Nuevas modalidades de delictivas en materia de cibercrimen durante la pandemia del COVID-19 en la República Argentina

El cibercrimen refiere a la criminalidad que agrupa a los llamados delitos informáticos. Los delitos informáticos o ciberdelitos pueden ser entendidos como todas aquellas conductas antijurídicas, ilícitas o ilegales que vulneran derechos o libertades de las personas y utilizan un dispositivo informático[1] como medio para la comisión del mismo o el mismo es el fin del delito[2]. En términos criminológicos, el delito informático posee una amplia cifra oculta. La mayoría de estas conductas ilícitas no llegan a los tribunales ni registran antecedentes en organismos públicos abocados a la recepción de las mismas. Este bajo índice de denuncias judiciales se explica a partir de una serie de factores, entre los que podemos enumerar; el desconocimiento de que una persona es víctima de estos delitos en algunos casos[3]; la desconfianza de un sector de la sociedad en la efectividad de la justicia en llegar a los responsables de estas conductas ilícitas; y la falta de capacitación y/o recursos legales y herramientas para la persecución penal de los responsables de este tipo de delitos, entre otros[4]. Pero los factores más importantes que explican esta brecha estadística es que la mayoría de estos hechos tienen habitualmente resoluciones **técnicas y administrativas** más que judiciales.

---

[1] Etimológicamente la palabra "dispositivo" alude a un aparato o mecanismo capaz de ejecutar una o varias acciones con un fin determinado. El término "informática", a su vez, es una conjunción de las palabras "información y "automática" y refiere al procesamiento automático de información mediante dispositivos electrónicos. Así, un dispositivo informático es un aparato capaz de procesar en forma automática datos e información con un fin determinado. Si bien las computadoras representan los dispositivos informáticos más utilizados en la actualidad, cualquier dispositivo capaz de producir la entrada, el procesamiento y salida de información es considerado como tal, para lo cual teléfonos móviles, cámaras fotográficas digitales, televisores inteligentes, consolas de videojuegos, entre otros.

[2] Una simple amenaza pasa a ser un delito informático si como medio para cometerla se utiliza una computadora, un celular o un a tablet. Como blanco del delito, la afectación de un dispositivo por un virus informático instalado en el mismo es un ejemplo de un delito informático donde el funcionamiento de la tecnología representa el fin del ilícito.

[3] La descarga involuntaria de un programa espía (spyware) en un dispositivo para el robo de información personal de un usuario es un ejemplo de ello. También por determinadas conductas indebidas que se encuentran penadas en los códigos y la persona desconoce que representa un delito.

[4] Otros factores que hacen a la cifra oculta de los ciberdelitos son la ausencia de legislación que incluya este tipo de conductas por la falta de tipificación en los códigos penales de los países, la baja resolución judicial de este tipo de casos por la falta de capacitación de los funcionarios —jueces y fiscales—, peritos y asesores legales especializados en el tema, y la dificultad que presentan estos delitos en términos de investigación criminal y el temor de las empresas privadas ante la posibilidad de ver afectada su imagen y reputación al ponerse en evidencia los fallos de seguridad de sus sistemas y redes, tanto así como tratar de evitar grandes indemnizaciones a sus clientes por la ausencia de medidas de seguridad certeras en la protección de los datos de terceros.

Un ejemplo de una *resolución técnica* sucede cuando ingresa un software malicioso a un dispositivo, un programa antivirus o antispyware[5] lo detecta y lo elimina del sistema. Si bien estamos ante la presencia de un delito en tanto que alguien programó y distribuyó el malware[6] e intentó ingresar sin autorización a un dispositivo[7], en la mayoría de estos casos la víctima no realiza la denuncia penal en tanto que no vio afectado los datos y la información que este almacena ni se alteró el normal funcionamiento del dispositivo. En relación a las *resoluciones administrativas*, la mayoría de ellas son brindadas por las empresas proveedoras de servicios y aplicaciones de Internet. Por ejemplo, para los casos de sustracción de fondos de una cuenta bancaria a partir de un acceso indebido al sistema de homebanking, el damnificado realiza un reclamo al banco a los fines de que le restituyan ese dinero, donde a partir de un resarcimiento económico, el cliente recupera los fondos y desestima la denuncia judicial. Este un caso de solución administrativa de un delito, que es básicamente el de estafa.

Durante la pandemia del COVID-19, varios medios de comunicación alertaron sobre un crecimiento exponencial del ciberdelito en Argentina[8]. Esta afirmación se basa en un incremento de incidentes informáticos registrados en las organizaciones -fundamentalmente del sector privado- y/o el aumento de denuncias de delitos informáticos en fiscalías de todo el país. Partiendo de la base de lo dicho anteriormente, un aumento de casos registrados no implica necesariamente un crecimiento de los niveles de este tipo de criminalidad en un determinado territorio, o por lo menos, no a ciencia cierta. Un aumento de casos puede provenir por el incremento de uso de TICs y servicios y aplicaciones de Internet a partir del teletrabajo y la educación a distancia, tanto así como el consecuente incremento del número de casos por la facilitación de canales de denuncia en forma remota. Lo que sí se puede afirmar a partir de un análisis de casos de incidentes gestionados por el Centro Nacional de Respuestas a Incidentes Informaticos (CERT.ar) de la Dirección Nacional de Ciberseguridad de la República Argentina[9] es **una mayor sofisticación**

[5] El spyware o software espía son programas o aplicaciones informáticas que tienen el objetivo de recolectar datos de un usuario de un dispositivo o del funcionamiento de un dispositivo mismo.

[6] La palabra malware es una contracción de *malicious software* –software malicioso en inglés- y refiere a programas o aplicaciones informáticas que tienen fines indebidos, ilícitos o ilegales.

