MINISTERIO PÚBLICO
PODER JUDICIAL DE RÍO NEGRO

Taller sobre Estafas Virtuales

Ministerio Público de Rio Negro – Año 2021

Ing. David Andrés Baffoni

Director de la Oficina de Investigación en Telecomunicaciones – O.I.Tel.-

Coordinador de Políticas Informáticas del Ministerio Público

Ministerio Público de Río Negro

INTRODUCCIÓN

- **El objetivo de esta charla es compartir la experiencia adquirida desde la O.I.TEL. en la investigación de causas de estafas virtuales:**

  - **MODALIDADES**
  - **LÍNEAS DE INVESTIGACIÓN**
  - **DIFICULTADES**

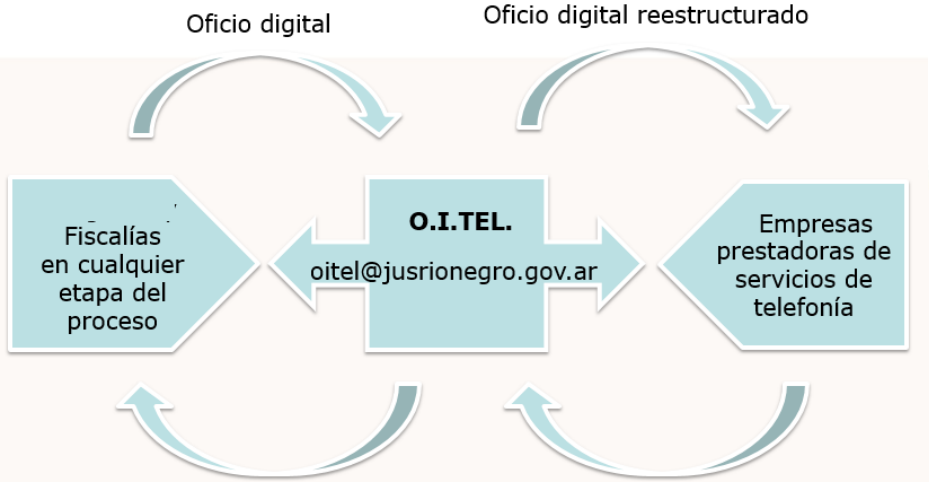
O.I.TEL.

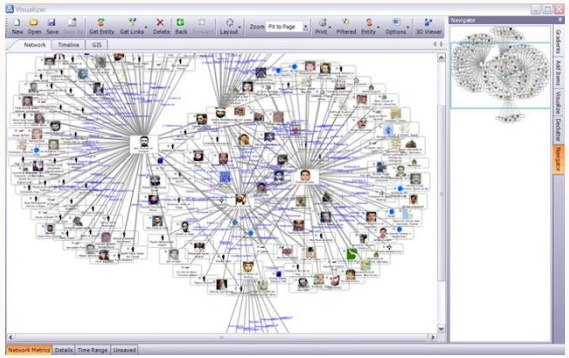
La Oficina de Investigación en Telecomunicaciones es un organismo dependiente de la Procuración General de Rio Negro cuyos objetivos principales son:

- *Centralizar y Gestionar los Requerimientos de Información a Empresas y Organismos de las Fiscalias* ***(agilizar)***
- *Realización de Análisis de Registros de Comunicaciones* ***(procesar)***
- *Realización de Exámenes Forenses a Dispositivos Móviles* ***(producir)***
- ***Asesorar*** *a los Fiscales en todo lo relacionado con delitos informáticos y telecomunicaciones (telefonía, internet, informática).*

Taller sobre Estafas Virtuales

O.I.TEL.





EVOLUCIÓN

"EL ENGAÑO NO PASA DE MODA: SE DIGITALIZA"

- Los delincuentes utilizan diferentes argumentos para defraudar a sus víctimas, con el fin de quedarse con su dinero
- ***ANTES**: para hacerse del dinero, se requería un contacto presencial (cuento del tío tradicional)*
- ***ACTUALMENTE:** la sustracción del dinero se hace por canales digitales (transferencias de dinero, robo de tarjetas de crédito/debito, etc.)*

NO SE NECESITA CONTACTO PRESENCIAL

NUEVA NORMALIDAD

- Desde el comienzo de la pandemia las estafas telefónicas proliferan como consecuencia de la nueva normalidad: los trámites comerciales y bancarios y las actividades financieras ya no se hacen necesariamente de manera presencial, sino de manera REMOTA.

- Los pretextos pueden variar pero el objetivo es el mismo: ***ganar la confianza del otro y obtener las claves bancarias*** para vaciar las cuentas —o apropiarse de la mayor cantidad de dinero posible— y obtener créditos cuyos montos son derivados a otros fondos

CONCEPTOS CLAVES

- **CBU (Clave Bancaria Uniforme**): nro. 22 dígitos que identifica de forma unívoca una cuenta bancaria en Argentina.
- **CVU (Clave Virtual Uniforme):** nro. 22 dígitos que identifica de forma unívoca una cuenta virtual no bancarizada en Argentina
- **DEBIN (Débito Inmediato**): medio de pago digital que debita un monto de una cuenta de manera inmediata solicitando una autorización previa.
- **IMEI**: nro que identifica de forma unívoca a un celular (equipo)
- **Nro. IP**: número que identifica de forma unívoca a un dispositivo conectado a internet en un momento determinado.

