de notificado de la presente deberá denunciar en autos la acción principal que promovería a consecuencia de los hechos descriptos en la pretensión cautelar.*

REGISTRESE. NOTIFIQUESE íntegramente la presente a la parte actora por Secretaría por cédula electrónica en los términos del art. 7 segundo párrafo del Ac.3845/17 SCBA, con carácter urgente y habilitación de días y horas inhábiles, y al B. de la P. de B. A. por cedula, quedando en cabeza de la parte actora la confección de la misma en los términos de la Res. 10/20 SCBA, con carácter urgente y habilitación de días y horas inhábiles a la parte demandada conforme se ordenará supra (arts. 38, 135, 143, 143 bis, 153 del C.P.C.C., texto según ley 14.142; 1° y sgtes, del Reglamento para la notificación por medios electrónicos que constituye el Anexo I del Ac. 3845/17 S.C.B.A.).

Déjase constancia que más allá que el escrito en proveimiento fue recibido en el módulo de presentaciones electrónicas y firma digital (Ac. 3886/18 S.C.B.A.), y que el presente proveído es firmado por el Infrascripto digitalmente, corresponde su impresión únicamente a los fines de su registro, por tratarse el presente de un expediente íntegramente digital (arts. 11 y sgtes. Ac. 3975/20 S.C.B.A.).

CARLOS JOSÉ CATOGGIO

JUEZ

Firmado digitalmente art. 5 Ac. 3975/20 S.C.B.A.[3]

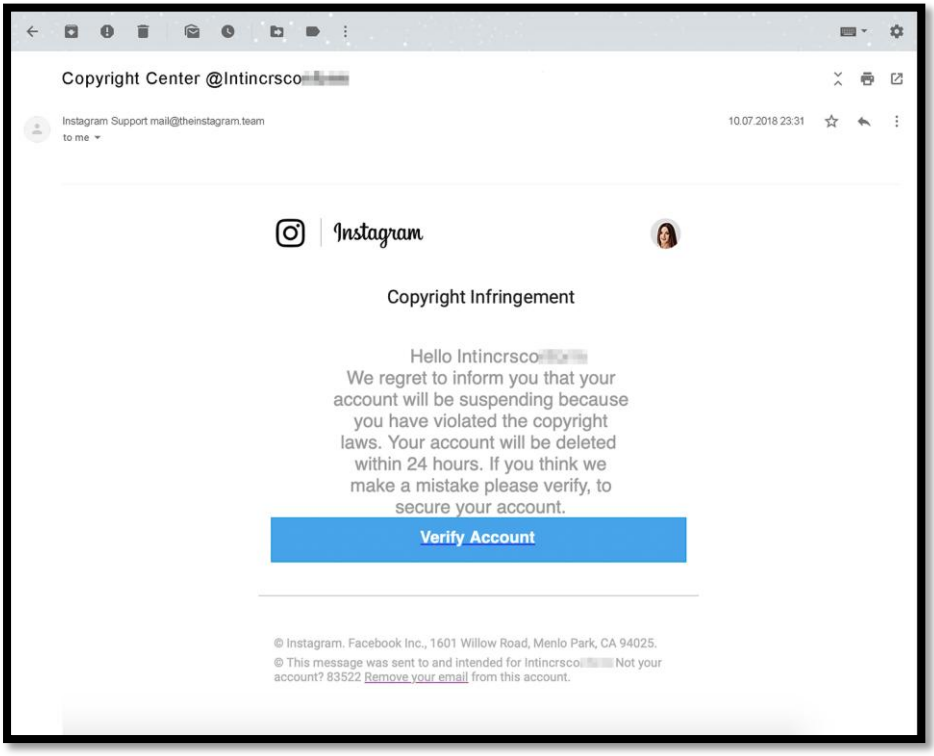
3

https://www.erreius.com/Jurisprudencia/documento/20200804140320535/medida-cautelar-innovativa-entidades-bancarias-responsabilidad-bancaria-defensa-del-consumidor-coronavirus-estafa-phishing

En la misma sintonía, ahora abordaremos el hurto de las cuentas de la red social INSTAGRAM, esto es un nuevo objetivo por parte de los delincuentes, ya que muchos comercios, ante el cierre de sus locales en venta al público, usaron la red social como vidriera para poder mover y vender sus productos. El auge de Instagram se dio, ya que, al ser una red social dedicada a las imágenes, fue adoptada por casi todos los comerciantes para poder mostrar sus productos, y llevar un catálogo personalizado a todos los dispositivos de bolsillos.

El fin de esta maniobra siempre ha sido el económico, por eso existe un mercado negro de venta de cuentas hurtadas, en lugares como la Deep web o darkmarket que abordaremos un poco más adelante para entender este mundo. Las cuantas sustraídas, incrementan su valor mientras más viejas o más tiempo de creación tienen, ya que estas pueden ser limpiadas en su totalidad y poder armar un nuevo perfil con una creación de cuenta de hace 5 años atrás.

Al elegir el delincuente este objetivo o víctima, el cebo o carnada que usará suele ser similar al siguiente:



Mensaje que alude a la infracción de los derechos de autor protegen trabajos u obras originales tales como obras literarias, obras musicales, grabaciones de sonidos, películas y grabaciones, obras teatrales, pinturas y esculturas, coreografías y pantomimas, y obras de arquitectura.

Esta alerta si bien es **FALSO** ante nuestro usuario que publicó una fotografía, y que suele agarrarte desprevenido, y que amenaza el bloqueo de nuestra cuenta, nos solicita en el botón azul verificar nuestra cuenta, esto llevará a una página falsa, totalmente falsa pero idéntica a la de logueo de la red social. El fin que busca es despojarnos de nuestras credenciales, usuario y contraseña. Quedando en manos del delincuente nuestro sitio.

Esta será rápidamente modificada, cambiando el correo electrónico asociado y el teléfono de respaldo, con el fin de quitarnos el acceso a ella.

Luego de esto, existen dos caminos que seguirá nuestra cuenta, la primera puede ser, borrar su contenido completo, dejando solamente el nickname sin fotografías ni posteos anteriores, para ponerla a la venta en el mencionado darkmarket.

La otra posibilidad es utilizarla como medio de extorsión y con mensajes tales como …"*si quieres obtener nuevamente tu cuenta, deposita …$ xxx dinero en mi cuenta y te restituiré tu cuenta*."

Logrando una tradicional extorsión con un objeto despojado nuestro. Pero las maniobras no terminan ahí, ya que el delincuente informático se caracteriza por la creatividad y su manera de mutar los modus operandi tradicionales. Otro destino que tiene esa cuenta, es utilizarla usurpando la identidad a la persona que le fuese sustraída la cuenta, y contactando a todos sus contactos, con propuestas como la siguiente: …" Holaaaa tengo

algunos dólares para vender a precio oficial y no al dólar blue, esto te puede generar un negocio interesante, si te sirven deposítame en esta cuenta CBU o CVU xxxxxxxxxxxxxx Alias: teestoyestafando nombre: Soy un delincuente…. Esta cuenta es de un amigo…" Con esa mentira logra que los contactos que ven un negocio redondo, ya que creen que están hablando con el dueño de la cuenta, depositan con confianza en esa nueva cuenta que les entrega por mensaje directo o privado el delincuente. Volviendo a retomar la premisa, el delincuente avanza en esta modalidad por las faltas de denuncias de los cientos o miles de intentos que lanzó hasta tener éxito. Pero qué pasa luego que somos despojados de nuestra vidriera digital como lo es nuestra cuenta de Instagram?. El primer paso lógico sería realizar un ticket ante la empresa y un reporte, para intentar restablecer nuestro acceso, luego sería realizar la denuncia ante la justicia argentina.

Ransomware:

El término con el que comienza, "**ransom**", es una palabra inglesa que significa "**rescate**" y "**ware**" proviene de soft**ware**". El ransomware es un software extorsivo: su finalidad es impedirte usar tu dispositivo hasta que hayas pagado un rescate. Pero qué pasa con la historia de esto, seria acertado decir que también esta técnica nació en esta era.

Si les cuento que hay registros de algo primitivo en 1989, que tenía similares características de un ransomware,

sería como hablar de la película que nos motivó hace muchos años, VOLVER AL FUTURO, denominado PC Cyborg reemplazaba el archivo AUTOEXEC.BAT, posteriormente ocultaba los directorios y cifraba los nombres de todos los archivos de la unidad C. Algo primitivo sonara ahora, pero en ese entonces era un virus muy potente. Su fin era que el usuario pagara 189 dólares para “renovar su licencia”.

En época del 2013/15 aparece **CryptoWall** es una variante no tan conocida de CryptoLocker, aunque logró superarlo en lo que refiere a infecciones. Donde se hace conocido en nuestro país, por atacar la Barranca SRL, un grupo propietario de estaciones de servicio en Río Cuarto y otras localidades de la provincia argentina de Córdoba, denunció ante la Justicia cordobesa que fue víctima de una extorsión informática. Un delincuente extranjero bajo el seudónimo de “Jack Williams” cifró todos los archivos de la compañía y tuvieron que pagarle 2.500 dólares para recibir las claves que les permitieron desbloquear sus datos y registros contables.[4]

Desde entonces este tipo de virus, empezó a mutar y hacerse más fuerte, con variantes de entrada a nuestros sistemas operativos, y diversas maneras de esconderse, esto hace que los profesionales de la seguridad informática y técnicos no puedan blindar el 100% de los sistemas, y estén a merced de estas maniobras extorsivas.

[4] https://www.welivesecurity.com/la-es/2014/05/08/empresa-argentina-victima-ransomware-2500-dolares-rescatar-archivos/

Otro punto fuerte de este tipo de virus, es que utiliza los pagos en monedas digitales como el Bitcoin BTC haciendo realmente duro el rastreo del dinero del pago del rescate.

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **20/01/15 - 16:13** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

167h **59**m **00**s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted **2860** files.

Refresh | Payment | FAQ | Decrypt 1 file for FREE | Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

bitcoin

1. **You should register Bitcon wallet (click here for more information with pictures)**

2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - **Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- coinmr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bticoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. **Send 2.17 BTC to Bitcoin address:** 1JYYzNHDaGC7noiE4eKatuYA4AThqVocDd

4. **Enter the Transaction ID and select amount:**

[ ] 2.17 BTC ~= 500 USD ▾ Clear

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. **Please check the payment information and click "PAY".**

PAY

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

0 valid drafts are put, the total amount of **0** USD/EUR. The residue is **500** USD/EUR.

Como si fuese poco, este potente virus mutó y empezó a apuntar a los dispositivos de bolsillo, como son los celulares, o dispositivos móviles. A mediados de 2014 ve la luz malware de la familia filecoder para Android, su función consistía en escanear la tarjeta SD del dispositivo móvil en busca de archivos con extensiones específicas, con el mismo propósito: cifrar y exigir el pago de un rescate para descifrarlos.

La rápida proliferación de este tipo de virus hace pensar que llegó para quedarse, y la creatividad de los delincuentes, hicieron que mutase tantas veces, que en 2020/21 este virus se convierta en lo que se conoce como **RaaS.** Este acrónimo es utilizado por su traducción al inglés de ransomware como servicio. Es un modelo basado en suscripción que permite a los afiliados utilizar herramientas de ransomware ya desarrolladas para ejecutar ataques de ransomware. Los afiliados ganan un porcentaje de cada pago de rescate exitoso. Este modelo pasó a ser no solo más peligroso, sino que muchos profesionales comienzan a tomar este servicio como un arma que puede ser utilizada contra infraestructuras críticas, que son todos aquellos sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económico, medioambiental y político. Una alteración o interrupción en su funcionamiento debido a causas naturales (por ejemplo: una inundación que afecta al suministro eléctrico) o provocada por el hombre (por ejemplo: un atentado terrorista o un ataque cibernético a una central nuclear o a una entidad financiera) podría conllevar graves consecuencias.

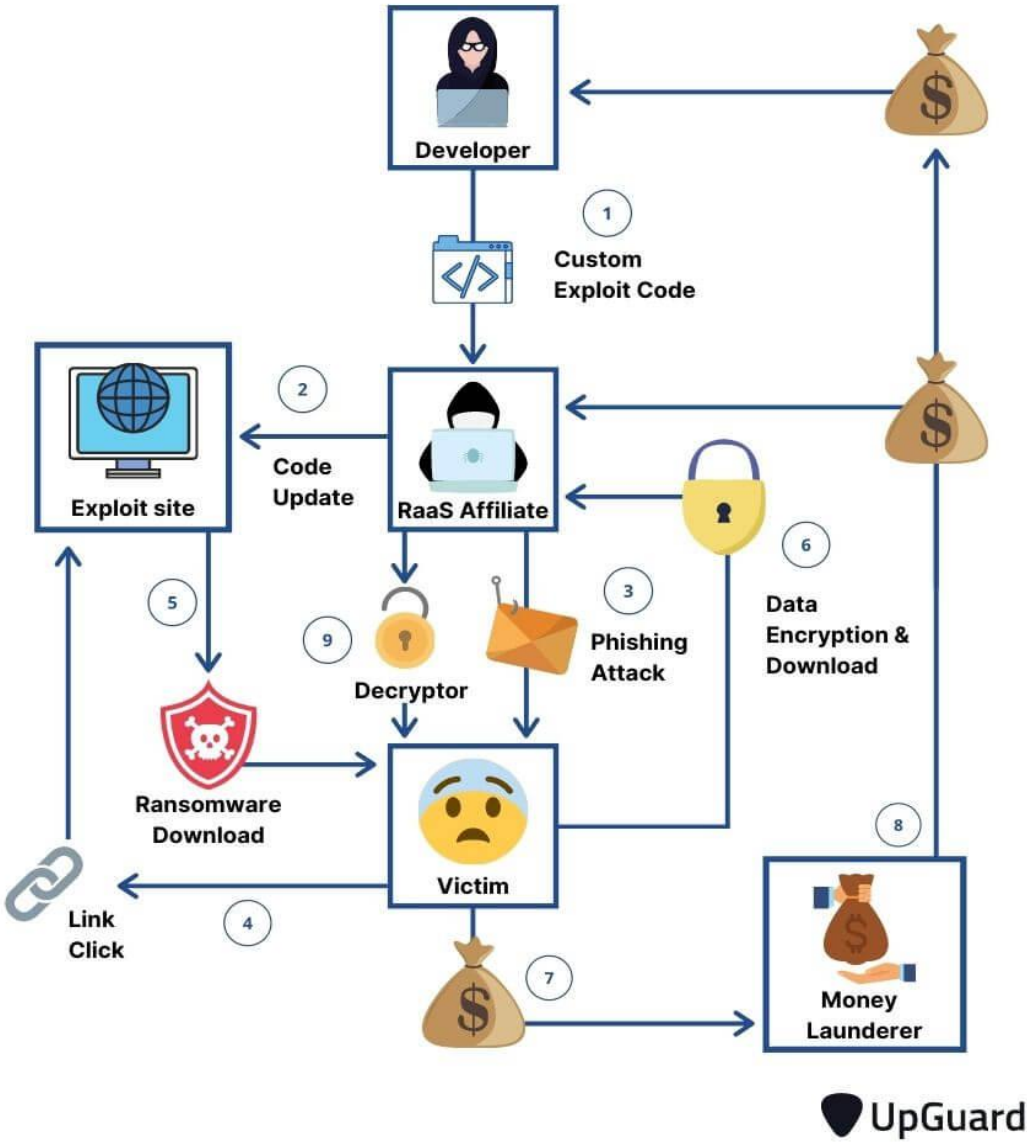
Para que este tipo de modelo de servicio de ataque funcione, debe tener tres patas centrales, la primera un buen programador informático que arme el software, y lo vuelva indetectable ante los sistemas actuales; por otro lado, un operador hábil en el uso para poder filtrar este virus, ante una víctima desprevenida, y, por último, una cantidad considerable de cuentas, electrónicas, de criptomonedas, que puedan lavar el dinero que se obtiene como ganancia, de este acto delictivo.