[7] En relación a este delito, en la República Argentina el artículo 183 del Código Penal de la Nación establece que *"Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".*

[8] "Ciberdelito: Cómo evitar una modalidad que creció un 3000% con la cuarentena". -Perfil edición online- 21/05/2021 [consultado 10-07-21]

y complejidad en las técnicas en la comisión de determinados delitos, fundamentalmente en tres tipos: los *fraudes y estafas en línea*, los ataques de *ransomware* y *blanqueo ilícito de capitales por Internet*. Esto arroja como resultado la presencia de **nuevas modalidades de delitos ya existentes.**

Para la Organización para la Cooperación del desarrollo Económico (OCDE) *"un fraude es la adquisición indebida de bienes ajenos por medio del engaño"*[10]. Es una acción que se comete con el objetivo de producir un perjuicio a una persona, organización o al Estado mediante un engaño o trampa en beneficio de quien lo practica. Puede realizarse a través de una ocultación, falsificación o artificio, entre otros. El fraude económico suele ser entendido como estafa, donde el objetivo del engaño es producir un perjuicio de tipo patrimonial a la víctima –financiero o material– con un fin puramente de lucrativo en beneficio del autor. Para el Departamento de Justicia de los Estados Unidos, el fraude por Internet es *"cualquier tipo de esquema de fraude que utiliza uno o más componentes de Internet, como salas de chat, correo electrónico, tableros de mensajes o sitios web, para presentar solicitudes fraudulentas a posibles víctimas, a realizar transacciones fraudulentas o transmitir el producto del fraude a instituciones financieras u otras personas relacionadas"*[11]

[9] Mediante la Disposición 1/2021 de la Dirección Nacional de Ciberseguridad se creó el Centro Nacional de Respuestas a Incidentes Informáticos -CERT.ar- que según su artículo 2 tiene como funciones:
a) Administrar y gestionar toda la información sobre reportes de incidentes de seguridad en las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios.
b) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten las entidades y jurisdicciones enumeradas en el artículo 1° de la presente medida.
c) Coordinar las acciones a seguir, ante incidentes de seguridad, con otros Programas y equipos de respuesta a incidentes de la REPÚBLICA ARGENTINA.
d) Contribuir a incrementar la capacidad de prevención, alerta, detección y recuperación ante incidentes de seguridad informática que puedan afectar activos de información críticos del país.
e) Interactuar y cooperar con equipos de similar naturaleza de otros países.
f) Llevar un registro de estadísticas y establecer métricas a nivel nacional.
g) Coordinar la gestión de incidentes de seguridad informáticos que afecten recursos críticos a nivel nacional
h) Impulsar la formación de capacidades de prevención, detección, alerta y recuperación para la respuesta ante incidentes de seguridad informática.
i) Cooperar con los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires en la gestión de incidentes de seguridad informática.

[10]

[11] United States Department uf Justice: ¿What is Internet Fraud?. En www.justice.gov [consultado 10-12-2007]

Fraudes y estafas en Internet

En cuanto a los **fraudes y estafas en línea,** en Argentina, la mayoría de los mismos se produjeron mayormente a través de campañas de *phishing*. Derivado de las palabras en inglés *password harvesting fishing* –cosecha y pesca de contraseñas- es un fraude de ingeniería social[12] aplicado para "pescar" datos personales de una víctima. Es utilizado como una técnica para el fraude más común de Internet, el robo de identidad, entendido como la obtención no autorizada de datos personales para la posterior suplantación o usurpación de identidad en el ilícito posterior. Las principales vías de contacto son los llamados correos no deseados (SPAM), mensajes de SMS en teléfonos móviles, servicios de mensajería instantánea como WhatsApp, o sistemas de mensajería privada en redes sociales, chats, foros, blogs, etc., tanto así como banners o pop ups[13].

En los casos de phishing, el estafador se hace pasar por un empleado de una institución bancaria, un organismo público, una tarjeta de crédito o una ONG, entre otras organizaciones, y envía comunicaciones fraudulentas distribuidas habitualmente a través de correos electrónicos generales. Los motivos son, habitualmente, un supuesto problema de seguridad, la actualización de datos, aprovechamiento de una oferta o promoción, donde se va a tratar de dirigir a la víctima a un sitio web falso similar al "oficial" para robar datos como número de tarjeta de crédito, credenciales de acceso a su sistema de homebanking (nombre de usuario y contraseña) o número de cuenta bancaria, entre otros. El fraude más común en Argentina es el *phishing bancario.*

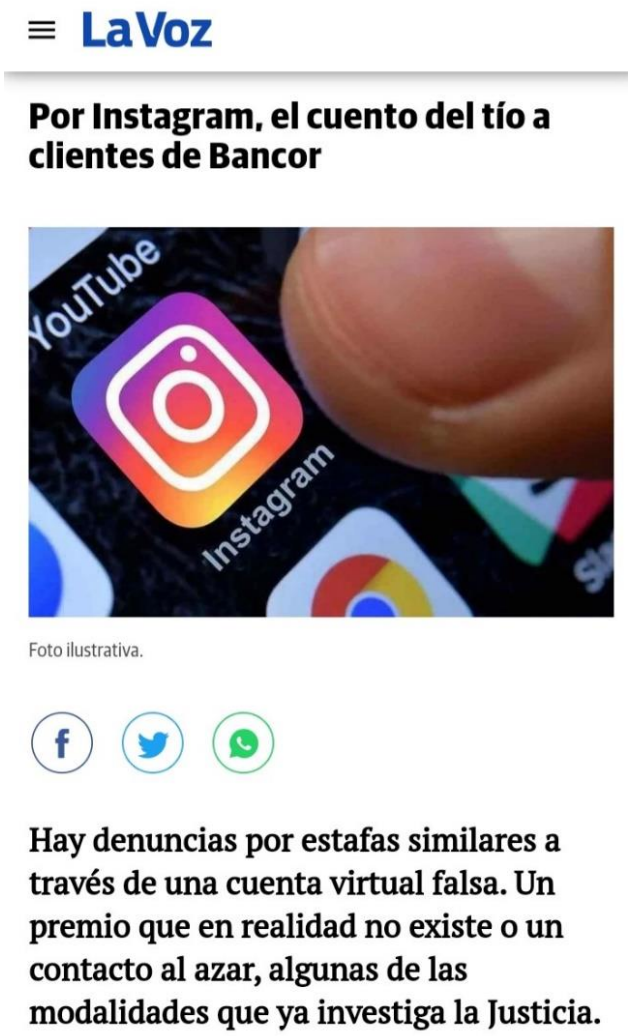
A partir del Aislamiento Social Preventivo y Obligatorio (ASPO) decretado por el gobierno durante marzo de 2020[14], se ha notado un incremento de modalidades fraudulentas a través de cuentas falsas de bancos creadas por los "phishers" en redes sociales. El aprovechamiento por parte de los estafadores de un aumento de vias de contacto web establecidos por las instituciones bancarias a partir del trabajo remoto de muchos de sus clientes y el aforo temporal en la atención personalizada en las sucursales. En este sentido, cuentas no certificadas en Instagram -y en menor