NUEVAS MODALIDADES

- **CUENTO DEL TÍO POR CAJERO AUTOMÁTICO**

- **Contacto**: llamada telefónica.
- **Engaño**: supuestos empleados de Anses (Bono ANSES), Ministerio de Desarrollo Social (IFE), etc.
- **Metodología**: consiguen que las víctimas vayan a un cajero automático y con engaños logran que les envíen las credenciales de homebaking y token. Con estos datos transfieren dinero existente y/o el obtenido por nuevos préstamos a cuentas de terceros (generalmente cuentas "mulas")

NUEVAS MODALIDADES

- **FALSO CANAL DE ATENCIÓN AL CLIENTE**

  - **Contacto**: llamada telefónica y redes sociales.
  - **Engaño**: los estafadores se hacen pasar por atención al cliente de empresas
  - **Metodología**: los delincuentes realizan ingeniería social en los perfiles de redes sociales de las empresas, detectando quejas de clientes. Luego se comunican con estos clientes insatisfechos y haciéndose pasar por personal de atención al cliente obtienen datos sensibles (claves, nros. de tarjeta de crédito/debito, etc.) que luego son usados para diferentes estafas.

NUEVAS MODALIDADES

- **COMPRA FICTICIA FACEBOOK/INSTAGRAM**
  - **Contacto**: chat (WhatsApp, Meesenger, etc.) y llamadas telefónicas.
  - **Engaño**: supuestos compradores se contactan con víctimas que venden cosas por redes sociales
  - **Metodología**: los "compradores" le piden datos bancarios (CBU/ALIAS) y luego informan que por error transfirieron mas dinero (envían comprobante falso). Para enmendar esto, un segundo estafador llama a la victima como empleado del banco y le pide a la lectura de un código que llega por SMS. Con este, se hacen de las credenciales del homebanking desde el cual transfieren el dinero existente y/o el obtenido por nuevos préstamos a cuentas de terceros (generalmente cuentas "mulas")

NUEVAS MODALIDADES

- **AUTORIZACIÓN DE TRANSFERENCIA (DEBIN)**
  - **Contacto**: chat (WhatsApp, Meesenger, etc.) y llamadas telefónicas.
  - **Engaño**: supuestos compradores se contactan con vendedores que ofrecen productos en sitios web y/o redes sociales.
  - **Metodología**: los "compradores" solicitan datos de la cuenta para realizar pago y luego informan que realizaron el pago mediante DEBIN, el cual debe ser autorizado por el vendedor (link junto al mensaje). **Cuando el vendedor acepta, en vez de recibir dinero, se lo debita de la cuenta.**

NUEVAS MODALIDADES

- **APODERAMIENTO CUENTA DE WHATSAPP**
  - **Contacto**: WhatsApp y llamadas telefónicas.
  - **Engaño**: con alguna excusa (Ej. Confirmar turno vacuna COVID, Soporte Técnico de WhatsApp, etc.) estafadores se contactan con las víctimas para solicitar un código de 6 dígitos que llega por SMS.
  - **Metodología**: con ese código los estafadores se apoderan de la cuenta de WhatsApp (lo usan en otro celular) y le piden a los contactos dinero para alguna urgencia, haciéndose pasar por la victima. La víctima no puede recuperar la cuenta, porque los estafadores activaron modo de verificación de dos pasos.

NUEVAS MODALIDADES

- **SIM SWAPING (CAMBIO DE SIM)**
  - **Contacto**: **NO HAY CONTACTO CON LAS VICTIMAS!**
  - **Metodología**:
    1. El estafador, usando datos personales de la víctima (Ingenieria Social) se hace pasar por esta ante la empresa prestataria del servicio de telefonía y solicita un cambio de SIM (manteniendo mismo número), indicando el retiro de la nueva en un local oficial.
    2. Con la nueva SIM en su poder, la activan en un nuevo celular (deja de funcionar la línea en el celular de la víctima) y realizan los cambios de contraseña de sus correos electrónicos y usuarios de home banking (envío de códigos por SMS)
    3. Con las nuevas credenciales, ingresan a las cuentas de las víctimas y transfieren el dinero existente y/o el obtenido por nuevos préstamos a cuentas de terceros (generalmente cuentas "mulas")

NUEVAS MODALIDADES

- **PISHING y SMISHING**
  - **Contacto**: Correo Electrónico, SMS y WhatsApp
  - **Engaño**: envío de mail o mensaje que simula ser de una entidad conocida (Banco, Tarjeta, etc.) con un link para actualizar datos.
  - **Metodología**: la víctima al ingresar los datos sensibles solicitados (datos de tarjetas, claves de acceso a home banking) posibilita:
    - **Robo de dinero de sus cuentas bancarias** existente y/o producto de nuevos créditos mediante transferencia a otras cuentas.
    - **Compras por Internet:** utilizar los datos de las tarjetas para realizar compras por la WEB

MEDIDAS DE INVESTIGACIÓN

- **SEGUIR EL DINERO (1)**

1. **Obtener CBU destino transferencia**: oficiar al Banco de la víctima para obtener CBU's y/o CVU's destinos de las transferencias de dinero (obviar este caso si la victima aportó comprobante o movimientos CBU/CVU destino).