Generalmente esto cuando se inicia, el informático que arma el virus, lo hace con múltiples usuarios, esto hará que los adquirientes puedan loguearse al sitio que usualmente se encuentra en la Deep Web, y bajar el archivo infeccioso, y puedan abonar el uso de este nuevo virus, para ser usado en objetivos específicos. Esto le dará al informático, acceso al destino infectado y cuando el delincuente logre cometer por fin la extorsión final, compartir con este desarrollador partícipe del delito un porcentaje del chantaje que logró obtener. Esta práctica no solo creció, sino que también trae aparejado un riesgo enorme, ya que el informático recibe dinero para mantener el virus actualizado e indetectable, claramente dando señales de la modalidad de crimen organizado. Hay que comprender que acá se empiezan a tejer nuevas modalidades delictivas en lo que se transforma una industria criminal, donde en foros de la Web Oscura, se reclutan a diario técnicos con habilidades específicas, para poder mantener esta industria creciente.

Las víctimas de esta nueva modalidad generalmente son abordadas mediante la técnica de Phishing o mensajes

directos, que presentan un link que les hace de punto de entrada al virus. Con la llegada de la pandemia, y la enorme información pública, sumado a los foros de opinólogos, que ensucian los canales de comunicaciones oficiales, hicieron un cultivo perfecto para que crezca esta modalidad, no sabiendo qué es cierto y qué no en cuanto a información recibida por tema Covid-19. Una vez que se descarga el virus, en tu sistema operativo, sea cual fuere este, (Windows, Android, etc.), se va moviendo y a cada paso intentara desactivar los antivirus u hacer que confíen en el para quedarse ahí. A esta altura el ransomware, se conecta con su servidor, fuera del sistema y realiza la descarga de los paquetes adicionales, para terminar de armarse el virus, dentro de su hospedador nuevo, empezando a cifrar todos los archivos e incluso a copiarlos y alojarlos en máquinas en la Deep Web. En estos últimos meses una nueva mutación del virus, logró adquirir la posibilidad de saltar dentro de la red donde está conectado el hospedador, y lograr mantener de rehén a toda una empresa. Una vez que se completa el ataque, el virus, deja en el sistema una nota escrita en un archivo .TXT donde instruye a la víctima a pagar un precio de rescate a cambio de la contraseña de descifrado.

Algunas de las bandas que surgieron en estos últimos meses, realizan una doble extorsión a sus víctimas, la primera es el pago para lograr acceder a su información que se encuentra cifrada, y el segundo es la NO publicación de esos datos sensibles robados. A continuación, se presenta un esquema de cómo es el ataque.



Fuente: https://www.upguard.com/blog/what-is-ransomware-as-a-service

Si llegamos a esta altura, y entendimos un poco este mundo del fraude informático, es hora al mejor estilo Netflix de recordar un caso que conmocionó al mundo cuando se habla de ataques con este tipo de virus.

WannaCry El ataque comenzó el viernes, 12 de mayo de 2017 y ha sido descripto como sin precedentes en tamaño, infectando más de 230.000 computadoras en más de 150 países.
La novedad que trajo este ataque es que el virus Wannacry fue utilizado con un exploit, (es una palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.).5 Utiliza el exploit conocido como EternalBlue, este exploit se supone que fue desarrollado por la NSA Agencia de seguridad Nacional de EEUU. Para saltar entre dispositivos conectados a una misma red.

Recuerdo como si fuese ayer, a las 18 hora argentina mi teléfono, comenzó a recibir mensajes de whatsapp, de informáticos amigos, dando cuenta que este ataque comenzó a surtir efecto en nuestro país, logrando quitar acceso a diferentes computadoras. Entendiendo que esto era un problema serio, todos los informáticos, nos dirigimos a nuestros lugares de trabajo para securizar los

[5] https://es.wikipedia.org/wiki/Exploit

sistemas o sacarlos de línea para evitar la propagación de este virus.

El miedo no deja de acechar, volviendo a esa tarde del 12 de mayo, el Sistema Nacional de Salud del Reino Unido (NHS por sus siglas en inglés) informó que 684 de sus organizaciones fueron atacadas por medio de un ransomware, incluidos los grupos de prácticas generales, hospitales y laboratorios. Se estima que tuvieron que cancelar 19 mil citas.

Esta cita nos deja un sabor amargo en la boca y el corazón agitado, en todos los países tenemos corporaciones médicas que actúan como empresas enormes, esto hace pensar que sus servicios informáticos tienen los estándares de empresas tradicionales, esto el delincuente lo sabe y por ello sus armas fueron apuntadas a estas corporaciones médicas, porque el objeto de extorción no solo es información financiera sino que empiezan a tomar valor, no la reputación sino las vidas humanas que dependen de ese servicio. Qué pasaría si un paciente falleciera producto de un ataque informático, esto sería una horrible película de terror, pero lejos está de ser ficticio.

Asesinada por un virus: un ataque 'ransomware' termina en la muerte de una paciente

Un paciente perdió la vida después de que el hospital alemán que debía atenderle no pudiese al sufrir un ataque de 'ransomware' en su sistema informático.

17 septiembre, 2020 - 19:51

Esto ocurrió el 10 de septiembre del año 2020, cuando un hospital universitario de la Universidad de Düsseldorf, fue atacado por un virus de esta familia de ransomware y provocó el fallo de todos sus sistemas, esto sumado a que en la era informática los pacientes empiezan a contar con historias clínicas digitales, entre los pacientes que tuvieron que ser derivados a otros hospitales se encontraba una mujer en condiciones graves, que tuvo que ser enviada de urgencia a un hospital en Wuppertal, a 32 kilómetros de distancia. Claramente esto deja en manos de los fiscales la carga de utilizar la imaginación para usar el código penal para investigar estas mutaciones de los delitos que empiezan a impactar en la vida cotidiana de las personas. Quedan en el tintero, preguntas como, ¿El desarrollador del virus, es responsable junto con quien utilizó el virus y atacó al hospital? ¿Es posible el secuestro del dinero virtual, que no está declarado por el estado como activo producto del crimen? ¿Puede ser considerado un virus

informático como arma? Y por último, ¿La programación de un virus en una computadora por parte de una persona, puede ser considerada un acto delictivo? Son muchas preguntas que el derecho argentino debe empezar a preguntarse y plantear nuevos escenarios que a nivel mundial se están dando.

CAPITULO II

Fraudes informáticos

Objetivos:

Los avances tecnológicos de las últimas décadas desembarcaron en la llamada tercera etapa de la revolución informática, tiempos en los que actualmente vivimos. La tecnología y las diversas plataformas informáticas son aliados estratégicos de la sociedad, siempre planteamos que este universo paralelo con efectos en la vida fisica es una ventana al mundo que permite comunicarnos, expresarse, acceder a información, trabajar, estudiar, entre las múltiples opciones que los ciudadanos pueden acceder para que su día a día sea más simple.

Los nuevos empleos, ejemplo desarrolladores, que se encuentran ligados a la industria relacionados con la tecnología crecieron a pasos agigantados en todo el mundo, es más la globalización tecnológica ha permitido poder trabajar o estudiar en el otro lado del mundo sin tener que viajar. Sin lugar a dudas los beneficios positivos de la revolución informática son cuantiosos y

sorprendentes, y continuarán una dinámica así diaria en materia de perfeccionamiento y desarrollo. Es decir, la tecnología y la inteligencia artificial seguirán sorprendiendo y es la sociedad – en su mayoría ya dependiente en forma directa o indirecta de la tecnología – quien deba seguir capacitándose y estudiando frente a los nuevos cambios que propone el sistema.

Si bien a las plataformas informáticas en los años prepandemia se fueron incorporando nuevos usuarios, el 2020 ha sido un año bisagra principalmente en los países que han tenido cuarentenas extensas como por ejemplo la Argentina, donde indefectiblemente millones de personas han tenido a las plataformas informáticas como una herramienta para trabajar, estudias o comunicarse. En resumidas cuentas, observamos más usuarios y más horas de usuarios frente a las plataformas informáticas. Es decir, un ciberespacio con más gente y mucho más activo.

Pero la inteligencia criminal nunca queda atrás de los cambios y más en un escenario de alcance global donde el nivel de esclarecimiento de los hechos delictivos aún tiene una tasa muy baja ya sea por la complejidad en la investigación como así también los bajos índices de denuncia. Es por es ello que siempre recomendamos resguardar la prueba y denunciar, ya que es la única llave que abre la puerta de la justicia y de las estadísticas criminales.

Las causas del crecimiento del fraude informático

En la obra “Crímenes en la Web, los delitos del siglo XXI” destacamos que gran parte de los crímenes tipificados en

el Código Penal, pueden configurarse a través de medios informáticos y otros que si bien por cuestiones físicas y quizás porque aún no avanzó la tecnología en forma suficiente en estos tiempos, no podrían configurarse a través de internet, esto puede ser un gran aliado para lograr los objetivos criminales, como las reducciones de elementos productos de un robo por citar un ejemplo.

A colación de los expuesto, es importante comprender la mente criminal que en su mayoría tiene objetivos netamente económicos sin importar el modus operandi. Ellos parten de dos premisas recaudar lo mas posible y arriesgarse lo menos posible. A veces no se logran cumplir ninguna de las situaciones, otras algunas, pero cuando hablamos del modus operandi virtual la situación de riesgo para las bandas criminales se atomizan y la recaudación se potencia.

Si bien el delincuente devenido en cibercriminal quiere “trabajar” a gusto y con menores riesgos, como destacaba anteriormente los objetivos económicos son los principales motores de las organizaciones criminales en la web. Entre ellos encontramos el narcotráfico, lavado de dinero, la extorsión on line, y los diferentes tipos de fraudes descriptos por el profesor Romero.

Si bien los incidentes pueden venir de cualquier parte del mundo en algunos casos se requiere mano de obra local para completar el delito. Hay casos en que un hecho esta dividido en células independientes, por ejemplo una roba o filtra datos a través de phishing o softwares espías y no comete el fraude, sino que vende la información en le mercado negro para que un tercero cometa el otro ilícito

(el primero es el robo de datos), tratándose de hechos autónomos ya que quien roba los datos no participa ni de la logística ni de los beneficios del fraude. Incluso en algunos casos las organizaciones tercerizan la logística del phishing, principal metodología utilizada para el robo de información sensible que posteriormente se utilizará para configurar el fraude.

1. **Compras de productos en portales no validados o redes sociales:** el usuario recibe o encuentra ofertas atractivas en redes sociales o portales en su mayoría alojados en el exterior, quienes reciben el pago por tarjeta de crédito o transferencia, no recibiendo el comprador la contraprestación o producto que intentó adquirir. En muchos casos dichos perfiles son eliminados y dejan de contactarse con las víctimas.

- En los casos que se abona con tarjeta de crédito la misma puede ser utilizada para realizar compras de forma ilegitima
- En el caso de realizar transferencias, en muchos casos el “supuesto” beneficiario puede ser un “presta cuenta”, que puede o no estar al tanto de la actividad criminal, aunque vale señalar que no está exenta su participación penal por ser partícipe en el hecho.

2. **Robo de información a través de llamadas telefónicas:** Se observaron casos donde el delincuente dice representar a organismos gubernamentales o empresas solicitando a la víctima datos sensibles bancarios para acceder a

diferentes beneficios. Aquí se descarga el ardid criminal quien mediante diferentes manipulaciones lingüísticas logra que la víctima brinde datos sensibles que le permitirán al delincuente configurar la estafa. Es por ello que siempre recomendamos no compartir información por ningún medio, aunque el solicitante suene muy convincente.

3. **Phishing:** los correos falsos de bancos o tarjetas de crédito han sido una constante en los últimos años ya que el nivel de profesionalismo y masividad con el que trabajan los delincuentes hace que en muchos casos la victima sea engañada y entregue los datos de su tarjeta de crédito -con su código de seguridad – para que el criminal pueda realizar diferentes compras o extraer dinero. El caso de fraude bancario lo veremos en el siguiente punto.

- el contacto puede hacerse a través de email falsos emuladas (el receptor a prima fase vera una apariencia real) o líneas prepagas con WhatsApp a listados de contactos usuarios segmentados o no obtenidos en el mercado negro.

- En ambos casos puede tratarse de organizaciones locales, internacionales o mixtas, pero todas con su conexión logística local.
- El robo de información a través de correos es una trampa donde no solo extraen datos bancarios o de tarjetas de crédito (mejor dicho, la victima los ofrece engañada) sino que también utilizan esos datos para crear falsas identidades o suplantadas y luego configurar otros ilícitos.
- El phishing también es utilizado para que la víctima cliquee en archivos con cargas de virus y afecte los

dispositivos como el Ransoware o correos espías que reportarán todos los movimientos del ordenador a los criminales.