[12] Rama área de la informática que hace alusión al proceso por el cual se intenta obtener información de un usuario mediante métodos y herramientas no técnicas como por ejemplo, el proceso comunicacional. Es utilizada por los "phishers" para ganarse la confianza de una persona por medio de la comunicación y así obtener datos personales de los usuarios para el robo de identidad.

[13] Los pop ups son publicidades en línea que emergen de los sitios web en forma en forma de micrositios

[14] A partir del 19 de marzo de 2020 el gobierno de la República Argentina decretó el Aislamiento Social Preventivo y Obligatorio en todo el territorio nacional como medida de salud ante la Pandemia del COVID-19.

medida Facebook- simulaban ser las cuentas oficiales del banco. A diferencia del phishing tradicional donde se envían las comunicaciones “al voleo” a partir de un listado de direcciones de correos electronicos generales -mailist-, aquellas personas que comenzaron a seguir dichas cuentas o agregarlas como parte de sus contactos, eran en su mayoría clientes de la institución bancaria, lo que hace más selectivo el fraude en cuanto al universo de potenciales víctimas. Una vez dentro de la red social, el estafador establecía comunicación con la victima vía mensaje directo con la misma lógica del phishing general.



≡ La Voz

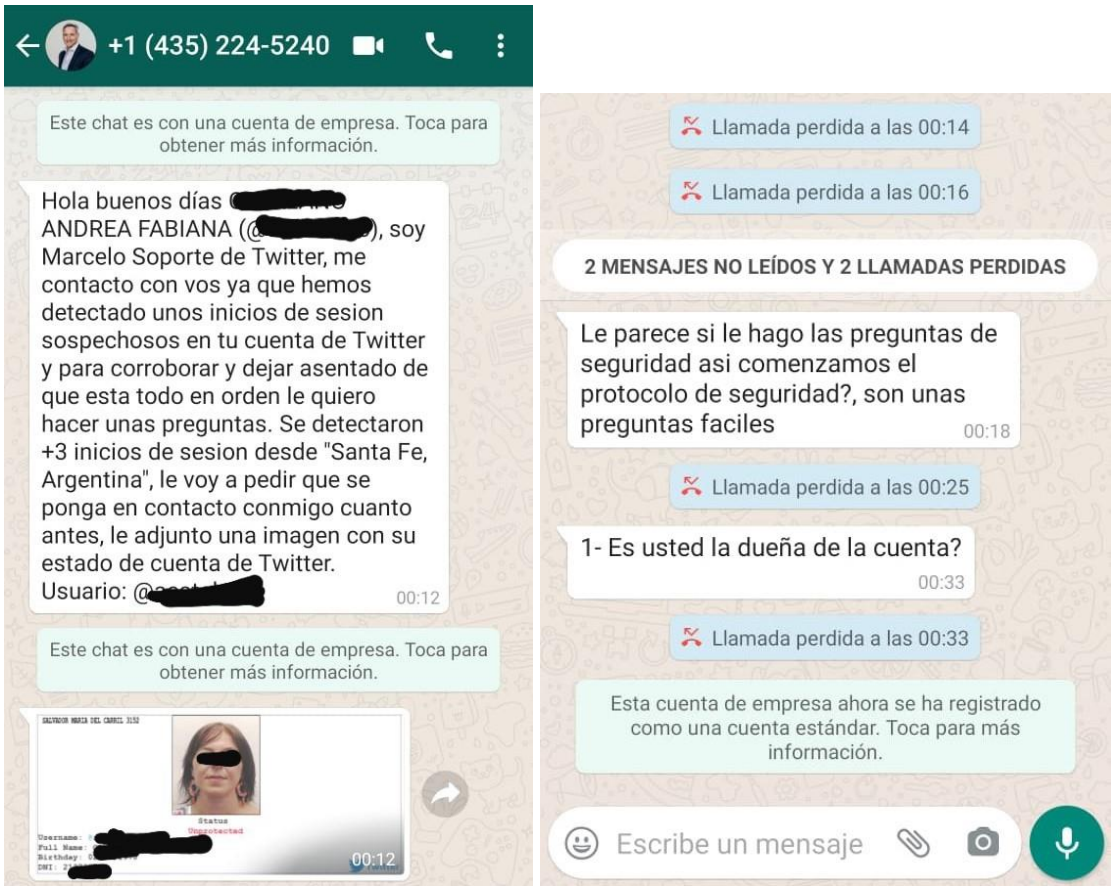
Por Instagram, el cuento del tío a clientes de Bancor

Foto ilustrativa.

Hay denuncias por estafas similares a través de una cuenta virtual falsa. Un premio que en realidad no existe o un contacto al azar, algunas de las modalidades que ya investiga la Justicia.

En relación a este tipo de engaños, durante la pandemia, estas solicitudes comenzaron a ser dirigidas, personalizadas; inclusive con datos previos de la víctima. Esta modalidad se denomina *spearphishing*. Asimismo, algunos de ellos estuvieron acompañados con técnicas de comisión similares a algunas modalidades delictivas propias del mundo físico. En este sentido algunos de éstos utilizaron un

modus operandi similar a los utilizados en los “secuestros virtuales”[15]. En uno de ellos, la victima recibe un mensaje de WhatsApp entrada la madrugada donde un supuesto empleado del servicio de microblogging de Twitter le informa que su cuenta ha sido vulnerada (hackeada) y para recuperarla, debe validar los datos que el estafador comparte mediante una imagen verdadero de la víctima, en este caso, su foto u número de pasaporte. El objetivo de la estafa es extraer datos de una persona para suplantar su identidad y cometer un posterior hecho ilícito. El contacto por escrito estuvo acompañado con videollamadas dentro de la aplicación tanto como comunicaciones telefónicas a su línea móvil.