   - ***Observacion1***: *el número de cuenta, CUIL, CUIT, DNI de las cuentas destino* ***NO SON SUFICIENTES PARA SEGUIR CON LA INVESTIGACIÓN***
   - ***Observación 2:*** *además de los CBU/CVU destino, los bancos de las víctimas pueden dar otros datos de interés como IP de ingreso al Homebanking*

MEDIDAS DE INVESTIGACIÓN

- **SEGUIR EL DINERO (2)**

2. **Obtener Datos y movimientos del CBU destino transferencia**: oficiar al Banco asociado al CBU/CVU destinos de las transferencias del dinero de la víctima consultando:
   - *Datos Registración de la Cuenta (Nombre, apellido, DNI, Tel., Dirección, etc.)*
   - *Movimientos de la cuenta (transferencias, débitos, créditos)*
   - *IP de conexión desde canales virtuales.*

➢ ***Observacion1***: *para determinar el banco al cual pertenece la CBU/CVU se puede consultar el sitio del Banco Central que detalla nómina de entidades* https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Sistema_financiero_nomina_de_entidades.asp

➢ ***Observación 2:*** *algunos bancos requieren orden de juez, donde este literalmente expresado que los liberan del secreto fiscal.*

MEDIDAS DE INVESTIGACIÓN

- **SEGUIR EL DINERO (3)**

Código	Denominación
00007	BANCO DE GALICIA Y BUENOS AIRES S.A.U.
00011	BANCO DE LA NACION ARGENTINA
00014	BANCO DE LA PROVINCIA DE BUENOS AIRES
00015	INDUSTRIAL AND COMMERCIAL BANK OF CHINA
00016	CITIBANK N.A.
00017	BANCO BBVA ARGENTINA S.A.
00020	BANCO DE LA PROVINCIA DE CORDOBA S.A.
00027	BANCO SUPERVIELLE S.A.
00029	BANCO DE LA CIUDAD DE BUENOS AIRES

Entidades según comienzo de CBU

CVU	NOMBRE	CANTIDAD_CVUS
0003	MERCADO LIBRE SRL	5529699
0007	Uala	1863223
0028	First Data Cono Sur	211702
0014	Naranja Cuenta	158233
0013	PREX	120745
0006	Pluspagos	71545
0025	Bitso Hot wallet	46008
0001	ONDA SIEMPRE PODES COMPRAR	32023
0022	SatoshiTango	18630
0011	INVOITION	15293
0039	BKR	12025
0038	Tienda Dolar	9376
0005	Ripio	5923
0004	TARJETA NARANJA S.A.	4290
0052	Orangedata	4120
0019	CAME PAGOS	4001
0027	Paymovil	3440
0010	MIIII SA	1737
0029	NUBI	1466
0012	PLATAFORMA DE PAGOS	891

Entidades según comienzo de CVU

MEDIDAS DE INVESTIGACIÓN

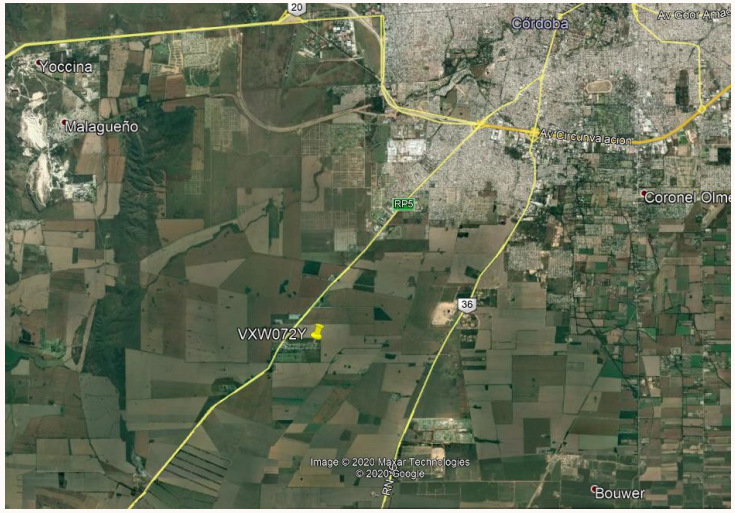
- **SEGUIR LAS COMUNICACIONES (1)**

1. **Obtener Datos de la Línea que se comunico con la víctima:** oficiar a las empresas (CLARO, MOVISTAR, PERSONAL) para consultar:
   - Datos de Titularidad de la línea (Nombre, Apellido, DNI, Dirección, etc.)
   - Registros de Comunicaciones (llamadas, SMS y trafico de datos) con **detalle de IMEI y celdas/antenas.**
2. **Obtener otras líneas que impactaron en los IMEI usados por los estafadores:** oficiar a las empresas (CLARO, MOVISTAR, PERSONAL) solicitando informen que otras líneas utilizaron el IMEI obtenido antes (**"IMEI TRACK"**)