- Tambien es utilizado para engañar en falsas aplicaciones de redes sociales cuando el delincuente obtiene los datos, cambia las claves y correos de seguridad para que la víctima no pueda recuperarlos. El objetivo puede ser: extorsionar a la víctima para que esta tenga q pagar un rescate; utilizar ese perfil para engañar e intentar estafar a los contactos o bien vender la cuenta en el mercado negro. Siempre se recomienda tipear la url o descargar la app del sitio oficial, nunca confiar en enlaces que solicitan validar datos.

4. **Engaño social:** en este nuevo modus operandi, el criminal tiene dos víctimas, a una le sustrae información de sus contactos telefónicos (generalmente se guardan en directorios de cuentas de email y estos son vulnerados a través de phishing o malwares espías en los dispositivos. También, como describimos, el delincuente puede adquirir el listado de contactos y datos de la víctima en el mercado negro.

   El primer paso de la organización criminal (generalmente es un proceso criminal industrializado, en escala y organizado) obtiene los datos de la víctima y sus contactos. Luego adquiere un número de telefonía celular prepago e instala whatsapp configurando el perfil como si fuera la propia víctima (en Argentina la usurpación de identidad no es delito aún). El tercer paso es informar a todos los contactos que cambió el

numero de teléfonos y así entablar una conversación con el objetivo del engaño económico. Ya sea que le solicita dinero prestado o que le cambien dólares indicándole una cuenta bancaria para que la víctima deposite – luego hablaremos del alquila cuentas-. Pero no estamos frente a simples encantadores de serpientes, sino que se trata de bandas organizadas que pueden estar en cualquier parte del país o en el exterior cuya preparación tanto en el léxico, su presentación y su procedimiento de contacto hace para muchas víctimas creíble al supuesto perfil y así lograr que en tiempo récord se le deposite el dinero en una cuenta bancaria.

Estos modus operandi varían todo el tiempo, hay es whatsapp, ayer eran las cadenas de emails, mañana serán otras herramientas las que utilicen los delincuentes para engañar. Pero la información siempre será la base fundamental de este tipo de metodología. La prevención es la base para evitar este tipo de hechos ya sea para evitar que el delincuente recopile datos como también para estar a la vanguardia de estas modalidades y hacer caso omiso ante este tipo de abordajes.

5. **Fraude bancario:** en los últimos tiempos, si bien los bancos han avanzado en la concientización de sus clientes sobre diferentes formas de abordaje que tienen los ciberdelincuentes para defraudarlos, el crecimiento de las herramientas digitales, el aumento de usuarios y el desarrollo criminal no han podido frenar el crecimiento de este tipo de delitos, que afecta a todos los estratos sociales con instrumentos bancarios.

El objetivo del delincuente es el dinero y éste va a hacer todo lo posible para llegar a él, no le importa quién es la víctima.

El primer paso es ingresar a la cuenta. Pero ello requerirá clave y contraseña. En algunos casos también un número de documento o número tributario, Estos datos lo pueden obtener de listados de clientes conseguidos ilegalmente como así también a través de campañas de phishing que como explicamos anteriormente, el cliente “engañado” le brinda a una página falsa todos sus datos a los efectos de una supuesta validación, que en realidad es parte de la estrategia criminal.

En muchos casos tener acceso al home banking, para el delincuente no es suficiente para hacerse con el dinero , si bien puede pesificar la moneda extranjera , observar las cuentas y hasta sacar créditos personales al instante y con un solo clic de varios cientos de miles de pesos , pero que lo que precisa ahora es transferir a una o varias cuentas “cómplices”, que como bien dijimos pueden ser cuentas alquiladas o prestadas por terceros que no tienen conocimiento que se utilizan para este fin pero no escapan a la responsabilidad penal. Para ello, y dependiendo de la entidad bancaria, cargan esas cuentas como amigables o proveedores con su cuit y CBU (no ocurre en todos los casos reportados).

En el segundo paso, tiene que actuar muy rápidamente para lograr ganar la confianza de la víctima y avanzar hacia su objetivo que es la transferencia del dinero. Uno de los modus operandi más habituales es el bloqueo del acceso home banking colocando DNI y usuario correcto pero la contraseña incorrecta varias veces.

Ni bien se bloquea, en cuestión de segundos el delincuente se contacta con la victima haciéndose pasar como empleado del banco (ya tienen todos los datos de la víctima), – si es por WhatsApp aparecerá el logo del banco – para advertir que notaron que se había bloqueado la cuenta y que ayudarían a reactivarla. El cliente confirma que eso es así e inicia el proceso para obtener una nueva clave. Puede ser que el mismo delincuente le indique una nueva clave. Acto seguido, delincuente ingresa en forma paralela y prepara una transferencia a una o múltiples cuentas, le va a pedir al usuario o bien que le indique un token, un nro. de seguridad que llegará por email o mensaje de texto o bien datos de la tarjeta de coordenadas, con esos datos que le brindó la víctima, el delincuente salvo algún imprevisto va a haber logrado trasferir el dinero.

Otras de las formas de operar, saltean el proceso de confianza de bloqueo de cuenta y al obtener a través de phishing los datos de accesos le solicitan el token o coordenadas para confirmar alguna validación que en realidad es la transferencia que configura el fraude.

Un ultimo engaño son las falsas redes sociales de bancos – muchas de ellas se dejaron de usar-, en donde el delincuente solicita los mismos datos sensibles para lograr sus objetivos. En estas redes sociales es muy probable que se trate de cuentas dormidas que se compran en el mercado negro –para lo que se demuestra cierta antigüedad en la fecha de creación – y que tengan cierta actividad durante meses para que la víctima considere creíble y realice su consulta. Tambien dentro de la puesta en escena, las cuentas se nutren de seguidores falsos y

descartan la sospecha de la falsedad al encontrarse con una cuenta con pocos seguidores.

El tema más sensible que observamos es que varias de las víctimas tenían poco dinero en cuenta, por ello el delincuente, que se encuentra detrás de una computadora, logró obtener créditos personales al instante y transferidos por alguno de los métodos enunciados. Debiendo la víctima pagar la cuota de un dinero que nunca recibió – difícilmente pueda pagar – y costear una investigación para dar con los autores del hecho sin garantías de recuperar el dinero.

En Argentina ya existen varios fallos en materia civil donde se ha planteado la responsabilidad objetiva y los métodos de confirmación para el otorgamiento de dichos créditos. Es decir, si bien la víctima puede tener un grado de responsabilidad, no es un experto en seguridad cibernética, por ende son las entidades las encargadas de velar por la protección de sus clientes e intentar mediante mecanismos de prevención evitar este tipo de incidentes, cuyas modalidades van cambiando constantemente. Recordemos que hoy en día el cibercriminal opera con mas tranquilidad que de manera física ya que en la mayoría de los casos no se expone físicamente como en un robo a mano armada, este tipo de hechos se denuncia poco y el detalle que hace más relevante al incremento de estas modalidades es que se recauda rápido y hasta se industrializa el crimen, ya que el objetivo fundamental es el económico.

Otras modalidades:

En esta tercera etapa de la revolución informática la tecnología avanza a alta velocidad para bien pero lamentablemente también para el crimen. Es que el mundo criminal ya está de lleno en el ciberespacio operando individual o muy organizadamente, se perfeccionan, coordinan entre diferentes bandas criminales para realizar acciones y por sobre todo van cambiando las modalidades para configurar diferentes tipos de delitos. Dichas modalidades, en este universo paralelo que es internet, llegan de un lado a otro del planeta en cuestión de días u horas, si hablamos de su adaptación al modo local, aunque en materia de delitos de modalidad tecnológica pueden concretarse desde cualquier parte del mundo, solo se precisa “información” y un modus operandi.

ESTAFAS MASIVAS A TRAVES DE WHATSAPP

Argentina no está aislada del mundo en materia tecnológica y de conectividad digital, por ello las metodologías que azotan a sus ciudadanos pueden tener muy pocas variantes a las que podrían afectar a todos los países de la tierra. La diferencia es que hay naciones en este mundo que tienen como política de estado la Ciber seguridad y la educación preventiva de sus habitantes. Es decir, la educación es una herramienta muy importante para evitar ser víctima de engaños digitales, fraudes, robo de datos, destrucción de archivos o extorsión todo depende del grado de compromiso, prioridades que tengan los gobiernos y por supuesto, su visión presente y futura en materia de hipótesis de conflictos.

Pero mas allá de los expuesto las variaciones de fraudes on line son constantes, algunas muy básicas, otras más estructuradas pero la realidad es que esto es y será una constante en tiempos donde la tecnología cada día depende más de las acciones del ser humano.

Una de las modalidades que más me sorprendió fue una forma de estafa a través de whatsapp, quizás por el desenlace de varios casos que conocí y por las diferentes hipótesis y conclusiones a las que llegamos.

Nuestro país entre fines de 2020 y fines 2021 comenzó a vivir un fenómeno masivo que afectó a ciudadanos de todo el país, al menos 18 provincias han detectado casos, que por el modus operandi es casi indubitable que se trata de mano de obra local.

El sistema es el siguiente: El delincuente adquiere una o varios números de teléfono móvil prepago, logra habilitar la línea (colocando un DNI cualquiera y acertando tres preguntas personales de habilitación que no son muy complejas, o bien terceros brindan esos datos sin saber cual va a ser el objetivo final, falsas encuestas, falsas promociones, ingeniería social, son algunos métodos de los delincuentes que utilizan para obtener información personal y luego habilitar las líneas).

Una vez habilitada la línea prepaga a nombre de determinada persona continúan con el segundo paso que es buscar a las víctimas a quienes se va a usurpar el perfil de WhatsApp (la usurpación / suplantación de identidad digital, no es delito en Argentina).

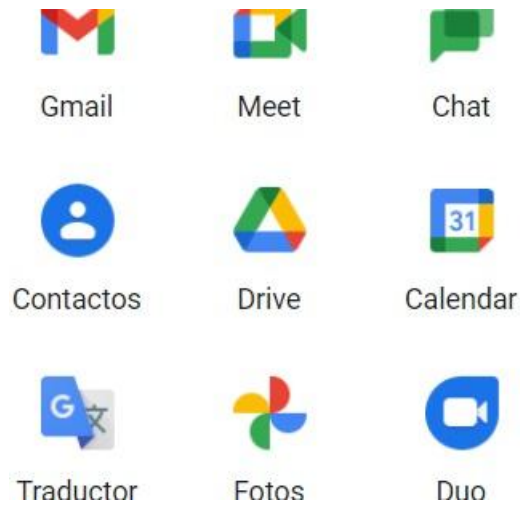
El siguiente paso es acceder a los contactos de WhatsApp de la víctima, que generalmente los guarda en archivos en correos electrónicos o en drives en la nube. Para ello el criminal intentará acceder a dichos correos, en muchos casos se utiliza la clásica metodología del “phishing “o “falsos correos” que llegan en forma masiva a las personas solicitando validar datos personales, entre ellos la contraseña.

Ese falso correo (con el logo y diseño grafico similar a la compañía como puede Hotmail, Gmail, etc.) los lleva a un link para hacer el supuesto proceso de validación (es una falsa página, con diseño grafico similar a la empresa donde le exigirá colocar datos personales y contraseña). [6]

Con dicha información el delincuente puede cambiar la clave y apoderarse de la cuenta o bien solamente almacenar la información de acceso sin tocarla.

Luego ingresa a la cuenta de correos y busca el archivo WhatsApp donde la víctima tiene almacenados todos los contactos y por ende los datos. Luego baja el archivo con todos los datos, lo carga en el WhatsApp falso. Previamente se va a haber creado un perfil de WhatsApp similar al de la víctima (Nombre y foto, pero con el número distinto – el prepago-).

[6] https://www.elperiodico.com/es/activos/innovadores/20210212/espana-cabeza-mundial-enganos-estafas-11513245



Con estos pasos el delincuente ya va a haber creado un perfil de WhatsApp idéntico al de la víctima, habilitado la línea de teléfono y cargado todos los contactos de la misma.

Luego comenzará a enviar WhatsApp masivos a todos los contactos diciendo “hola como estas, soy …. este es mi nuevo número agéndalo “, (el envío puede ser manual o a través de programas de envió masivo de whatsapp). Al poco tiempo, minutos, horas, días, llegará otro WhatsApp masivo (de la víctima con el perfil usurpado) solicitando cambiar dólares de urgencia y ofreciendo una buena comisión (tambien existen casos de pedido urgente de dinero).

Se le pide a la otra víctima (los contactos) que les depositen la suma correspondiente a los pesos en una cuenta de un banco local (generalmente utilizan cuentas

alquiladas a personas que en su mayor parte no saben para qué las alquilan). Ni bien se recibe el dinero en la cuenta por diferentes mecanismos la retiran y bloquean al contacto que la depositó (obviamente nunca le llevan los dólares ni le devuelven el supuesto préstamo de "urgencia").

En algunos casos utilizan el mismo número que se utilizó en casos anteriores para cometer fraudes para suplantar la identidad de otras víctimas, cargar sus contactos e intentar nuevas estafas o bien habilitar nuevas tarjetas.