Por otro lado, se produjeron diversos fraudes de robo de identidad basados en la sustracción de cuentas de usuario para diversos fines, principalmente económicos. Las técnicas utilizadas por los phishers estaban basadas en la obtención de datos de autenticación brindados por algunas empresas proveedoras de Internet. El factor de doble autenticación de usuario o autenticación multifactor[16] es una medida de seguridad que poseen algunos servicios y aplicaciones donde mediante la solicitud

[15] Los secuestros virtuales se producen mediante la vía de contacto telefónico por parte del supuesto secuestrador donde un llamado alerta a un familiar durante la noche del secuestro del mismo y del lugar de pago de un rescate para su pronta liberación, generalmente un lugar de pago cercano al domicilio.
[16] “El factor de autenticación doble y multiple”. -sitio web www.osi.es- 27/02/2019 [consultado 01-08-21]

de un dato anexo se intenta acreditar la identidad del titular o el legítimo usuario. El servicio de mensajería WhatsApp cuando un usuario intenta instalar el servicio desde un dispositivo nuevo o no habitual, envía un código numérico de seis dígitos mediante mensaje de texto –SMS- al número que dejó registrado el titular del número telefónico para verificar que efectivamente es él quien está iniciando la sesión.

A partir de este dato, se produjo durante la pandemia el *fraude de turno de asignación de vacunación*, donde el phisher contaba con el número de celular, nombre, apellido y documento de la potencial víctima y establecía una comunicación fraudulenta por WhatsApp haciéndose pasar por el organismo de salud de determinado distrito e informándole la fecha, hora y lugar de aplicación de la dosis de la vacuna contra el COVID-19. El fraude consistía en que el usuario debía confirmar el mismo mediante el código numérico que había llegado a su casilla de mensajes de texto del móvil, cuando en realidad el estafador había iniciado sesión de su cuenta en un dispositivo en su poder y necesitaba validarla con el factor de doble autenticación del usuario. La estafa posterior consistía, una vez apoderado de la cuenta, en enviar mensajes a sus contactos haciéndose pasar por la víctima y solicitarles dinero por un problema personal[17].

Otra estafa relacionada con fondos bancarios es el *Fraude de DEBIN*. El débito automático es un sistema de pago electrónico autorizada por el Banco Central de la República Argentina en 2017 donde un vendedor de un producto o servicio o una persona física en acuerdo con otra envía una solicitud de débito automático de fondos de una cuenta bancaria al titular de la misma. Con el objetivo de agilizar el intercambio de activos financieros, los sistemas de home banking cuentan con esta

[17] "Tenés turno para la segunda dosis contra el Covid: alertan sobre estafas por Whatsapp". -Clarín edición online- 13/07/2021 [consultado 22-07-21]

modalidad en el país. Durante la pandemia circularon engaños mediante el uso de esta modalidad, donde los estafadores enviaban a la víctima mensajes fraudulentos donde se solicitaba autorizar una transferencia de fondos en calidad de pago cuando en realizad quien desconocía esta modalidad, al autorizar la operación lo que realmente estaba haciendo el titular es dar el visto bueno a la sustracción de dinero de su cuenta bancaria, previa solicitud de número de cuenta, alias o CBU[18].

Otros tipos de fraudes reportados en cantidad durante la pandemia fueron los *fraudes de empleo desde el hogar*. Mediante correos electrónicos o publicidades en línea se publican avisos invitando a las personas a trabajar desde el hogar sin ningún antecedente profesional ni experiencia previa bajo promesa de una buena remuneración invirtiendo pocas horas de trabajo. Los únicos requisitos son los de tener una dirección de mail e informar una cuenta bancaria para el pago del sueldo, todo sin la firma de un contrato legal sino apócrifo. El engaño consiste el solicitar dinero al suscriptor en calidad de gastos administrativos, pago por adelantado o simplemente la compra de materiales. Algunos de los empleos ofrecidos habitualmente son *data entry, trabajos de ensamblaje, control de calidad de productos, fabricación de artesanías y realización de encuestas y cadete de firma, entre otros.*

[18] "DEBÍN: débito automático" -sitio web www.bcra.gob.ar- [consultado 06-08-21]