MEDIDAS DE INVESTIGACIÓN

- **SEGUIR LAS COMUNICACIONES (2)**

3. **Obtener Datos de las celdas que captaron llamadas de la Línea del estafador:** oficiar a las empresas consultar datos de las celdas obtenidas en el punto 1: U*bicación (Latitud, Longitud), Radio de Cobertura, Azimut, Apertura Horizontal.*



Ubicación Celda usada estafador

Radio de Cobertura Celda usada estafador

MEDIDAS DE INVESTIGACIÓN

- **SEGUIR PERFILES REDES SOCIALES (1)**

1. **Obtener Datos de la Perfiles Sociales usados para contactar a la víctima:** oficiar a las empresas de redes sociales para obtener datos de registración y de ingreso de las cuentas usadas por los estafadores:

   - **INSTAGRAM:** solicitar nombre, apellido, teléfono/mail asociado y registro de IP´s de ingreso.
   - **FACEBOOK**: solicitar nombre, apellido, teléfono/ mail asociado y registro de IP´s de ingreso.
   - **WHATSAPP**: solicitar IP´s de ingreso.
   - **GOOGLE y MICROSOFT**: solicitar nombre, apellido, teléfono/mail asociado y registro de IP´s de ingreso.

➢ ***Observación1***: Facebook, Instagram y WhatsApp requieren oficios (castellano e ingles) firmados por fiscales, y se solicita por plataforma. ***Demora 15/20 días*** (en el día casos de *emergencia*)

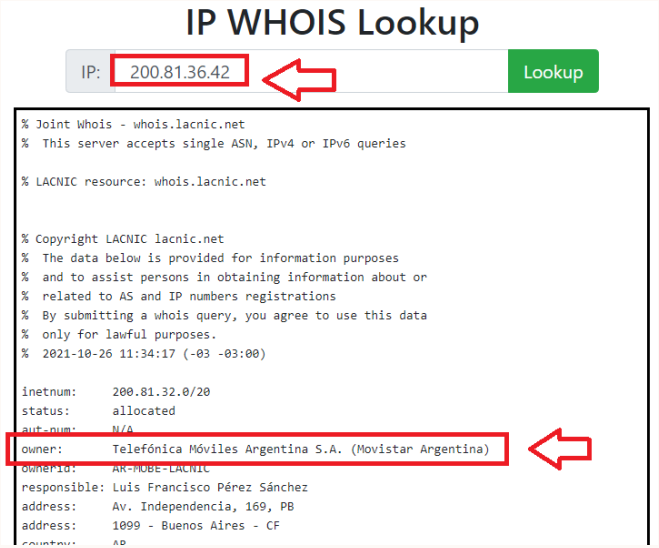
➢ ***Observación 2:*** Google requiere oficio (castellano) con firma del juez y se solicita por plataforma. ***Demora 15/20 días*** (2/3 días casos de *emergencia*).

➢ ***Observación 3:*** Microsoft requiere oficio (castellano) con firma de fiscal y se solicita por plataforma. ***Demora 20/30 días*** (en el dia casos de *emergencia*).