Todos estos pasos no significan que una misma organización criminal sea los que los realice, porque puede tratarse de diferentes organizaciones criminales que se dedican a cuestiones específicas. Unas a habilitar líneas prepagas y "calentarlas" (término que se utiliza cuando se le da cierto uso a una cuenta de whatsapp nueva para que esta no sea bloqueada por spam); otros pueden ocuparse de conseguir los datos de la víctima usurpada y sus contactos; y la tercera, hacer el fraude. Es decir las dos primeras células pueden no estar conectadas con la última (aunque claro está que cometen el delito de acceso indebido a medios informáticos entre otros), incluso no necesariamente estén en Argentina, ya que el phishing, robo de datos y la habilitación de líneas telefónicas puede hacerse desde cualquier parte del mundo (dejando claro que también líneas ip pueden habilitarse para whatsapp), ya que los primeros pueden

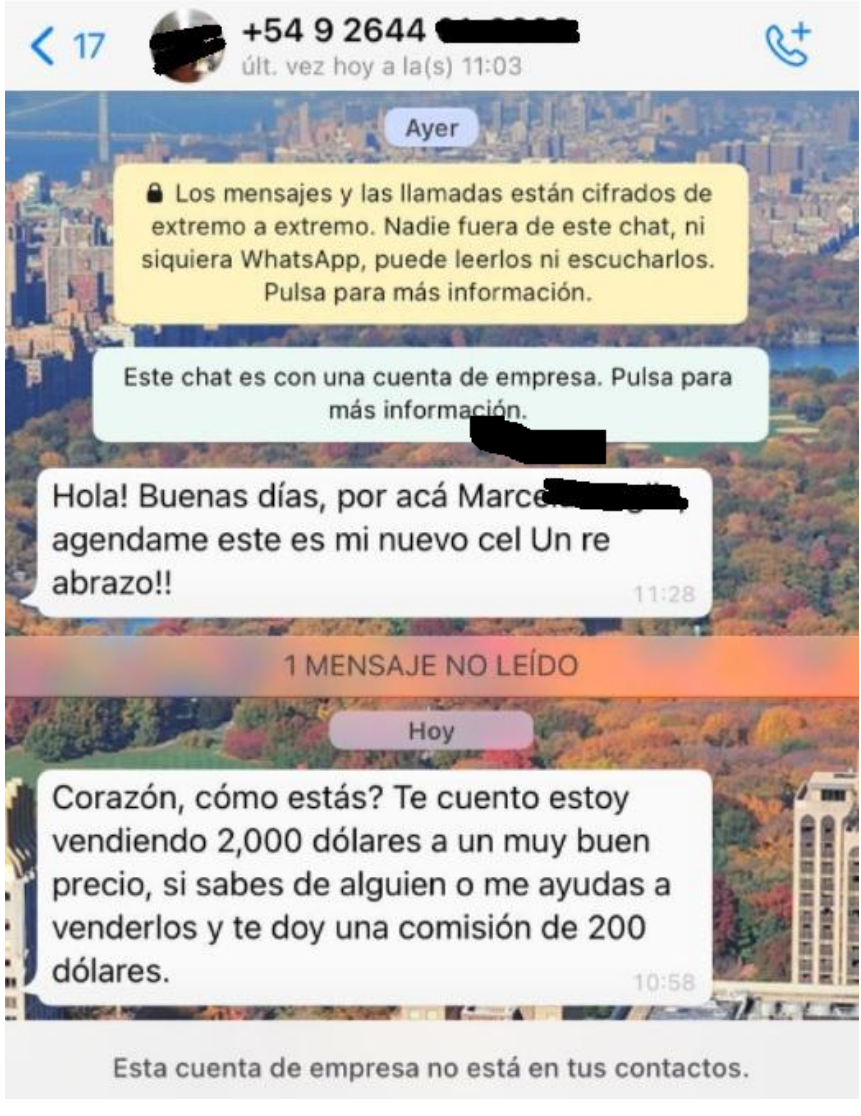
solamente vender los datos a los últimos en el mercado negro.[7]

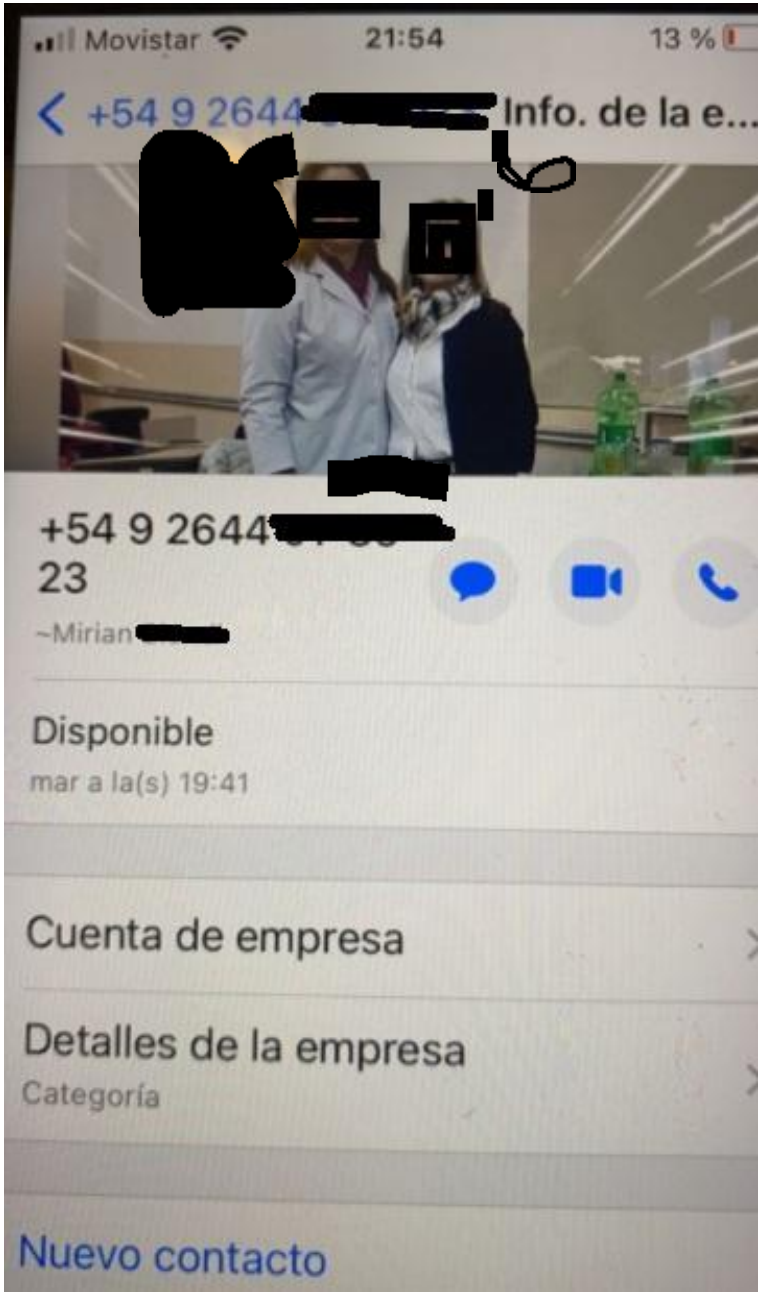
Otras formas de hacerse con los contactos de la víctima – aunque consideramos menos probable para el caso en análisis – es el envío masivo de archivos espías, la compra en el mercado negro de información de cuentas producto de filtraciones en las compañías.

Por lo expuesto bridamos las siguientes recomendaciones:

1) Colocar contraseñas seguras en las cuentas de correo (mayúsculas, minúsculas, números y caracteres) y cambiarlas de manera frecuente.
2) Colocar el doble factor de identificación tanto en WhatsApp como en las cuentas de correo.
3) Colocar clave de seguridad en whatsapp.
4) No validar ninguna contraseña si llega un correo o whatsapp solicitando ello o cualquier tipo de información.
5) Si uno quiere realizar algún cambio, tipear la página o ir a la app original.
6) Escanear con antivirus tanto el móvil como otros dispositivos.
7) Si es víctima de este u otro delito a través de internet denunciar y aportar todos los datos que se tenga a disposición.

[7] https://www.infobae.com/sociedad/policiales/2020/08/01/mafia-de-instagram-el-drama-de-la-joven-de-quilmes-a-la-que-le-secuestraron-su-cuenta-con-mas-de-300-mil-seguidores/


17
+54 9 2644
últ. vez hoy a la(s) 11:03
Ayer
Los mensajes y las llamadas están cifrados de extremo a extremo. Nadie fuera de este chat, ni siquiera WhatsApp, puede leerlos ni escucharlos. Pulsa para más información.
Este chat es con una cuenta de empresa. Pulsa para más información.
Hola! Buenas días, por acá Marce
agendame este es mi nuevo cel Un re abrazo!!
11:28
1 MENSAJE NO LEÍDO
Hoy
Corazón, cómo estás? Te cuento estoy vendiendo 2,000 dólares a un muy buen precio, si sabes de alguien o me ayudas a venderlos y te doy una comisión de 200 dólares.
10:58
Esta cuenta de empresa no está en tus contactos.


Movistar
21:54
13 %
+54 9 2644
Info. de la e...
+54 9 2644
23
~Mirian
Disponible
mar a la(s) 19:41
Cuenta de empresa
Detalles de la empresa
Categoría
Nuevo contacto

Capitulo III

Ataque a las Comunicaciones

Si decimos te mandé mensaje, tácitamente nos estamos dirigiendo a la aplicación adoptada a nivel mundial como plataforma de mensajería, si es **WHATSAPP** y al ser el vehículo de nuestras comunicaciones, claramente estamos ante un nuevo objetivo suculento para los criminales. Por ese motivo cuando el ojo de estos criminales se posó en este nuevo objetivo, nuestro sistema de comunicación adoptado como casi única plataforma, se vio afectado más de una vez. Entremos en un pantallazo de algunos ataques comunes que sufre esta plataforma de comunicación.

Sin alejarnos del fin del delincuente que sigue siendo obtener un dato para poder cambiarlo a modo de extorsión por dinero, la plataforma de mensajería no solo pasa mensajes tradicionales como un…" Buen Día" y algún emoji que refleje nuestro estado de ánimo. Sino que es utilizada por empresarios, para impartir opiniones de negocios, utilizada por parejas para la práctica de sexting (Es un término que implica la recepción o transmisión de imágenes o videos que conllevan un contenido sexual a través de las redes sociales y/o mensajería). O por ejemplo, utilizado por el Estado de diferentes países para poder notificar a las personas su turno de vacunación en esta pandemia que transitamos. Fue tan aceptado que hasta la justicia tomó esta plataforma para la notificación judicial de resoluciones, sin olvidarnos de los bancos que lo utilizan para recordarte los turnos que tienes al igual que los hospitales. Recordando uno de los mensajes del

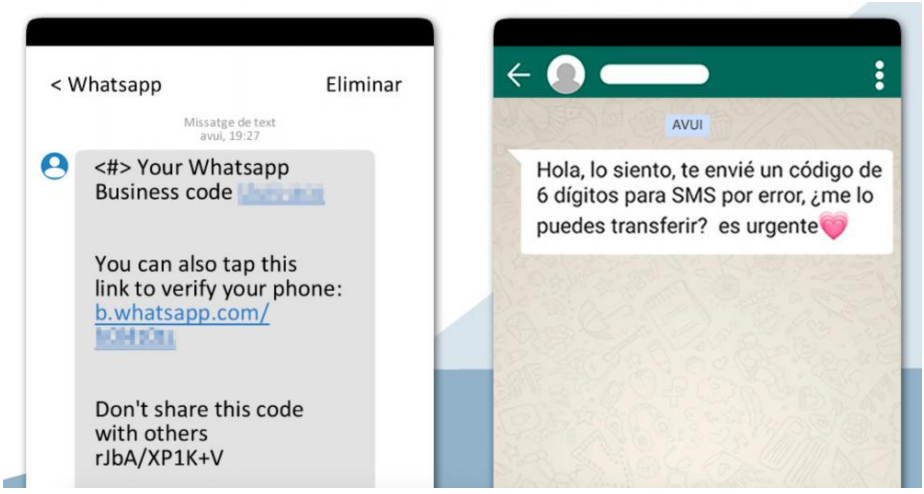
gobierno argentino que ante el avance del coronavirus recomendó la práctica de sexo virtual, conocido como sexting.

El médico infectólogo José Barletta afirmó durante el parte matutino de la cartera de salud que "todavía hay poca información sobre cómo puede transmitirse el coronavirus durante el acto sexual". Por eso, desaconsejó tener relaciones “con desconocidos” y dio más pautas sobre cómo practicar sexo seguro durante la emergencia sanitaria. Ante este comunicado, los expertos informáticos vieron la posibilidad de que éste sea un nuevo vector de ataque por parte de los delincuentes, ya que esa información alojada en las bases de datos de la plataforma de mensajería whatsapp dejaría expuestos momentos de la intimidad de una persona que puede ser utilizada para la extorsión si cae en manos equivocadas.

El médico infectólogo José Barletta

Al estar a la orden del día, como suele llamarse cuando una técnica se transforma en moda, el rápido aprendizaje por parte de los delincuentes de este nuevo vector les da la delantera transitoria a los delincuentes para preparar el cebo y mediante nuevamente la técnica de Phishing, intentar tomar control de las credenciales de mensajería de la desafortunada víctima.

Todo comienza con un mensaje que la víctima recibe en un momento que no está en guardia con su seguridad, este estado desprevenido hace que el delincuente, aborde con un mensaje simple intentando sacarle los seis (6) dígitos de verificación de la cuenta. Para poder usurparle su identidad ante el resto de los interlocutores.



Mensaje recibido a la izquierda por la víctima y a la derecha el delincuente intenta convencer mediante cualquier ardid que le entregue esos dígitos para lograr entrar a sus comunicaciones.

Capitulo IV

Sexting

Cuando nos referimos al sexting acrónimo de 'sex' o sexo y 'texting' o escribir mensajes, claramente esto cambió con el avance del tiempo y la tecnología, ya que se incorpora también mensajería instantánea, chat de diferentes plataformas, claramente ampliando la capacidad y elección de las personas al elegir un canal de comunicación para esta práctica. Sumado esto al despertar sexual de los jóvenes de la nueva era digital, que son nativos de estas plataformas nuevas, y promovedores de las nuevas. Además del erotismo nativo, fenómeno que se ve en aumento en las plataformas digitales. Donde los usuarios suben representaciones de sensualidad a través del cuerpo y la imaginación, quizás de esa forma pueda representarse al erotismo, donde cada día se aprecia más el contenido sensual-sexual.

De este tema se desprenden dos situaciones casi típicas, la primera: Cuando dos personas en pareja se filman, guardan en sus dispositivos las fotos y videos. Pero luego cuando se pelean, o separan, uno de ellos que tiene los archivos guardados, y sin saber cuál es el motivo exacto, quizás celos, venganza, o simplemente intento de dañar a la otra persona, los hace circular por diferentes plataformas. Claramente la obtención de esos archivos, sí fue aceptada por las dos partes, pero no así su publicación.