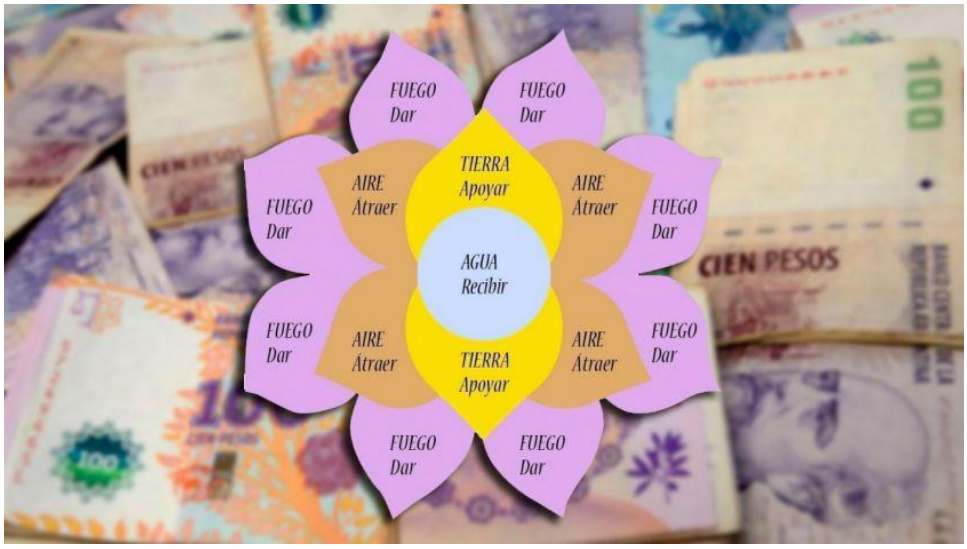
Otro tipo de fraude son los *fraudes piramidales o de esquema Ponzi.* Dicha estafa lleva esa denominación fue ideada por el italiano Carlo Ponzi en 1919[19]. El engaño comienza con la oferta realizada por una supuesta persona física o jurídica que ofrece altas rentabilidades por ingresar dinero a un esquema piramidal de inversión. La misma busca atraer dinero prometiendo ganancias basadas en intereses elevados a medida que ingresan más "inversionistas" a la pirámide, motivando a cada participante a captar gente para que también aporten fondos. En un momento la cadena se corta; los fundadores se quedan con la mayor parte de los ingresos, y los últimos en llegar nunca recuperan lo invertido. Ya desde antes de la pandemia se vieron estafas bajo nombres como la *"Flor de la Abundancia", "Mandala de la Prosperidad", "Telar de los Sueños", "Ruedas de amistad"*[20] entre otros, que prometen ingresos rápidos y elevados a cambio de un aporte inicial. Muchos de ellos buscan

[19] Carlo Ponzi percibió que los cupones que los inmigrantes italianos enviaban desde los Estados Unidos para sus familiares en Italia para que los cambiaran por dinero, había un gran negocio. Para tal fin fundó la empresa *Securities Exchange Company* y empezó a repartir cupones que dejaría al beneficiario 50% de ganancias en 45 días o el 100% luego de tres meses. Durante los primeros meses no hubo inconvenientes en el pago en tanto los intereses se pagaban sin demoras por el dinero que ingresaba proveniente de los ahorros de los "inversionistas" como de las hipotecas de sus propiedades que se sacaban para entrar en el "negocio. Un analista financiero de nombre Clarence Barron denunció que a pesar de los intereses que se pagaban, Ponzi no reinvertía en su empresa. El denunciante calculó que para cubrir las obligaciones que se generaban, hacían falta 160 millones de cupones en circulación pero que en realidad solo había 27.000. Esto hizo que una multitud de personas demandaran su dinero frente a las oficinas del inmigrante italiano. El 1 de noviembre de 1920, Ponzi fue declarado culpable de fraude.

[20] "Telar de la abundancia: el regreso de un engaño antiguo". -Clarín edición online- 23/07/2019 [consultado 10-02-20]

captar mujeres con mensajes feministas, basados en un discurso que genera una mística de empoderamiento apoyados en testimonios de violencia doméstica e intercambio de mantras.

La *"Flor de la abundancia",* por ejemplo, es una estafa que se compone de 15 "pétalos" y un "centro"; lo que representa 15 personas en total, divididas en cuatro niveles. En el nivel 4, el cual lleva el nombre del elemento del *Fuego*, se ubican ocho personas que pretenden ingresar en la flor. Para hacerlo, deben depositar en la cuenta de alguien —conocido o no— una determinada cantidad de dinero. En el tercer nivel, llamado *Aire*, hay cuatro personas que ya depositaron la suma inicial y ahora deben atraer dos nuevos interesados para escalar al siguiente nivel. En el nivel 2 -Tierra- se sitúan dos personas que están a la espera de que el individuo del escalafón superior cobre para ocupar su lugar. Por último, en el nivel -Agua- se centra la persona que recibe el dinero de los primeros ocho interesados. De este modo, cobra el 800% de su inversión inicial. Es decir que si su depósito fue de 2 mil pesos, se lleva 16 mil. La estafa consiste en que se promete ganancias en base a un capital invertido. Sin embargo, las ganancias del capital se obtienen por la plata que otras personas invirtieron. Así se genera una estructura que se agranda de manera cuadrática hasta el punto que colapsa y deja a varios inversores con pérdidas totales. En definitiva, una persona debe convertirse en estafador para no perder dinero.



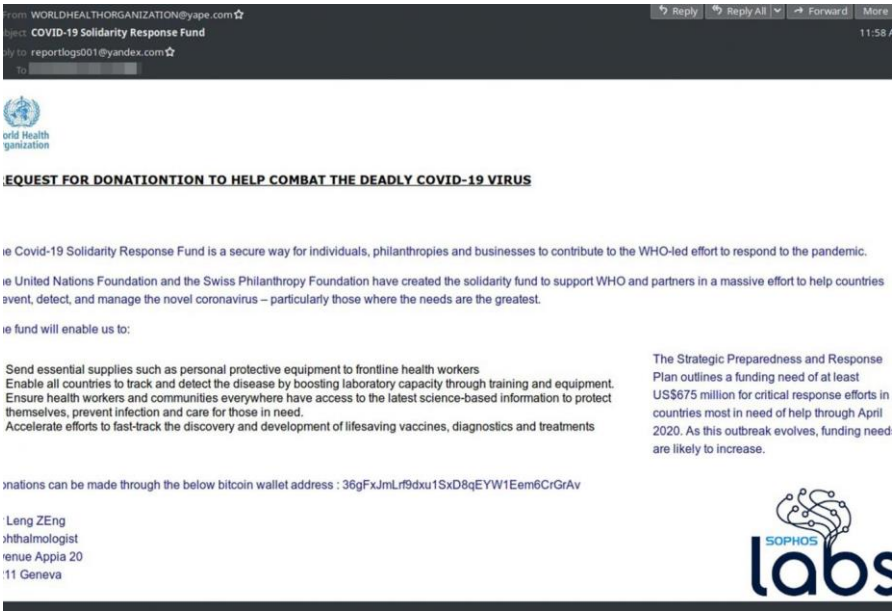
A nivel global, tres tipos de nuevas estafas relacionadas con el COVID-19 circularon en este último tiempo; *el fraude de resultados de test falsos, el fraude de inmunización del COVID-19 y el fraude de donaciones para combatir al Coronavirus.* En relación al fraude del test falso; en diferentes países se vieron casos de bandas que vendían resultados de testeo negativos del COVID-19 vendidos en zonas turísticas o aeropuertos pero adquiridos previamente por Internet. Los mismos se ofrecían a