MEDIDAS DE INVESTIGACIÓN

- **SEGUIR PERFILES REDES SOCIALES (2)**

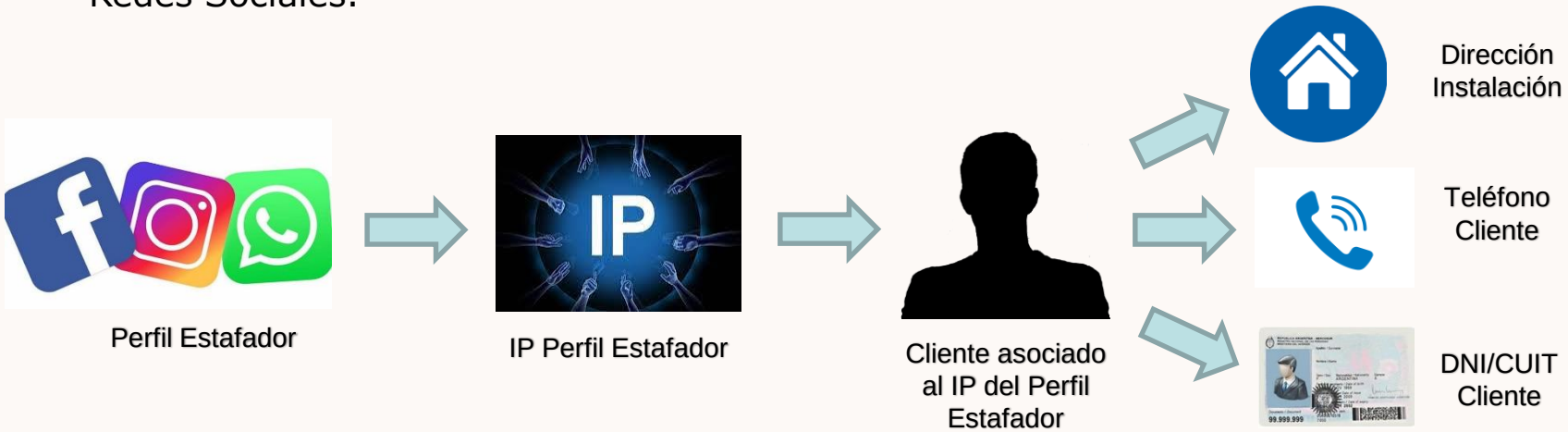
2. **Obtener ISP (proveedor Internet) de la IP usada por los perfiles de los estafadores:** existen múltiples páginas libres para obtener esta información: Ej. https://www.whatismyip.com/ip-whois-lookup/



MEDIDAS DE INVESTIGACIÓN

- **SEGUIR PERFILES REDES SOCIALES (3)**

3. **Obtener datos del cliente que uso la IP utilizada por los estafadores para conectarse con la víctima:** oficiar al ISP (Speedy, Fibertel, Cablevisión, Telecentro, etc.) solicitando datos contractuales (nombre, apellido, DNI, dirección de conexión) del cliente que uso la IP obtenida en el punto 1, en los horarios informados por las Redes Sociales.



MODALIDAD DE INVESTIGACIÓN DE CYBERFRAUDE

- **NUEVO ENFOQUE DE INVESTIGACIÓN**

➢ **FISCALÍA ESPECIALIZADA o FISCALIAS EN RED**: Por la complejidad y la cantidad de delitos, abordar las investigaciones de este tipo de estafas virtuales de manera tradicional (compartimiento estanco) generalmente no tiene buenos resultados.

➢ **CARGA DE DATOS**: Es necesario definir los datos que se deben recabar en cada investigación y una vez obtenidos, registrarlos en una Base de Datos Central que contenga la información de todas las causas investigadas.

➢ **ENTRECRUZAR DATOS**: Disponer de sistemas/procesos que permitan entrecruzar los datos registrados, con el objetivo de buscar coincidencias y patrones comunes entre las diferentes causas.

MODALIDAD DE INVESTIGACIÓN DE CYBERFRAUDE

- **NUEVO ENFOQUE DE INVESTIGACIÓN**

Ejemplo: Estafas Virtuales VIEDMA - Marzo a Junio 2020 – (1)

- Durante el segundo trimestre del 2020 (pleno inicio de la pandemia y confinamiento) se evidenció un crecimiento exponencial de las denuncias por estafas virtuales.
- Inicialmente se hizo un enfoque tradicional de investigación: cada fiscalía investigaba las denuncias que le tocaban por turno.
- Esta situación – compartimientos estancos – tenía como resultado poca efectividad en el resultado de las investigaciones.

MODALIDAD DE INVESTIGACIÓN DE CYBERFRAUDE

- **NUEVO ENFOQUE DE INVESTIGACIÓN**

Ejemplo: Estafas Virtuales VIEDMA - Marzo a Junio 2020 – (2)

- Por lo expresado anteriormente, se decidió ***centralizar toda la información importante de cada denuncia en un repositorio de datos compartidos*** y destinar a una Fiscal como líder de este trabajo transversal a varios organismos.
- Al analizar este repositorio de datos centralizado, se logró establecer que:
  - ***Había información que faltaba recabar en algunas causas***
  - ***Había causas de diferentes Fiscalias que tenían datos en común (mismo nro. de teléfono del estafador, mismo IMEI entre números de teléfono distintos, misma cuentas mulas de transferencias, etc.).***

MODALIDAD DE INVESTIGACIÓN DE CYBERFRAUDE

- **NUEVO ENFOQUE DE INVESTIGACIÓN**

Ejemplo: Estafas Virtuales VIEDMA - Marzo a Junio 2020 – (3)