Otro caso es, ante la etapa de seducción de estos nativos digitales, suelen pasarse varios archivos, de contenido

casi sexual, para irse conociendo o experimentando etapas nuevas. Esto claramente fue instaurado por esta generación que vive a través de los bytes, pero ese material sensual-sexual queda alojado en los dispositivos y en muchos casos con copias en las nubes, esto quiere decir que por lo menos habrá cuatro copias en cada dispositivo del mismo archivo, esto acarrea un problema enorme porque cuando borramos el archivo lo borramos de una sola locación del dispositivo quedando sin saberlo 3 copias más. A modo de ejemplo, se vería así el proceso, al sacar una fotografía y enviarlo a través de la plataforma de whatsapp. Quedaría en la carpeta DCIM que corresponden a las palabras “Digital Camera Images”. Pero al enviarla a través de whatsapp como plataforma de comunicación, se hace una copia en la carpeta Whatsapp/Imágenes, por tal motivo tenemos dos archivos idénticos, en dos locaciones. Pero si creemos que acá termina, falta todavía. Como cada dispositivo, necesita un correo sea Android o IOS y esos correos tienen nubes, que permiten tener backup en automático de todo, nuestras fotos, se guardan localmente en un tercer lugar dentro de nuestro dispositivo, carpeta denominada Drive/Backup la cual prepara el material para subir, y por último, como nativamente no tenemos una galería vistosa en nuestros teléfonos, solemos bajar galerías en forma de software, y este hace lo propio, al tener acceso a nuestras fotografías y videos, quedando en muchos casos una última copia en sus carpetas internas. Con todo lo expuesto hasta aquí, queda demostrado que perdemos el rastro de nuestros archivos digitales no solo cuando

subimos estos a internet, sino en nuestro propio dispositivo también.

A esto se le sumará un nuevo lenguaje técnico-jurídico si me lo permiten, para intentar describir situaciones relacionadas con la mutación del delito. Sextorsión nueva palabra que quiere imponer la extorsión con uso de estos archivos sensual-eróticos. … *Ciberseguridad, Se multiplican los casos de sextorsión: "Tenemos imágenes suyas en situaciones íntimas",* titulan algunos diarios sobre estos temas, claramente llama la atención de los lectores, pero qué pasa con las causas verdaderas de extorsión en estos temas.

El modus operandi

Según la denuncia del joven extorsionado en la causa del fiscal Quintana, todo se inició el 25 de diciembre pasado, cuando ingresó al sitio de encuentro ar.skokka.com y allí contactó a una mujer que se hacía llamar "Camila" y decía tener 21 años.

Tras intercambiar una serie de fotos y chatear vía WhatsApp, la supuesta joven -se cree que se trata de perfiles falsos-, le ofreció sus servicios sexuales y la víctima aceptó concretar un encuentro.

Sin embargo, desde el número de WhatsApp le llegó un primer audio de un hombre que le decía que "estaba en problemas" porque la chica que acababa de contactar era una menor de edad que estaba desaparecida y que había sido captada por una red de trata.

El supuesto policía le advirtió que habían hecho la denuncia contra él por haber ingresado al perfil de la chica y que iban a hablar con el juez para que manden la orden de detención.

El joven borró todos los chats, pero el mismo hombre le mandó un audio por WhatsApp desde otro teléfono cuya foto de perfil tenía un policía vestido de uniforme y allí le dijo que era miembro de la Policía Federal (PFA) y que si quería evitar la detención debía pagarle 10.000 pesos.

El denunciante, asustado, accedió y pagó esos primeros 10.000 pesos a través de un link de Mercado Pago, pero a la media hora recibió un mensaje de otro número distinto y esta vez otro hombre le dijo que era "el comisario", que estaba esperando la orden de su detención "por el tema de la chica desaparecida y que, si quería "frenarla", le debía pagar 20.000 pesos.

En esta oportunidad, el extorsionador tenía como foto de perfil un martillo y una balanza como símbolos de la justicia y borraba los mensajes del chat cada vez que la víctima los leía.

El joven volvió a pagar con otro link que le enviaron y a través de la misma aplicación Mercado Pago, pero cuando todo parecía terminado, una semana más tarde volvieron las extorsiones.

El mismo hombre le pidió otros 40.000 pesos, por lo que realizó el tercer pago, pero a los pocos días el mismo falso comisario le dijo que su "tema" le había costado "15 días de suspensión" y lo obligó a transferirle otros 20.000 pesos.

Al otro día, volvió a mensajearlo con la excusa de que Mercado Pago le había cobrado más de 16.000 pesos y que debía mandarle otros 20.000 pesos, a lo que el joven volvió a acceder llegando a un total de 110.000 pesos en los cinco pagos que hizo, hubo un sexto intento de extorsión cuando el falso comisario le pidió otros 20.000 pesos "para un compañero", pero allí la víctima explicó que ya había agotado todos sus recursos económicos con los pagos que hizo con sus tarjetas de débito y crédito, donde quedó endeudado y decidió cortar toda comunicación y hacer la denuncia en la DDI de Pilar.

Tras el análisis de las cuentas, las transferencias, usuario del sitio de pagos y números telefónicos, el fiscal Quintana pidió y consiguió los tres allanamientos.[8]

Queda asentado que el éxito de esta nueva modalidad de extorsión es el miedo que tienen las victimas a la exposición del material privado, por tal motivo la única arma que se puede aportar a la sociedad es la educación, no solo la educación tradicional sino la nueva educación a la seguridad digital, donde las personas que no son nativos digitales deben aprender a entender y manejarse en este nuevo mundo digital, donde cada uno de los Bytes en internet tiene un efecto directo en el mundo real. Cabe recordar una de las películas que fue furor en 1999 año que se estrenó **MATRIX**, donde el personaje clave es tentado a elegir tomar una pastilla entre dos, una azul y

[8] https://www.telam.com.ar/notas/202103/547111-sextorsion-investigacion-pilar.html

una roja. Para cambiar su mundo el símbolo de dicho proceso es aceptar tomar una píldora roja; en cambio, la píldora azul podría devolverlo a su mundo actual sin que, aparentemente, nada de lo que está sucediendo hubiera pasado. Neo (el protagonista) acepta tomar la pastilla roja, olvidar su vida y todo lo que conoce para descubrir «qué es Matrix». Esto parece una escena del hoy, donde la mayoría de las personas que no son nativos digitales se resisten a entender qué es la vida digital, y prefieren pensar que al ser en el ciberespacio donde se da este fenómeno no tiene impacto en la vida real.

Mercado Negro

Antes de hablar del mercado negro, o también con un título más marketinero **Dark Market**, tenemos que hablar del Convenio de Budapest[9], denominado como *"Convenio Sobre la Ciberdelincuencia",* se trata del primer acuerdo internacional que hace referencia a los delitos en el mundo digital, teniendo por objeto facilitar la detección, investigación y sanciones a nivel nacional como así también internacional, establece las acciones que permitirían la cooperación internacional, siendo esta rápida y flexible, para la persecución de estos tipos de delitos, También, busca homogeneizar las definiciones sobre ciberdelito, establecer el intercambio de información en lo que respecta a estos ilícitos, garantizar el debido equilibrio entre los intereses de la acción penal y el respeto a los derechos humanos.

[9] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Cuantos países adhirieron al convenio?, figuran 68 firmados y 66 ratificados, esto hace que, en la parte legal, el o los delincuentes, organizados a esta altura como bandas criminales internacionales, sepan dónde están los países conocidos como paraísos para los delincuentes, entendiendo que ellos no están en este tratado de cooperación internacional y están atrasados en materia penal sobre Cibercrimen.

Ahora que tenemos un pequeño pantallazo de lo que sería el convenio, nos adentraremos en una aplicación que no estigmatizaremos, pero se intentará demostrar que es la más usada por algunos delincuentes que la utilizan por su anonimato.

Telegram

Telegram FZ-LLC es una organización británico-emiratí fundada por Pável Dúrov[10], entre idas y vueltas, telegram emigró de Rusia por constantes intentos por parte de este país, a conocer las claves de cifrado de la plataforma, y desde entonces, se consolidó como una plataforma de comunicación segura, y casi anónima.

Responderemos algunas preguntas, basados en la página de la misma aplicación con la intención de que al finalizar la lectura, pueda comprender su uso.

Qué es Telegram?: es una aplicación de mensajería enfocada en la velocidad y seguridad, es súper rápida, simple y gratuita. Con Telegram, puedes enviar mensajes, fotos, videos y archivos de cualquier tipo (doc, zip, mp3,

[10] https://es.wikipedia.org/wiki/Telegram_(organizaci%C3%B3n)

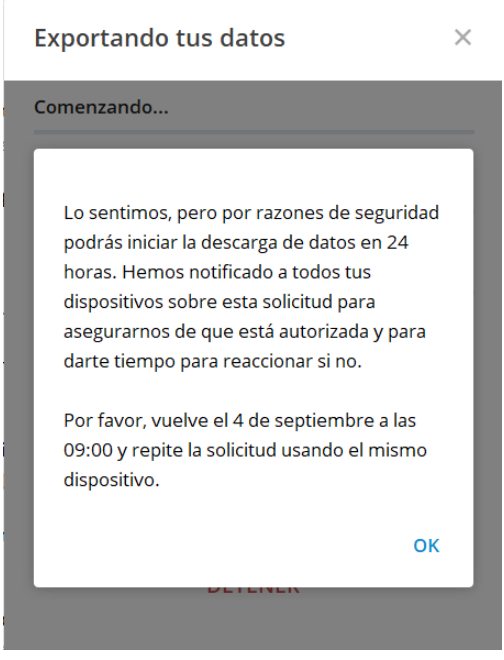
etc.), como también crear grupos de hasta 200.000 personas o canales para hacer difusiones a audiencias ilimitadas. Puedes escribir a tus contactos del teléfono y encontrar personas a través de sus nombres de usuario. Como resultado, Telegram es como el SMS y el correo electrónico combinados, y puede satisfacer todas tus necesidades de mensajería personal o de negocios. Además, ofrece llamadas de voz y videollamadas con cifrado end-to-end, así como chats de voz en grupos que permiten miles de participantes. Como Telegram permite tener hasta 200.000 miembros por grupo, tiene respuestas, menciones y hashtags, que ayudan a mantener el orden y la eficiencia en la comunicación para las comunidades grandes.

A diferencia de WhatsApp, Telegram es mensajería basada en la nube con sincronización constante. Como resultado, puedes acceder a tus mensajes desde diferentes dispositivos a la vez, incluyendo tablets y computadoras, y compartir un número ilimitado de fotos, videos y archivos (doc, zip, mp3, etc.) de hasta 2 GB cada uno. Esto hace que muchos usuarios que deben pasar pesados archivos por una plataforma de mensajería opten por esta, como así también, tener el chat en la nube, le da la ventaja de no hacer backup en ningún dispositivo de bolsillo pudiendo abrir en tiempo real su cuenta de mensajería y tener todo lo escrito y pasado en esa aplicación.

Uno de los puntos más fuerte de telegram en contra de whatsapp es que Telegram necesita menos de 100 MB en tu dispositivo. Puedes mantener toda tu multimedia en la

nube sin necesidad de eliminar cosas, simplemente borra la caché para liberar espacio. Al contrario de whatsapp que cada vez que se comparte algo, quedan copias en tu dispositivo que va ocupando espacio físico en el mismo.

Otros de los puntos que brilla en esta plataforma, que, si quieres tener una copia de todos los datos que telegram posee de ti, debes completar una serie de pasos, que requiere el dispositivo, que posee la cuenta original, y luego de esto abrir una sesión en telegram desktop en el escritorio de una pc, y solicitar una copia de todos tus datos, que se exportará, luego de 24 horas, y aceptando en el dispositivo que posee la cuenta, lo cual implica que debe estar desbloqueado.



T.me es una funcionalidad gracias a la que puedes crear enlaces cortos con tu nombre de usuario o nombre de canal o grupo. Estos enlaces, cuando son pinchados, abren de forma automática una conversación en un chat con el usuario, grupo o canal en cuestión y en este caso al ser tú quien lo comparte, contigo. El cual puedes modificar para que los usuarios que se conecten no vean tu número y solo quede visible un nombre de usuario con el cual te identifiques.

Check Point Software Technologies, una compañía que se ocupa principalmente de la seguridad informática, expone que más del 70% de los delincuentes también están presentes en Deep Web con varias cuentas en el mercado ilegal y utilizan estos sistemas de comunicación para vender y comprar productos y materiales ilegales, desde drogas hasta billetes falsos, desde cuentas hasta maniquíes para falsificar documentos, por ejemplo. Sin mencionar el número infinito de material de abuso sexual infantil y Gore que se vende, compra y se intercambia a través de estos mensajeros.

En Argentina no estamos exentos de la capacidad creativa de los delincuentes, basta con ver la siguiente noticia: ***"Crece la cantidad de delincuentes que venden certificados de vacunación falsos en Telegram"*** [11] . Hemos recorrido un poco el mundo de esta aplicación, ahora tenemos que conectar los temas, con lo que venimos leyendo más arriba.

[11] https://www.infobae.com/america/tecno/2021/08/18/crece-la-cantidad-de-delincuentes-que-venden-certificados-de-vacunacion-falsos-en-telegram/

Cuando se termina de configurar una estafa, un fraude, el delincuente necesita un canal para mover ese material producto de un ilícito, esto lleva a tomar un riesgo por parte de ellos a ser descubierto, por eso a la hora de utilizar un canal, lo que hacen generalmente es utilizar canales de telegram, o grupos, claramente para entorpecer el accionar de las fuerzas de seguridad.

Cuando terminamos el tema de Sexting, y pasamos al de Dark Market, teníamos que intentar juntar dos temas que parecen alejados entre sí, pero que a medida que avanzamos podemos empezar a entender el camino del archivo. Ahora empezaremos a entender donde esos archivos de la vida privada tienen su carretera clandestina y se ponen a la venta para ser utilizadas en futuras extorsiones, o simplemente ponerlas a la venta para consumo de diferentes internautas.