través de cuentas falsas de redes sociales como Instagram y se pagaban previamente bajo acuerdo particular con los interesados. En cuanto a los *fraudes de inmunización del COVID-19*, en diferentes sitios web empezó a circular la venta de productos que ofrecen remedios o curas falsas contra el coronavirus tales como tés, aceites esenciales y terapias intravenosas con vitamina C son solo algunos de los supuestos tratamientos antivirales que se venden por la red. También ha habido venta online de supuestos remanentes de vacunas como Sputnik V y Astrazeneca, entre otras. En Argentina se ofrecieron productos como suero equino para aliviar la enfermedad de aquellos que se contagiaron el virus, sin autorización de las autoridades sanitarias[21].

En cuanto al *fraude de donaciones para combatir al Coronavirus*, la Organización Mundial de la Salud advirtió sobre una serie de mails engañosas sobre supuestas donaciones a nombre del organismo a partir de los efectos económicos generados por el Coronavirus. Los mismos no solo tienen como finalidad robar dinero a las victimas sino también datos personales de los estafados[22].

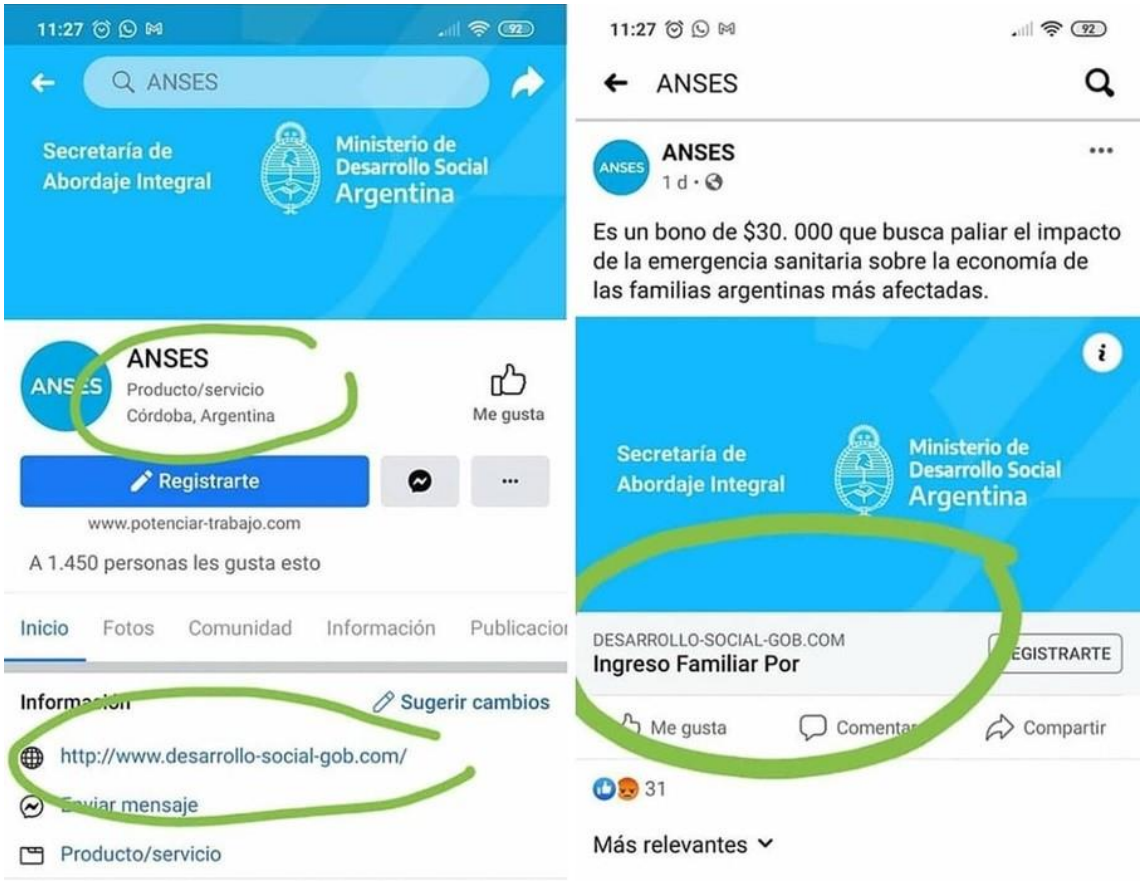
[21] "3 nuevos fraudes y estafas surgidos por la pandemia del coronavirus". -BBC edición online- 09/02/2021 [consultado 07-04-21]

[22] "Coronavirus: la advertencia de la OMS sobre los estafadores que están usando el nombre de la organización para robar dinero y datos". -BBC edición online- 24/03/2020 [consultado 27-10-20]



También en el país circularon *fraudes relacionados con programas o beneficios gubernamentales.* A través de anuncios en sitios web, mensajes de texto móviles (SMS) o WhatsApp se informa de un supuesto beneficio a la víctima relacionado con un bono o beneficio excepcional, como por ejemplo, el Ingreso Familiar de Emergencia (IFE) lanzado por el gobierno para asistencia familiar[23]. Los estafadores crean sitios web o perfiles de redes sociales falsos simulando ser la autoridad gubernamental competente. En oportunidades falsos gestores de la Administración Nacional de la Seguridad Social (ANSES) contactaron a los supuestos beneficiarios por teléfono, pidiéndoles sus nombres, fechas de nacimiento y otras informaciones para otorgarles el subsidio, e incluso haciéndolos ir hasta un cajero para que tramitaran una clave de seguridad, con la que luego podían acceder a la cuenta de la víctima.