Ciudad	Nro. Legajo	Fiscal - Obs	Edad	Fecha	Hora	Nombre del Victimario	Telefonos Victimarios	Intervenciones Telefónicas - Fecha	IMEI victimario	Monto Transferencia/Pago	Banco Victimario
SAO	MPF-SA-00390-2020	COY	76	1/5/2020	13:00	AHUMADA MARCOS ALEJANDRO	3424427498	NO		$ 25.900,00	Galicia
SAO	MPF-SA-00359-2020	COY	53	29/4/2020	18:00	AHUMADA Marcos Alejandro - ANSES	3424427498	no	356238086797650	$ 99.000,00	Nacion
VALCHETA	MPF-SA-00440-2020	COY	39	1/6/2020	12:30	alberto - Anses	3512869637	NO	355762081059930	$ 102.000,00	1)Macro 2) Transatlantica
Viedma	MPF-VI-01216-2020	VIOTTI ZILLI	52 - 81	7/5/2020	18:45	ANSES	3512869637	no	355762081059930	1) 9,000 2) $270,000	1) Cordoba 2) Córdoba 3) Nacion
Viedma	MPF-VI-01193-2020	PUNTEL	38	06-05-2020	16:00	Anses	3512869637 y 1126891120	no	355762081059930	99000	BRUBANK
SIERRA GRANDE	MPF-SA-00505-2020	COY	62	8/5/2020	17:40	Anses	3512817769	NO	355958071647430	$ 119.000,00	
SAO	MPF-SA-00312-2020	COY	57	14/6/2020	13	Anses	1141411363	no	358678077243880	$ 230.000,00	1) Galicia 2) Banco de Pcia Cordoba 3) Brubank
Viedma	MPF-VI-01623-2020	RODRIGUEZ FRANDSEN	65	6/4/2020	09:00	BASAVILVASO Emiliano	2920385187 AMX ARGENTINA S.A. (antes CLARO) GUARDIA MITRETELEFONIA MOVIL	no	351574093288289	$ 14.000,00	Galicia
Viedma	MPF-VI-01308-2020	ORTIZ	51	x	14:49	Busto del ANSES Valentin Bosi	3512869637 - 3515378054	3512869637 3515378054 1126891120 1121689725	355958071647430	$ 170.000,00	1) Macro 2) Provincia
SAO	MPF-SA-00614-2020	COY	27	04/06/2020	18,3	CABRERA ANSES	3512817769	no	355958071647430	$24.000,00	Banco Dino
SAO	MPF-SA-00274-2020	COY	82	16/05/20	16:50	ECHEGARAY Ruben Oscar	1141411363	no	358678077243880	154.000	1) GALICIA 2) ICBC
SAO	MPF-SA-00351-2020	COY	83	6/4/2020	08:53	Emilio Basavilvaso	2920385187	no	351574093288289		
Viedma	MPF-VI-01307-2020	RODRIGUEZ FRANDSEN	25	25/4/2020	13:30	Flores	3515378054 -3512820944 - 1121689725	NO	355958071647430	$ 125.000,00	1) Nacion 2) Santander 3) Transatlantica
VIEDMA	MPF-VI-01209-2020	VIOTTI ZILLI	44	13/04/20	18:00	FLORES MAXIMO ALEJANDRO - ETCHEGARAY FERNANDO	3515378054	no	355958071647430	$121.000,00	Galicia los dos
Viedma	MPF-VI-01052-2020 (cargada doble en MPF-VI-01212-2020)	PUNTEL	28	8/3/2020	16:45	Leonardo	1121689725 - 3515378054	no	355958071647430	$ 24.000,00	Galicia
Conesa	MPF-VI-01441-2020	Gonzalez Sacco Guillermo	59	4/6/2020	12:10	Marcos - Anses	1121659836	NO	353108087533794	$ 186.000,00	1) Brubank 2) Nacion
SAO	MPF-SA-00585-2020	COY	60	08-04-2020	17:00	Martinez Roberto Alejandro	3512211016	no	356482091875090	55000	Brubank
Viedma	MPF-VI-01638-2020	ORTIZ	30 - 59	22/4/2020	13:35	Maximiliano Alejandro Flores ANSES	3515378054 y 3512817769	19/06/20 3515378054 y nro. 3512817769 por 10 dias	355958071647430	$ 74.000,00	Macro
Conesa	MPF-VI-01098-2020	PUNTEL	43	16/4/2020	14:10	MORINI Claudio	1123103678	no	356575089343300 - 011768009279390		
Gral. Conesa	MPF-VI-01258-2020	ORTIZ	56	9/4/2020	10:00	MORINI Claudio	1123103678	no	356575089343300 y 011768009279390	$ 240.000,00	1) Credicoop 2) ITAU 3) Banco Santa Fe 4) Frances
SAO	MPF-SA-00315-2020	COY	59	12/4/2020	13:00	SOSA Horacio	1170003554	no	352442020245860	$ 9996,59	
Viedma	MPF-VI-01204-2020	VIOTTI ZILLI	52	30/4/2020	12:35	Valentin Bosi	3512869637	inter el 18/06/20 por 10 dias	355762081059930	$ 10.000,00	Brubank