Capitulo V

La importancia de la información

La información es clave, porque podemos decir que es la llave para la configuración del fraude o la extorsión. La información es el elemento clave para que el delincuente pueda avanzar en sus propósitos. Dicha información se puede obtener de diferentes formas:

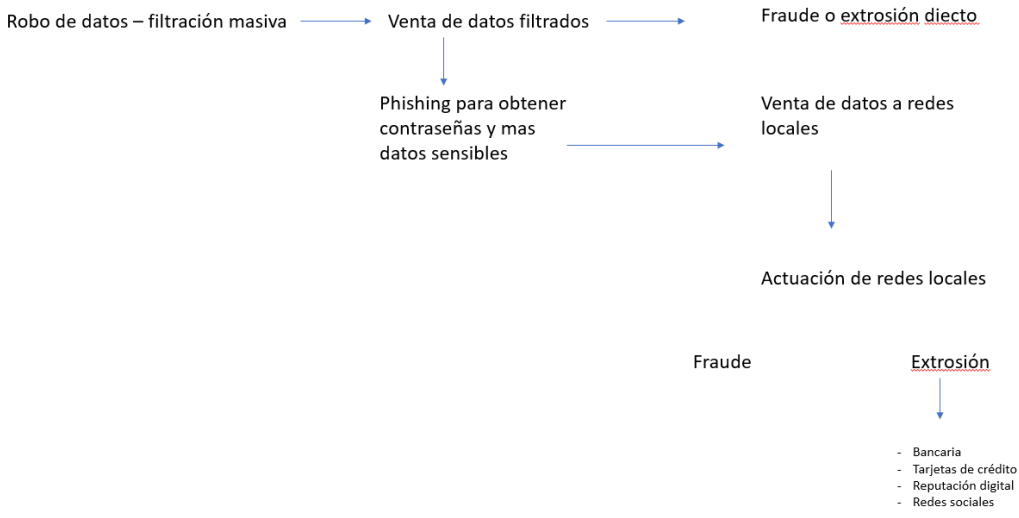
6. **Fuentes Abiertas**: Navegando en redes sociales con datos personales abiertos o en fuentes públicas de información abierta que luego se utilizará para anzuelo para ganar la confianza de la víctima y luego perpetrar el hecho delictivo (Ejemplo número de teléfono, email, nombre o datos sensibles publicidad en forma pública de una red social), esta metodología que en muchos casos es manual – aunque podría extraerse a través de scripting – se llama también inteligencia social
7. **Contactos trampa**: tambien llamados phishing, donde el objetivo es hacer creer a la víctima que la contactan de una entidad, red social, tarjeta de crédito a los efectos de que ésta ingrese a enlaces falsos diseñados cuasi idénticos a los de los portales originales (inclusión con las URL embebidas ocultando la real que es falsa) para que brinde datos sensibles como claves, nombres, tarjetas de coordinadores, respuestas a preguntas de seguridad, datos de tarjetas de créditos, etc. Si bien el phishing habitualmente llega a través de correos electrónicos hoy el email ya no es una exclusividad , y los contactos malisiosos pueden

venir por whatsapp, redes sociales, juegos en red, por citar algunos de los tantos ejemplos. Si bien en la mayoría de los casos el objetivo es económico esos enlaces maliciosos pueden descargar malware para dañar el dispositivo o bien archivos espías que remitirán mientras esté encendido el dispositivo toda la información que allí se encuentre, claves y datos sensibles incluidos, dicha información y puede utilizar para la extorsión, fraude o venta de información. El procedimiento del contacto trampa tiene los siguientes efectos:

- la utilidad inmediata para perpetrar el fraude o la extorsión.
- el cambio de claves y acceso para que la víctima no pueda acceder.
- el almacenamiento de la información en forma silencioso, es decir no cambian nada solo toman nota de los datos para utilizar más adelante.
- la venta de esa información a otras bandas criminales o al mejor postor.

Las diferentes metodologías, sin lugar a dudas, van a seguir perfeccionándose con el correr del tiempo, recordemos que los ciber delincuentes cada día van incorporando tecnología e inteligencia ya sea para recabar datos, venderlos para que otras redes criminales cometan el ataque final y directo contra el usuario, es decir, como planteamos páginas atrás bien frío y silencioso no significa que sea menos letal, ya que lo que está haciendo el delincuente es recabar datos para venderlos a otras redes criminales posiblemente locales que conocen bien las

costumbres de cada región o país para cometer delitos con acento local.



8. paginas a las que se accede por error: typosquattg y Cibersquatting

Estas son 2 metodologías muy comunes en el ciberespacio, se trata del registro de dominios de internet con errores muy comunes de tipeo, que asiduamente, el usuario que el usuario común realiza o bien la utilización de un dominio existente muy utilizado con una extensión distinta, por ejemplo si el sitio original es www.correoargentino.com.ar, las bandas criminales pueden registrar – como ya ocurrió –

www.correoargentin**OO**.com o bien .info.online, entre miles de posibilidades. Es importante en principio como ya alertó el profesor Romero, nunca confiar en los links que nos envían para validar datos y siempre que una persona tenga la intención de cambiar alguno ingresar en forma directa al portal oficial de la empresa.

Este tipo de modalidades puede utilizarse con dos objetivos, ambos últimos, el primero es sacar una ventaja comercial haciendo un uso ilegal de marcas o aprovechar – por parte de una empresa que quiera realizar lo denominado competencia desleal, registrando una página web, para que el usuario ingrese por error y asi desviar la clientela de su competencia.

El otro netamente para intentar sustraer información mediante phishing, que será utilizada, como vimos para diferentes objetivos, estos en su mayor parte son económicos, el delincuente priorizará esos datos principalmente en conjunto con elementos locales, realizará diferentes tipos de estafas como las bancarias o de tarjetas de crédito principalmente. Por ejemplo, utilizando whatsapp luego obtendrá datos sensibles:

El delincuente compra una tarjeta prepaga de telefonía móvil y configura un whatsapp bussines usurpando la marca del banco y obviamente el logo del mismo.

Delincuente: buenas tardes, sr xxxxxxxxxx, mi nombre es Carlos Lopez del Banco Nacional, su domicilio es xxxxx, su email seguro es xxxxxxx, nos contactamos porque observamos que alguien quizo ingresar a su cuenta, vamos a ayudarlo a cambiar la clave y sus accesos de seguridad

El primer paso del criminal es ganar la confianza de la víctima – cliente del banco o de la tarjeta de crédito-, para ello los datos personales sustraídos inicialmente son fundamentales para armar el speach que el delincuente local precisa desarrollar para hacerse pasar por funcionario bancario de la tarjeta de crédito a los efectos de recopilar, a través del engaño, la manipulación, y la utilización de perfil falsos utilizando ilegítimamente el logo y la marca de dichas entidades, para poder ganar la confianza del cliente, y que esté así brinde la información sensible como datos del token o variables de la tarjeta de coordenadas o bien claves de seguridad de la tarjeta de crédito a los efectos de configurar el fraude directo.

La prevención es la mejor herramienta, es una herramienta fundamental para poder evitar caer en este tipo de delitos, los datos sensibles que terminan para confirmar una operación tanto de transferencia como de compra nunca deben ser remitidos ni siquiera a terceros que dicen llamar de las propias entidades.

Por otro lado, la denuncia es una herramienta muy importante, no solamente para cuestiones estadísticas sino para poder llegar efectivamente a todos los eslabones

de la cadena delictual que configuran el fraude. No olvidemos que si bien muchas de estas compañías tienen seguros que probablemente cubren este tipo de situaciones, el fraude se está haciendo en nombre de una persona determinada, dañando en cierta forma el buen nombre y honor de dicho ciudadano.

Es por ello por lo que se debe seguir hasta las últimas consecuencias tanto la investigación como la denuncia que debe realizar el damnificado, en mi opinión es un compromiso cívico porque, de lo contrario, siguen dando vueltas delincuentes que operan libremente, y estaremos frente a una situación de impunidad.

Sin esclarecer estos hechos no haremos otra cosa que potenciar el accionar criminal.

La denuncia es la única llave para poder iniciar una investigación, y la prevención, estando a la vanguardia de todos los cambios y modalidades que van a ir modificándose en forma constante es una herramienta fundamental para evitar ser víctima.

En mi opinión, la primera opción es evitar el daño, por lo tanto, la capacitación constante de los poderes del Estado sea nacional, provincial o municipal como así también organizaciones civiles deben contribuir firmemente en campañas de prevención y capacitación para evitar este tipo de delitos. El ciudadano debe comprender que en esta tercera etapa de la revolución informática el robo de datos, el envío de malware, el fraude, la extorsión, entre otros delitos configurables a través de internet, va a ser una constante, más en mundo, en una sociedad que cada día

es más dependiente de las altas tecnologías, yo considero que debemos vivir en un mundo sin impunidad y para eso deben reforzarse las herramientas y las capacidades de las fuerzas de seguridad y los investigadores para combatir el delito en todos sus ámbitos, pero si se puede evitar, y muchos delitos son evitables, debemos contribuir firmemente a ese fin.

a) Venta de información

Como planteamos anteriormente, en estos tiempos donde la comunicación y la interconexión de los ciudadanos hacen que internet sea un universo paralelo sin fronteras, la información cotiza más que el dólar, más que el oro, tanto en materia comercial como criminal, es por eso que existe un mercado negro de datos personales que sigue creciendo en todo el mundo y los objetivos como observamos a lo largo del presente pueden ser de los más variados. Por ello no debemos distraer nuestra atención en qué y para qué brindamos información personal y si alguien intenta recabar más datos a través de supuesta información nuestra que ellos tienen, desconfiar porque puede tratarse de alguien que quiera nutrir nuestros expedientes en su base de datos, que como dijimos puede ser utilizada para diferentes fines.

La sofisticación de los ciber delincuentes ya es un hecho por varios motivos, el principal es la dinámica para recaudar información de las víctimas, la segunda es la dinámica para recaudar a través del fraude u otros delitos con objetivos económicos, la tercera simplemente data de que este tipo de delitos tiene un bajísimo grado de denuncia y de esclarecimiento, lo que le permite al

delincuente un bajísimo grado de exposición a ser descubierto.

Si bien los asaltos a mano armada, los hurtos, entre otros delitos van a seguir existiendo -porque mientras haya criminales dando vueltas por las calles eso va a ocurrir como una cuestión lamentablemente natural-, es muy probable que el modus operandi de ese mismo objetivo que es recaudar valores, en cierta forma vaya mutando, a los delitos configurables a través de internet, con esto quiero decir que, para un sector de la población criminal con cierto grado de inteligencia, es más rentable trabajar en delitos con federales a través de internet qué exponerse físicamente en la calle.

b) Objetivos de la venta de información

Tal como lo destacamos a lo largo del presente, la información que es sustraída a través de filtraciones masivas, hackeos a importantes bases de datos donde se almacena información personal de los usuarios, o bien lo obtenido mediante el engaño a través de diferentes métodos como los que estuvimos presentando en el presente, phishing, llamados telefónicos, whatsapp, la utilización ilegítima de marcas entre los presentes y los diferentes y novedosos modus operandi que vamos a observar en el futuro, como por ejemplo la inteligencia artificial para realizar ingenieria social y recabar datos personales, gustos, intereses y afinidades de los usuarios para configurar diferentes tipos de delitos con objetivos económicos.

La información es y será una moneda de altísimo valor en tiempos de la revolución informática, porque no se trata de un bien fungible como el dinero se trata de datos certeros de las personas, de las empresas que perduran con el tiempo y forman parte de la identidad real y digital de cada individuo, es decir, puede ser utilizado para diferentes finalidades sean comerciales o criminales como así también para generar perfiles usurpados o falsos y ser una herramienta para el engaño a tercero.

Por eso la información forma parte de un activo muy relevante en estos tiempos y hay muchos postores interesados en adquirir bases de datos ya sea de forma legítima como ilegítima para acciones criminales, comerciales o contradictorias a la protección de la privacidad de las personas.

Sin entrar en el análisis jurídico y reglamentario del derecho a la privacidad y en la protección de los datos personales, vale destacar, que cada país tiene su régimen interno para la protección de la información sensible de los datos de sus ciudadanos, tanto su protocolo de almacenamiento, objetivos y utilización de esos datos y por supuesto las acciones recomendadas para evitar que esas bases de datos sean vulneradas por ataques externos o filtradas por personas que abusen de la confianza del titular de la base de datos.

Si bien existen sanciones administrativas e incluso penales para quien accede ilegítimamente a una base de datos sea pública o privada, es importante destacar que en estos tiempos podemos decir que la privacidad puede tratarse de un hecho relativo, ya que no existe una

seguridad plena, una vez que brindamos cierta información a 1/3 y éste la digitaliza, el cómo se tratarán esos datos, cuál será su grado de protección y con quién se compartirán, por lo tanto la información que nosotros suministramos a la web, más allá de los órdenes jurídicos y por más rígida que puede ser la normativa, es muy probable que fluya por el ciberespacio.

El usuario tiene a su alcance diferentes herramientas para que quien se haga con la información sensible e intenta engañarlo pueda estar advertido y actuar en consecuencia, así evitar fraudes y estafas u otro tipo de delitos configurables a través de internet.

Ante este escenario tanto las redes sociales, como los bancos, como las tarjetas de crédito comenzaron a tomar seriamente nota del presente y del futuro cercano generando barreras de validación para acceder a diferentes cuentas:

- Doble factor de autentificación
- Token
- Protocolo especial si se accede desde otro dispositivo no usual
- Pin de validación en tiempo real a un mail un número de teléfono
- Contacto de validación y protocolo especial para transacciones de altos montos

Estas son algunas de las herramientas, mientras que nosotros observamos que, a lo largo del tiempo, más allá de las campañas publicitarias advirtiendo todo este tipo de

situaciones, vale destacar que la Argentina sufrió una oleada muy fuerte de fraudes informáticos de todo tipo cuyo criminal contaba con esa información personal del cliente que sumado a un buen speach, es una herramienta trascendental para cometer el engaño. Las advertencias están en los sitios web de cada entidad financiera o al menos en la mayoría, las nuevas modalidades para validar una operación o acceso a cuentas se fueron solidificando y es muy probable que esta dinámica y esta adaptación precise retoques constantes ante los nuevos retos que van a ir surgiendo a lo largo del tiempo.