[23] "Los delitos informáticos crecieron durante la pandemia". -Página 12 edición online- 01/05/2021 [consultado 02-06-21]



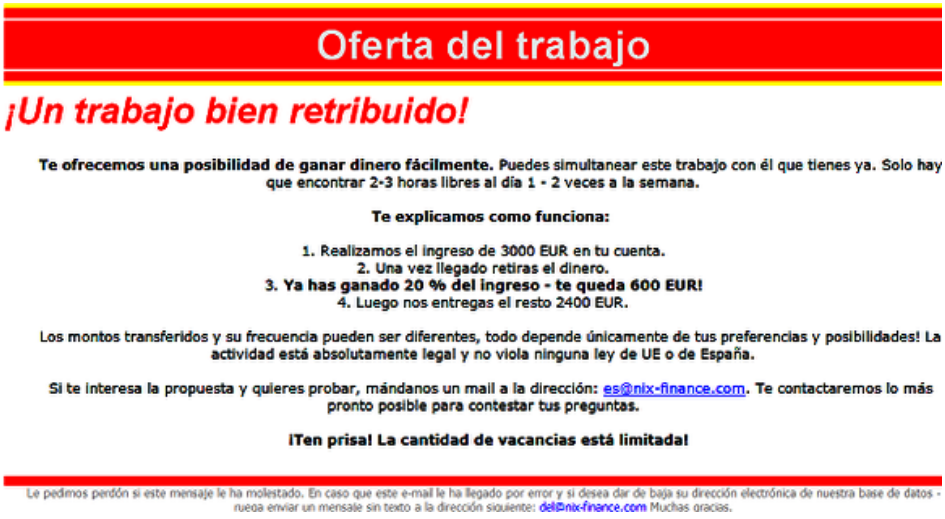
Lavado de dinero en línea

Otra modalidad ilícita que se dio durante la pandemia es el de **blanqueo ilícito de capitales**, comúnmente conocido "lavado de dinero"[24]. Durante el ASPO se han registrado casos producidos mediante fraudes de empleo. En este caso, tras el ofrecimiento formal de formar parte de una empresa, se solicita a la víctima autorización para ingresar fondos a su cuenta bancaria como parte de los movimientos financieros de la firma. Una vez realizado el depósito, se le solicita al "empleado" entregarla a un "corresponsal" de la firma. Así, en la operatoria ilícita, el único registro final electrónico es la cuenta bancaria de la víctima, lo que en este caso está oficiando como se conoce en la jerga como "mula". Durante el último tiempo se ha incrementado esta modalidad solicitando el uso de cuentas de Mercado Pago[25] -el sistema de pago electrónico de la empresa Mercado Libre- fundamentalmente para el cobro de dinero obtenido de fraudes.

---

[24] El blanqueo ilícito de capitales consiste en legitimar fondos provenientes de actividades ilegales. Es un delito difícil de descubrir a partir del uso de testaferros o "prestanombres" y la realización de operaciones por debajo del umbral permitido por las autoridades de control financiero establecida por el Grupo de Acción Financiera Internacional (GAFI), esta última conocida como "técnica de smurfing".

[25] Sitio web www.mercadopago.com.ar



Oferta del trabajo

¡Un trabajo bien retribuido!

Te ofrecemos una posibilidad de ganar dinero fácilmente. Puedes simultanear este trabajo con él que tienes ya. Solo hay que encontrar 2-3 horas libres al día 1 - 2 veces a la semana.

Te explicamos como funciona:

1. Realizamos el ingreso de 3000 EUR en tu cuenta.
2. Una vez llegado retiras el dinero.
3. **Ya has ganado 20 % del ingreso - te queda 600 EUR!**
4. Luego nos entregas el resto 2400 EUR.

Los montos transferidos y su frecuencia pueden ser diferentes, todo depende únicamente de tus preferencias y posibilidades! La actividad está absolutamente legal y no viola ninguna ley de UE o de España.

Si te interesa la propuesta y quieres probar, mándanos un mail a la dirección: es@nix-finance.com. Te contactaremos lo más pronto posible para contestar tus preguntas.

¡Ten prisa! La cantidad de vacancias está limitada!

Le pedimos perdón si este mensaje le ha molestado. En caso que este e-mail le ha llegado por error y si desea dar de baja su dirección electrónica de nuestra base de datos - ruega enviar un mensaje sin texto a la dirección siguiente: del@nix-finance.com Muchas gracias.

El "secuestro" de datos mediante ransomware

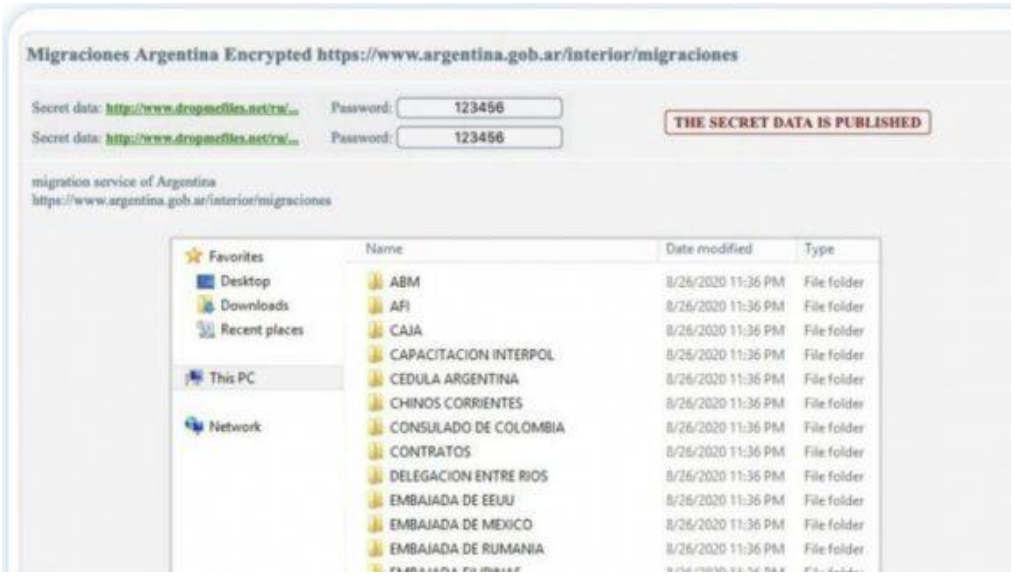
El **ransomware** es un software malicioso que encripta determinados archivos sensibles de un dispositivo o sistema o el acceso a los mismos. El "secuestrador" de los datos solicita un "rescate" de la información a cambio del pago de criptomonedas, generalmente, bajo amenaza de hacer público los mismos en Internet. El caso más conocido sobre este tipo de malware es el del emblemático caso del ransomware Wannacry de 2017 por afectar a más de 150 países en todo el mundo. Dicho malware no justamente fue noticia por la filtración de datos privados de las organizaciones afectadas sino por la sensibilidad que generó en un comienzo al afectar la información de un hospital de Gran Bretaña, una semana después del ataque al puente de Westminster a metros del Parlamento Británico[26].