MODALIDAD DE INVESTIGACIÓN DE CYBERFRAUDE

- **NUEVO ENFOQUE DE INVESTIGACIÓN**

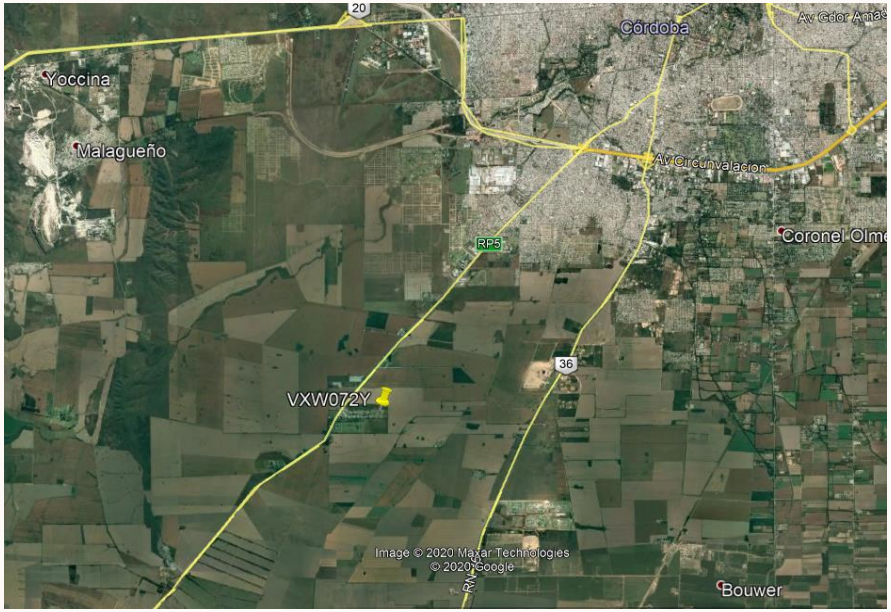
Ejemplo: Estafas Virtuales VIEDMA - Marzo a Junio 2020 – (4)

- Luego, utilizando los registros de comunicaciones de las líneas de los estafadores, se pudo establecer que en la gran mayoría de los hechos, ***todas las llamadas (mas de 17.000) provenían de la celda VXW072B/Y***, situada en cercanía a la ciudad de Córdoba capital.
- Al solicitar los datos de estas celdas, se pudo apreciar que su ***radio de cobertura*** correspondía a una zona semi-rural, ***que abarcaba el Complejo Carcelario Nro 1*** "Reverendo Francisco Luchesse" (BOUWER)

MODALIDAD DE INVESTIGACIÓN DE CYBERFRAUDE

- **NUEVO ENFOQUE DE INVESTIGACIÓN**

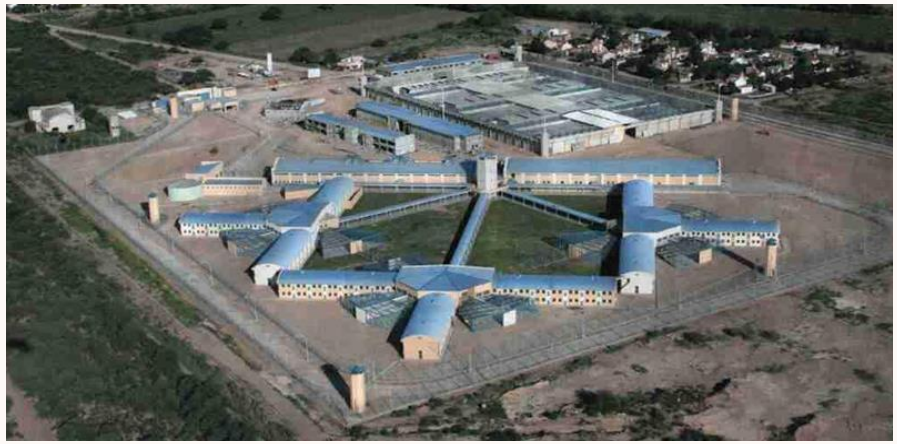
Ejemplo: Estafas Virtuales VIEDMA - Marzo a Junio 2020 – (5)



MODALIDAD DE INVESTIGACIÓN DE CYBERFRAUDE

- **NUEVO ENFOQUE DE INVESTIGACIÓN**

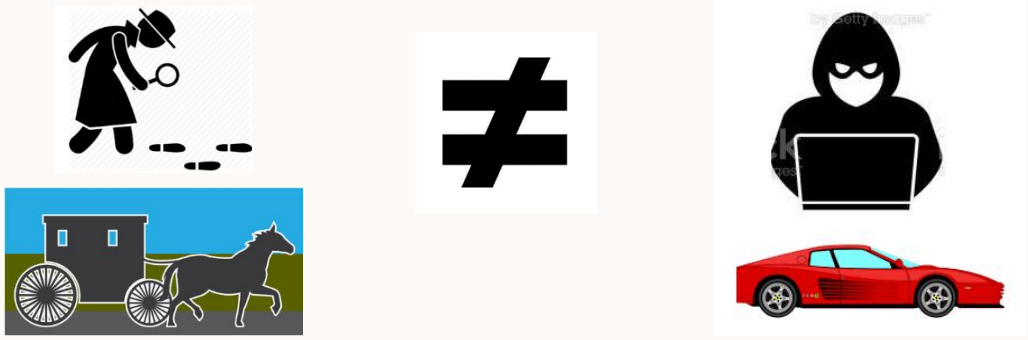
Ejemplo: Estafas Virtuales VIEDMA - Marzo a Junio 2020 – (6)



DIFICULTADES EN LA INVESTIGACIÓN

DISPARIDAD DE TIEMPOS!!!