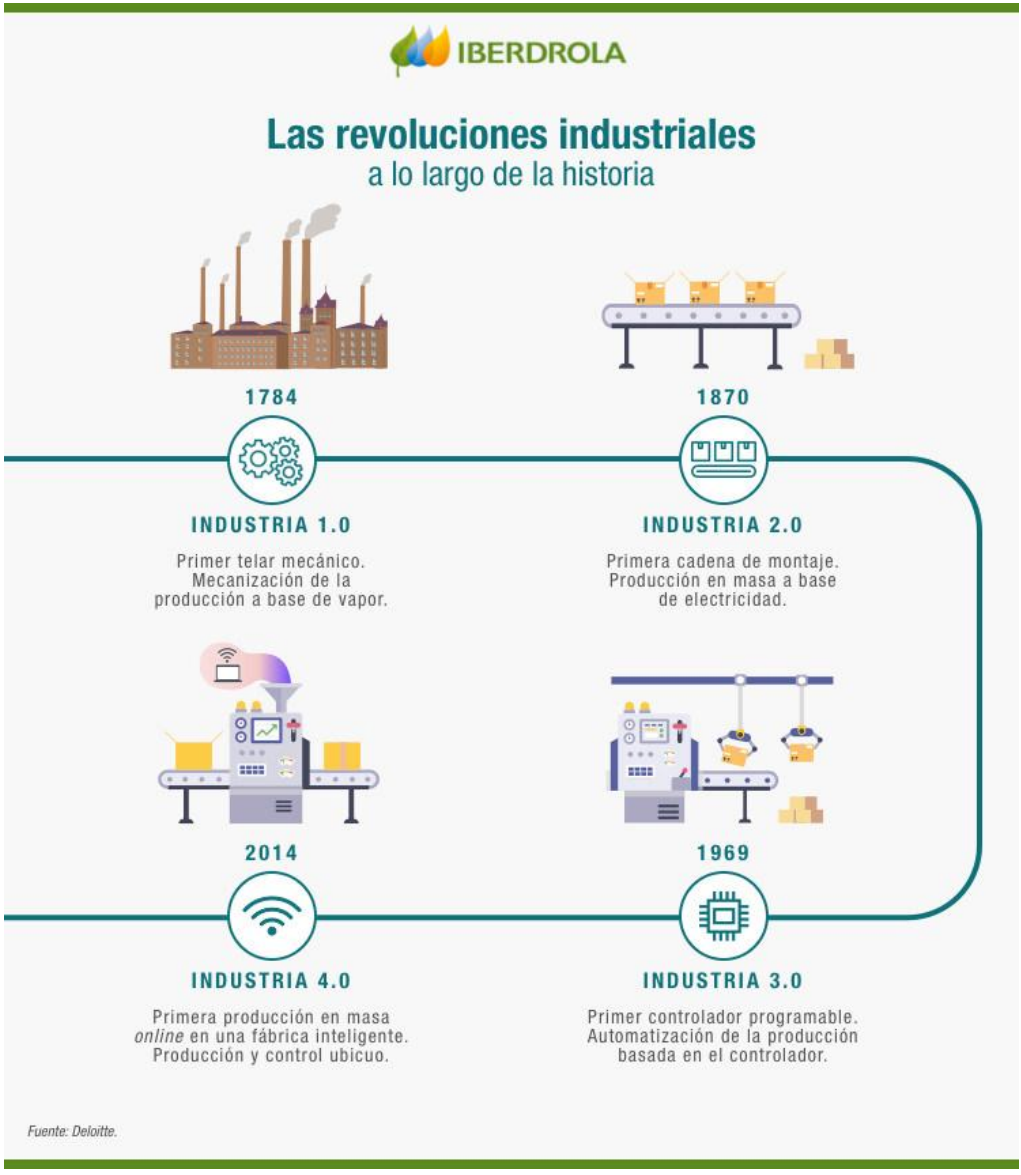
Pero cualquier tipo de medida que uno pueda tomar, incluso previniendo archivos maliciosos espías con el más potente de los antivirus, entre otras acciones que puede hacer el usuario, si este es engañado y él cree que está hablando realmente con una red social con entidad bancaria o financiera o con un comercio determinado, es muy probable que termine el mismo brindando esos datos sensibles que le van a permitir al criminal configurar la estafa. Por lo tanto la solución, aparte de todas las herramientas de protección, es también el comportamiento del buen uso de las altas tecnologías y el partir del concepto de la desconfianza respecto al tercero que nos vienen a requerir información o nos vienen a ofrecer algo prácticamente irrechazable, ingresando a los sitios oficiales contactando uno en forma directa y no dejando que 1/3 se contacte, es una de las recomendaciones más firmes que podemos brindar al día de hoy para evitar una medida como el robo de información o fraude.

Capítulo VI

La cuarta revolución: la era de la Informática

Podemos escuchar algunos que denominan esta era como la cuarta resolución industrial, al mejor estilo de ciencia ficción de una película, hablan de inteligencia artificial, y algoritmos.

Esto dará que hablar, porque las industrias cambiaron hace mucho con la llegada de la tecnología, pero no podemos dejar de tocar temas como PROMETEA, esto no es nada más ni nada menos que un software que realiza principalmente automatización de tareas reiterativas y aplicación de Inteligencia Artificial para la elaboración automática de dictámenes jurídicos.



Solo por nombrar algunas cosas que cambiaran el mundo tal cual lo conocemos, son:

Internet de las cosas (IoT): es el proceso que permite conectar elementos físicos cotidianos al Internet: desde objetos domésticos comunes, como las bombillas de luz, hasta recursos para la atención de la salud.

Robótica: La robótica es la rama de la ingeniería mecánica, de la ingeniería electrónica y de las ciencias de la computación, que se ocupa del diseño, construcción, operación, estructura, manufactura y aplicación de los robots.

Big Data: Big Data es un término que describe el gran volumen de datos, tanto estructurados como no estructurados, que inundan los negocios cada día.

Realidad Aumentada o Realidad Virtual: Acá buscaremos algunas definiciones para poder entender este nuevo tema, que últimamente cambio el paradigma de unas empresas.

La Realidad Virtual (RV) es un entorno de escenas y objetos de apariencia real —generado mediante tecnología informática— que crea en el usuario la sensación de estar inmerso en él. Dicho entorno se contempla a través de un dispositivo conocido como gafas o casco de Realidad Virtual.

La realidad aumentada (RA) es el término que se usa para describir al conjunto de tecnologías que permiten que un usuario visualice parte del mundo real a través de un dispositivo tecnológico con información gráfica añadida por este.

Veremos que son sinónimos, algunos términos, pero a medida que avanza la tecnología, los significados parecen desaparecer o mutar en nuestras mentes, para darle paso a un nuevo concepto. Meta o también conocido como METAVERSO

Meta, que proviene de más allá, y verso, que viene de la palabra universo, resumiendo MAS ALLA DEL UNIVERSO.

A diferencia de la RV y RA en este estilo de conectividad estarás dentro de internet, por ende, sumergido en una experiencia, cada usuario es capaz de comunicarse directo con otros dentro de este mundo, eso quiere decir que tendrá influencias en su comportamiento como también influirá en los objetos. Este mundo es persistente, quiere decir que, aunque el usuario no esté conectado el mundo virtual seguirá funcionando, cambiando, dando la necesidad al usuario de querer entrar, (se vendrán nuevas adicciones) lo dejo como pregunta, por la dependencia que crea este tipo de tecnologías.

Cuando me sume al desafío de armar este pequeño libro al alcance de todos, para realizar una introducción a la prevención de estafas en internet, jamás imaginé llegar a esta altura de tener que explicar que es el mataverso, y todo lo relacionado a él para poder llevar al lector, al siguiente nivel. Aceptación de que hay algo más allá que el internet 2.0 llegando ahora META.

Seguiremos un poco intentando antes de abordar el tema de metaverso, una palabra que aparecerá a lo largo de nuestras vidas a partir de ahora, NFT o también conocido

como **Non Fungible Token**, con mucha paciencia intentaré explicar qué es esto y porqué toma relevancia a partir de ahora. La definición de **TOKEN** es lo más parecido a lo que conocemos como VALE… (*Un vale es un documento para pagar ya sea un producto, o bien un servicio*). Como entonces, un token es algo que vale por otra cosa… esto permite inferir que lo puedo cambiar por el producto cuando quiero, pero siempre fungible, o sea que se gasta, que cambia su valor con el uso. A diferencia de lo No fungible, sería el caso de las criptodivisas, que no pierde su valor por ser intangible, no se gasta.

Entonces, cualquier cosa que se publique en internet, es factible de ser asociada a un NFT, esto tomará el lugar o hará la función de certificado de autenticidad. Pudiendo asociar una fotografía un archivo de música o lo que queramos y viralizarlo en internet, pero si está asociado a un NFT sabremos quién es el dueño, quién posee ese VALE por esa obra.

Jamás pensé qué difícil es poder explicar en palabras simples un tema tan complejo, pero si han llegado hasta aquí entendiendo que es NFT o **Non Fungible Token,** habremos logrado el cometido.

Entenderemos porqué los mundos virtuales de metaverso estarán asociados a los NFT, para volvernos únicos, y darles valor y sentido a lo virtual.

Escena del mundo de https://secondlife.com/

Donde creo que fue el primer universo de este estilo, que te sumerge en una actividad totalmente virtual. Por ello es nombrado ahora, claramente necesitamos avanzar años para llegar a metaverso, pero esto nos servirá de ejemplo. En la imagen observamos que el usuario d7wq se encuentra ausente, pero podemos ver su avatar, esto quiere decir, que podemos interactuar, aunque no esté conectado su usuario, a lo que, en meta, se promete que no será así, que no estará el avatar cuando el usuario no esté, dando por sentado que creará dependencia de que nos conectemos cuando los usuarios estén. Pero lo importante es que en el terreno virtual donde está mi avatar **chelochelito**, puede ser una propiedad comprada, si leyó bien, este bien intangible puede ser adquirido, a través de la tecnología blockchain, utilizando NFT y criptodivisas.

Ahora empezamos a ver como las tecnologías crean una línea difusa entre lo virtual y lo real, o podría decir ahora virtual.

Esto nos llama la atención a nosotros, pero a los delincuentes de guantes blancos se les acaba de abrir un nuevo mundo, uno virtual donde intentarán realizar las estafas por eso, ahí es donde nosotros apuntaremos las siguientes palabras.

Publican 20 TB de NFT robados: ¿simples ciberdelincuentes o una nueva postura socio-política?

En algún momento iba a pasar: crearon un sitio estilo el recordado Pirate Bay, con NFT robados, pero dicen que no son delincuentes, sino educadores

Esto recién empieza, estamos ante una nueva era de convivencia en el mundo digital por tal motivo, habrá muchos más estafadores aprendiendo las modalidades de estafas que se desprenden de este nuevo activo creado por los usuarios, los NFT, tal como ocurrió ya.

Los ladrones rastrean Internet en busca de obras de arte digitales que circulan libremente por la red para tokenizarlas y venderlas como NFT en mercados como OpenSea.[12]

[12] https://es.cointelegraph.com/news/nft-theft-is-the-newest-form-of-cybercrime-on-the-rise

Seguiremos escribiendo sobre estas modalidades nuevas, pero a no desesperarse y esperar un nuevo capítulo en 2022 que incorporaremos estos temas y la nueva revolución de metaverso en el.

.

Capitulo VII

Jurisdicción aplicable:

Llegamos al final de este breve ensayo que intenta dar una visión sobre la problemática del fraude informático y del robo de datos en tiempos donde la dinámica del ciberespacio crece a pasos agigantados. y siempre en el caso de los delitos configurables a través de internet o de los delitos transnacionales existe la disyuntiva de qué jurisdicción aplicar.

Hay países que en su normativa interna consideran que la aplicación jurisdiccional es del lugar en donde primero se denunció, otros consideran que debe aplicarse la jurisdicción del damnificado o del domicilio del damnificado, también están quienes entienden que se aplicara la jurisdicción del lugar desde donde opera el delincuente, o bien existe otro criterio que considera que debe ser la jurisdicción del lugar de los efectos del delito, este último es el criterio que considera la legislación argentina.

Aunque si hablamos de crimen organizado y de sucesos de delitos encadenados en diferentes países con diferente criterio en materia de aplicabilidad del derecho penal, la situación puede complejizarse y más en estos momentos donde podemos encontrarnos en jurisprudencias, doctrinas y pensamientos o intereses encontrados entre diferentes países.

Por ejemplo, si una banda de criminales opera desde Argentina realizando estafas en el país y en los Estados Unidos, la República Argentina va a considerar la jurisdicción aplicable la del lugar de los efectos del delito en su territorio en cambio, Estados Unidos podrá aplicar el mismo criterio, pero también podrá basarse en la nacionalidad del damnificado o bien de la empresa damnificada o bien la jurisdicción en donde realizó la denuncia.

Hemos visto muchos casos de infracción a la propiedad industrial, derechos de autor, como por ejemplo el caso de Megaupload, servicio de almacenamiento gratuito de archivos operado por Megaworld desde Hong Kong; casi siete años después, el 19 de enero del 2012, fue cerrado por el FBI.[13]

El mencionado sitio permitía a los usuarios usar hasta 2 GB de forma gratuita y compartir los links de esos archivos de forma que otros usuarios pudieran descargarlos.

[13] https://www.eleconomista.com.mx/tecnologia/7-preguntas-sobre-el-escandalo-de-Megaupload-20170220-0009.html

Los dueños de la plataforma fueron acusados de haber orquestado un pirateo informático a gran escala gracias a su portal de descargas, que fue cerrado por las autoridades estadounidenses. Entre las acusaciones se encuentra la de haber sacado 175 millones de dólares en beneficios y causar más de 500 millones de dólares de pérdidas a los derechos habientes de obras musicales, cinematográficas y otros productos pirateados.

Este es uno como tantos casos dónde nos encontramos frente a crímenes transnacionales configurados a través de internet, donde rige un principio distinto, en mi opinión, respecto a la aplicación de la jurisdicción territorial.

Si bien existe un principio y considera que la jurisdicción internacional es el lugar de situación de los hechos, más allá de que algunos países difieran de esta postura, debemos considerar que el criterio mayoritario establece que el derecho internacional público se determina en el principio de territorialidad, en el caso del derecho internacional privado la jurisdicción aplicable tiende a ser la del lugar de situación de la parte demandada.

Si bien estamos atravesando la tercera etapa de la revolución informática o bien como mencionaba Marcelo Romero páginas atrás en vísperas, de la cuarta etapa vemos de replantear la dinámica de este fenómeno que es internet , donde en las fronteras físicas no existen y la volatilidad de los efectos en uno o en múltiples lugares del planeta en forma simultánea producen un fenómeno realmente complejo, donde aún debemos sortear análisis y debates a nivel mundial para encontrar la mejor alternativa en el ámbito jurídico y en el ámbito práctico

para que los países puedan brindar un servicio de Justicia conforme a las nuevas demandas procesales y de juzgamiento que nos depara este universo paralelo qué es el ciberespacio.

La celeridad y la coordinación estratégica debe ser una condición fundamental para poder llevar adelante los procesos, independientemente de la jurisdicción que los tratados y convenios internacionales determinan.

En el caso de la República Argentina, la jurisdicción aplicable es la del lugar de los hechos.