Durante el transcurso de la pandemia se produjo un notable incremento de estos ataques a nivel de organizaciones que tuvieron como objetivo fundamentalmente al sector privado, donde los blancos principales fueron grandes empresas, fundamentalmente por la capacidad adquisitiva para pagar las millonarias sumas demandadas. Firmas multinacionales como Telecom, Cencosud o Galeno, por ejemplo, fueron víctimas de este malware en Argentina, donde bajo amenaza de hacer publica dicha información institucional, solicitaron rescate mediante el pago de *Bitcoins*[27]. A nivel de sector público, en agosto de 2020, la Dirección Nacional de Migraciones dependiente del Ministerio del Interior de la Nación fue víctima de ransomware con un pedido de rescate de 4 millones de dólares al cual el gobierno

[26] "WannaCry, un año después" -sitio web www.xataka.com-, 22/05/2018 [consultado 09-02-21]

[27] Bitcoin es una criptomoneda creada en 2009 por una persona bajo el seudónimo "Sathoshi Nakamoto" que opera de persona a persona –sistema P2P o "entre pares"- de características anónimas y que funciona bajo un sistema criptográfico fuera del circuito financiera tradicional.

no accedió al pago. Una vez vencido el plazo, se publicó en la Dark Web información privada del organismo, pero no vinculada a ciudadanos argentinos. Los ciberdelincuentes se hicieron de los archivos a través de la transferencia de los mismos en forma remota para obtener una copia una vez que fueron encriptados.



Un hecho significativo sucedió en mayo de 2021 un ataque de ransomware a una empresa de transporte de petróleo y gas de los Estados Unidos, "Colonial Pipeline", produjo demoras en los servicios a toda la Costa Este de ese país durante casi una semana. De manera preventiva, la firma decidió suspender la provisión de gas y petróleo que va desde la ciudad de Houston hasta New York que ante la posibilidad de que los ciberdelincuentes dañaran físicamente el oleducto de transporte[28]. Si bien el ataque solo comprometió información corporativa sensible, la empresa pagó 5 millones de dólares para la liberación (o no publicación) de la información cifrada. Para el FBI se trató de un grupo organizado llamado "DarkSide" que produjo el ataque a partir de una vulnerabilidad del sistema de energía, pero sin aportar prueba alguna de ello. Este hecho representa un ataque a una *infraestructura crítica de información* o "Sistema SCADA" (acrónimo de Supervisión, Control y Adquisición de Datos), a saber, redes informáticas inteligentes que hacen al funcionamiento de los servicios esenciales de un país (sistemas de gestión hidrológica, los conductos de gas, las redes de transmisión y distribución eléctrica, los sistemas eólicos, los sistemas de control medioambiental y los sistemas de control de tráfico aéreo, ferroviario o vial, entre otros) donde se reconoce haber pagado el rescate de los

[28] "Ciberataque al oleoducto Colonal Pipeline: esto sabemos". -New York Times en español edición online- 11/05/2021 [consultado 12-5-21]

archivos por motivos aun no esclarecidos, pese a las recomendaciones habituales de no efectivizar el pago por parte de los especialistas[29].

Ataque de denegación de servicio indirecto

Por último, cabe señalar un hecho ilícito por las particularidades de la modalidad adoptada. Durante la pandemia se produjo también un notable incremento de distribución de noticias falsas, un tema de debate en los últimos años a partir de caso Cambridge Analytica y la supuesta distribución durante la campaña electoral para la presidencia de los Estados Unidos de 2016[30]. Si bien las mismas no representa un delito, en Argentina, días previos al ASPO decretado por el gobierno, se montó una campaña de desinformación a través de mensajes de WhatsApp donde su finalidad no era establecer confundir a la opinión pública sino atacar un servicio público brindado por el gobierno nacional; el Boletín Oficial de la República Argentina.

El contenido de dichas noticias -que se viralizaron por redes sociales, sistemas de mensajería instantánea y sitios web- remitían a supuestas comunicaciones oficiales relacionadas con el virus COVID-19; personas "beneficiadas" para realizar teletrabajo, otorgamiento de subsidios varios, excepciones impositivas para

[29] Sain, Gustavo: "¿Qué és la ciberguerra?" -sitio web de la revista Pensamiento Penal- 27/02/2016 [consultado 16-8-19]
[30] "5 claves para entender el escándalo de Cambrigde Analytica que hizo que Facebook perdiera US37.000 millones en un día". -BBC edición online- 20/03/2018 [consultado 05-01-20]

sectores productivos y un supuesto colapso de Internet a nivel nacional, entre otros. Los mensajes contenían el enlace web verdadero al sitio del Boletín Oficial. Obviamente tal normativa no existía y el objetivo era saturar o hacer "caer" el sitio oficial de los actos de gobierno a modo de ataque de denegación de servicio indirecto. Un ataque de denegación de servicio se realiza habitualmente a través de botnets, redes de dispositivos que realizan tareas programadas como por ejemplo, dirigir solicitudes de acceso al mismo tiempo a un servidor que aloja un sitio web, con el fin de saturarlo, ralentizar su funcionamiento o producir la caída del servicio.