Pero es importante destacar los principios que plantemos en la obra que escribimos junto al doctor Eduardo Fox "Crímenes en la Web, los delitos del siglo XXI" donde destacamos que:

"Se podría decir que la delincuencia informática tiene la característica de transaccionalidad, siendo en consecuencia su persecución uno de los problemas más presentes entre los juristas, gobernantes, investigadores, legisladores y, por supuesto, los gobiernos.
Ahora bien, cuando se habla del concepto de la aplicación de la ley penal en el espacio, se hace referencia a las normas que delimitan espacialmente la aplicación del poder punitivo por parte de cada Estado. Estas cuestiones se resuelven sobre la base de los principios de territorialidad, real o de defensa, nacionalidad y justicia universal.
La Argentina, sobre la base de lo dispuesto en el artículo 1 del Código Penal, se vale de dos principios, el de territorialidad y, en forma subsidiaria, del principio real o de defensa. "

José D'Alessio define el principio de territorialidad como el criterio que establece la exclusiva aplicación de la ley penal del territorio en todos los hechos delictivos que ocurren en su ámbito, con prescindencia de la nacionalidad de los sujetos activos o pasivos y de la nacionalidad de los bienes jurídicos lesionados o puestos en peligro. En resumidas cuentas, considera que su fundamento radica en la soberanía territorial.[14]

Debemos comprender el concepto jurídico de territorio, en el que se debe incluir la superficie geográfica de la Argentina, es decir, el espacio comprendido dentro de los límites internacionalmente reconocidos que nos separan de los países limítrofes y del mar libre y el llamado mar territorial, su lecho y el subsuelo, que se extiende por doce millas marinas a contar desde las líneas de base que se establecieron en la Ley 23968.
A ello debemos sumarle, por una parte, la zona contigua que mide 12 millas marinas, la zona económica exclusiva de 200 millas de ancho y la plataforma continental. Por último, cabe considerar el espacio flotante y el espacio aéreo. Los buques de pabellón nacional se hallan sometidos al ordenamiento jurídico argentino, en tanto se encuentren en mar libre, salvo que los hechos hayan ocurrido en aguas jurisdiccionales de otro Estado.
En cuanto al espacio aéreo, está regido por las leyes de la Nación respecto de delitos cometidos en una aeronave privada argentina sobre territorio argentino, aguas jurisdiccionales o donde ningún Estado ejerza soberanía (Leyes 20094 y 17285). Por lo tanto, aplicando este

---

[14] Andrés José D'Alessio (dir.), *Código Penal comentado y anotado*, Tomo I, Parte General, Buenos Aires, La ley, 2005, pp. 4 y 5.

criterio, al que adherimos, si, por ejemplo, una persona desde una aeronave argentina, con conexión a Internet, utiliza el servicio para cometer algún ilícito, la jurisdicción argentina será la que entenderá en el caso.
La problemática que este principio trae aparejada es precisamente la que se da en el escenario de delitos cometidos en el ciberespacio, un lugar donde no existen fronteras territoriales y el delito puede configurarse en un país y generar efectos en otros. De esta manera, nos encontramos con la dificultad que resulta su persecución. Así, los creadores de los virus informáticos, como el conocido "Love-Bug" surgido en Filipinas, han causado daños en todo el ámbito mundial sin poder ser juzgado en la excolonia española ni en los países afectados. A veces, la falta de legislación específica y de coordinación procesal entre los Estados agudiza la tarea de la investigación y juzgamiento.
Para solucionar estos problemas se han formulado otras teorías que consideran relevante la manifestación de la voluntad, la producción del resultado o la posibilidad de considerar ambas a la vez.[15]

La teoría de la voluntad considera como lugar de comisión el sitio en que el sujeto llevó a cabo su acción delictiva. Lo más importante

[15] Andrés José D'Alessio, óp. cit., arts. 1 a 78 bis, p. 8.

es la exteriorización objetiva de ese querer interno. Su crítica es que no elimina los problemas de los delitos cometidos a distancia, situación dada, precisamente, en el campo del derecho informático.

La teoría del resultado entiende el delito como cometido en el lugar donde se produce el resultado.[16]

Por último y para superar las deficiencias de ambas teorías, **la teoría de la ubicuidad** entiende que el delito se puede cometer tanto en el lugar donde se efectuó la manifestación de la voluntad como también en el sitio donde se ha producido el resultado o sus efectos.

Esta teoría tuvo su origen en la sentencia de nuestra Corte Suprema de Justicia de la Nación en el caso Ruiz Mira (fallos 271.396). Se trató de un caso de injurias proferidas en el extranjero en perjuicio de un tercero residente en el país. Se sostuvo que: "… corresponde aplicar la ley penal argentina […] en tanto la teoría de la ubicuidad –aceptada por la Corte Suprema– interpreta que el delito debe considerarse cometido tanto donde se exterioriza su acción, como donde se produce el resultado, lo cual permite que el bien jurídico tutelado protegido fue lesionado en el país". (CNCrim. y Correc. Sala III, 1990/12/20 "Maradona, Diego A." *La Ley*, 1991-C, 373).[17]
También se ha dicho: "Dado que nuestro derecho penal está gobernado por el principio de la ubicuidad consagrado en el artículo 1 del Código de fondo que

[16] José Manuel Rodríguez Devesa, *Derecho Penal español,* Parte General, 8va ed., Madrid, 1981, p. 185. Durmus Tezcan, *Territorialité et conflits de juridictions* en *Droit pénal international*, Ankara, AUSBF, 1983, p. 285.

[17] Alude al actual artículo 118 de la Constitución Nacional.

dispone la aplicación de la ley argentina para los delitos cometidos o cuyos efectos deben producirse en su territorio, debe tenerse presente que los efectos de la puesta en circulación o creación de bonos externos falsos o adulterados perjudica las rentas de la nación, su moneda o sus títulos y, en consecuencia, de cometerse el delito en el exterior, igual sus efectos se tienen por producidos en nuestro país, independientemente de la presencia de su autor en el mismo" (CFed. CCorr., Sala I, 18-5-88. JA 1990 I-422).[18]

Otro de los principios que destacamos en materia de jurisdicción aplicable es el denominado "principio real, de defensa o de protección de intereses", cuyo espíritu es la protección de los intereses nacionales sin importar el lugar en donde se cometió el delito. Lo fundamental en este principio es que se constituya un ataque o amenaza a los intereses del Estado.

El doctor Carlos Fontán Balestra advierte que "el ejemplo menos discutido a que puede acudirse cuando de ese régimen de defensa o protección se trata, es el de la falsificación de moneda 17

[18] Fallo mencionado en Edgardo Alberto Donna, *El Código Penal y su interpretación en la jurisprudencia,* T. I, Rubinzal Culzoni Editores, 2003, p. 20, art. 1 a 78 bis.

perpetrada en el extranjero, que afecta al Estado cuyo signo monetario es objeto de imitación…".[19]

El mismo autor advierte que en la mayoría de las legislaciones se enumeran los delitos que, por atacar la existencia política o económica del Estado, sus autores pueden ser juzgados y penados según la ley del país al que afectan.[20]

Carlos Creus en referencia a este principio advierte que la ley argentina se aplicaría a todo delito cuyo resultado producido de daño o peligro se concretase en el territorio de la república.[21]

No obstante, lo expuesto, es importante destacar que la aplicabilidad de este principio también puede ser de gran importancia en materia de aplicabilidad de la ley penal en determinados delitos informáticos, específicamente cuando el Estado o sus intereses son afectados, como por ejemplo el ataque a servidores del gobierno nacional o del ejército. Pero la solución a estas cuestiones no gravita en el pensamiento de una o varias personas, sino en una acción efectiva y coordinada entre todas las naciones.

Jurisprudencialmente se ha dicho: "En los delitos a distancia se explica la función protectora del sistema real u objetivo para el bien nacional lesionado, porque siendo el delito un todo indivisible, el ordenamiento jurídico del Estado queda violado, tanto en el momento de la ejecución como en el momento consumativo. El fin sociológico político de la incriminación no debe confundirse con la estructura del delito, pues la expresión

---

[19] Carlos Fontán Balestra y Guillermo Ledesma, *Derecho Penal,* Introducción y Parte General, 17ma ed., Buenos Aires, Lexis Nexis-Abeledo Perrot, 2002, p. 124.

[20] Ibíd., p. 130.

[21] Carlos Creus, *Derecho Penal*, Parte General, 4ta ed., Buenos Aires, Editorial Astrea, 1999, p. 112.

‘efectos del delito’ no puede referirse a otros que aquellos que entran a formar parte de la figura delictiva, que son en ellos elementos constitutivos” (SCJ de Tucumán, 11-6-42, LL 26-828).[22]

Otro de los principios que no podemos dejar de analizar es el de la nacionalidad que propone tomar como punto de referencia la nacionalidad del sujeto activo o pasivo del delito (víctima o victimario). Para que quede más clara la idea, expresa que se aplicará la ley nacional a toda persona vinculada por su nacionalidad que cometiere o fuere víctima de un delito en un Estado extranjero.

Este principio reconoce dos subvariantes, la de la personalidad activa, en la que la ley del país obliga al ciudadano donde quiera que este vaya, y el de la personalidad pasiva, en virtud de la cual la ley lo protege con independencia del lugar de comisión del hecho. De estas dos modalidades, la primera apunta al autor de la infracción; la segunda toma en cuenta únicamente a la víctima.[23]

[22] Carlos Alberto Donna, óp. cit., pp. 17 y 18.

[23] Andrés D’Alessio, óp. cit., p. 15.

Por último, nos encontramos con el principio de justicia universal que apunta a perseguir los delitos que afecten por igual a todos los miembros de la comunidad internacional.[24]
La responsabilidad de su juzgamiento recaerá en cada Estado en donde el autor del crimen se encuentre, casos como el genocidio, terrorismo son algunos ejemplos para la aplicabilidad de este principio.
Es valedera esta clasificación ya que de allí se desprenden la jurisdicción aplicable en materia de delitos informáticos. Si bien en la práctica el principio de territorialidad es el que prima en la mayoría de los países, en otras naciones se aplican otros criterios de jurisdicción como los que acabamos de describir. Y cuando colisionan esos criterios nos encontramos verdaderamente en un problema, pues, en materia de delitos informáticos, el origen de la acción delictiva puede establecerse en un país y tener efectos en otro u otros. Hoy, la tecnología prácticamente ha eliminado las fronteras políticas de los Estados y, por ende, el delito ha tomado conocimiento de ello.

Para finalizar y considerando que es muy importante determinar la jurisdicción aplicable en materia de delitos configurables a través de internet como también en materia de cualquier tipo de controversia entre ciudadanos en el ciberespacio es menester destacar que lo fundamental en estos tiempos donde la dinámica de internet viaja a la velocidad de la luz, por decirlo de una forma metafórica, es indefectiblemente una coordinación internacional. Es decir, no es lo mismo el mundo en la

[24] Carlos Fontán Balestra y Guillermo Ledesma, óp. cit., p. 124.

década del 80 que entrada la tercera década del siglo XXI, donde la dinámica y la conectividad es prácticamente una constante y donde las acciones de uno o múltiples usuarios pueden producir efectos directos en diferentes lugares del planeta.

Por lo tanto, podemos hablar de jurisprudencia, de doctrina, del pensamiento destacados juristas en el ámbito nacional e internacional, pero aquí se trata de barajar y dar de nuevo porque las situaciones y los eventos que anteceden y preceden a esas situaciones son totalmente distintos ya no pueden resolverse en forma autónoma, sino que en estos tiempos es de vital importancia la coordinación internacional para poner pautas claras ante el avance de la tecnología con los ciudadanos del mundo.

Por otro lado, otro tema de vital importancia es la producción de la prueba, si bien ya existen tratados y convenios internacionales que esbozan soluciones a la producción de prueba en extraña jurisdicción, debemos reiterar que la celeridad necesaria para actuar en materia de derechos configurables a través de plataformas informáticas interconectadas requiere un proceso y tiempos distintos, es decir, la casi inmediatez de la producción de prueba y su correcto almacenamiento y resguardo son detalles que no podemos escapar al análisis, porque está íntimamente relacionado a la cuestión de la jurisdicción aplicable.

Por ejemplo, consideremos el caso de que todos los países integrantes de las Naciones Unidas suscriben un convenio donde la jurisdicción aplicable en materia de delitos informáticos es la del lugar de los efectos del delito.

Si no consideramos el otro pilar que es la producción de prueba de informática -que en estos casos puede estar situada en cualquier país del mundo - un protocolo de almacenamiento y procedimiento de resguardo y remisión a la jurisdicción requerida, nos vamos a encontrar con la esencia estratégica para avanzar en una investigación judicial.

La Convención de Budapest sobre cibercriminalidad del año 2001 marco parámetros esenciales en algún sentido para poder ordenar una problemática que 2 décadas después aún no pudo establecerse, ya sea porque aún faltan muchos países suscribirse a la misma, como así también muchos de esos países quienes se suscribieron, inclusive la Argentina, no adaptaron su legislación interna para su plena aplicabilidad.

Si bien si sigue trabajando en materia jurídica internacional sobre el nuevo convenio considerando los nuevos desafíos quedan pendientes grandes asignaturas, como por ejemplo que los países suscriban en su totalidad al convenio internacional; que en su legislación interna adopten la obligatoriedad del guardado de conectividad IP (que no es lo mismo que guardado de tráfico); que se agilicen los procesos de pericias de dispositivos en extraña jurisdicción (es decir, por citar un ejemplo si una persona comete un fraude desde Francia hacia un ciudadano argentino, la investigación, posiblemente y en el escenario ideal determine, con la ayuda de la justicia de Francia que el delincuente está en el usuario de internet. Pero si no se secuestra el dispositivo y no se somete a una pericia que determine ya una imputación concreta a

determinado usuario, la investigación iría camino al limbo, por eso la importancia de la coordinación estratégica y de establecer un idioma universal de procedimientos de resguardo y pericia que están íntimamente relacionados con la jurisdicción aplicable siempre que se trate de delitos transnacionales.

En resumidas cuentas, debo pensar el ciberespacio como un todo y no como lugares autónomos que se restringen por idiomas o fronteras digitales que no existen. Ese es uno de los grandes desafíos de los hombres y mujeres del derecho, de los especialistas en informática forense de las fuerzas de seguridad del mundo. Son objetivos y desafíos claros y contundentes que no pueden esperar y los gobernantes del mundo deben estar a la altura para avanzar y poner en práctica esos cambios