Mientras que la estafa se realiza en cuestión de minutos, obtener la información que permita dar con los autores demanda semanas... incluso meses!!!



DIFICULTADES EN LA INVESTIGACIÓN

- **OBTENER DATOS DE LAS ENTIDADES BANCARIAS**

1. **RECEPCIÓN DE OFICIOS**: solo ***lunes a viernes de 08:00 a 17:00 hrs (no hay guardias los fin de semana ni feriados)***. Los delincuentes saben de esta situación: los hechos suceden mayoritariamente los días Viernes después de las 13 horas….

2. **DEMORA RESPUESTA DE OFICIOS**: en promedio de observa una ***demora de 15 días en obtener la respuesta de una entidad bancaria*** Además, un pedido de rectificación puede demorar semanas.

3. **INFORMACIÓN ERRÓNEA**: en muchas oportunidades se recibe información que no es correcta (CBU inválidos, IMEI inválidos, Nrs. IP erróneos) y luego demanda mucho tiempo su rectificación.

DIFICULTADES EN LA INVESTIGACIÓN

- **OBTENER DATOS DE LAS ENTIDADES BANCARIAS**

Ejemplo 1 : BRUBANK

- **13/10/21 –** Ingresa Pedido Urgente Fiscal solicitando datos del titular de una cuenta (CBU) que fue utilizada para recibir el destino de una estafa.
- **13/10/21 –** OITEL envía Oficio Urgente a BRUNBANK.
- **15/10/21 –** Ante falta respuesta, OITEL reitera Oficio Urgente a BRUNBANK.
- **20/10/21 –** Ante falta respuesta, OITEL reitera Oficio Urgente a BRUNBANK.
- **26/10/21 –** Ante falta respuesta, OITEL reitera Oficio Urgente a BRUNBANK**.**
- **AÚN SIN RESPUESTA**

DIFICULTADES EN LA INVESTIGACIÓN

- **OBTENER DATOS DE LAS ENTIDADES BANCARIAS**

Ejemplo 2: BANCO PATAGONIA (1)

- **29/07/21** – OITEL oficia al Banco PATAGONIA para corrobore dos CBU's destino de una estafa (los informaron con 23 dígitos)
- **30/10/21** – Ingresa respuesta Banco PATAGONIA, informando CBU's nuevamente con 23 dígitos.
- **01/08/21** – OITEL oficia al Banco PATAGONIA para volver a reclamar que corrobore CBU's destino, ya que siguen infamando con 23 dígitos.
- **04/08/21** – Ingresa respuesta Banco PATAGONIA, informando que los CBU's de 23 dígitos es lo único que tiene en el sistema, que pregunte a los otros bancos.

DIFICULTADES EN LA INVESTIGACIÓN

- **OBTENER DATOS DE LAS ENTIDADES BANCARIAS**

Ejemplo 2: BANCO PATAGONIA (2)

- **25/08/21** – Por pedido del Fiscal, OITEL oficia al Banco NACION y BAPRO con los CBU's destinos informados por el PATAGONIA con 23 dígitos)
- **30/08/21** – Ingresa respuesta Banco NACION informando que el CBU consultado no es válido (tiene 23 dígitos en lugar de 22).
- **08/09/21** – Ingresa respuesta Banco BAPRO informando que el CBU consultado no es válido (tiene 23 dígitos en lugar de 22).
- **15/09/21** – OITEL solicita al Banco Central intervenir para que el Banco PATAGONIA envíe CBU's con 22 dígitos.

DIFICULTADES EN LA INVESTIGACIÓN

- **OBTENER DATOS DE LAS ENTIDADES BANCARIAS**

Ejemplo 2: BANCO PATAGONIA (3)

- **25/09/21** – OITEL reitera solicitud al Banco Central de intervención para que el Banco PATAGONIA envíe CBU's con 22 dígitos.
- **12/10/21** – OITEL vuelve a reiterar solicitud al Banco Central de intervención para que el Banco PATAGONIA envíe CBU´s con 22 dígitos.
- **12/10/21** – Ingresa respuesta Banco CENTRAL, donde indica que le solicitó al Banco PATAGONIA la rectificación de los CBU's.
- **15/10/21** – Ingresa respuesta Banco PATAGONIA rectificando los CBU's destinos de la transferencia con 22 dígitos.

Trascurrieron en total 80 días y se enviaron mas de 10 oficios para consultar por dos CBU utilizados por un estafador para sustraer el dinero a la víctima.

DIFICULTADES EN LA INVESTIGACIÓN

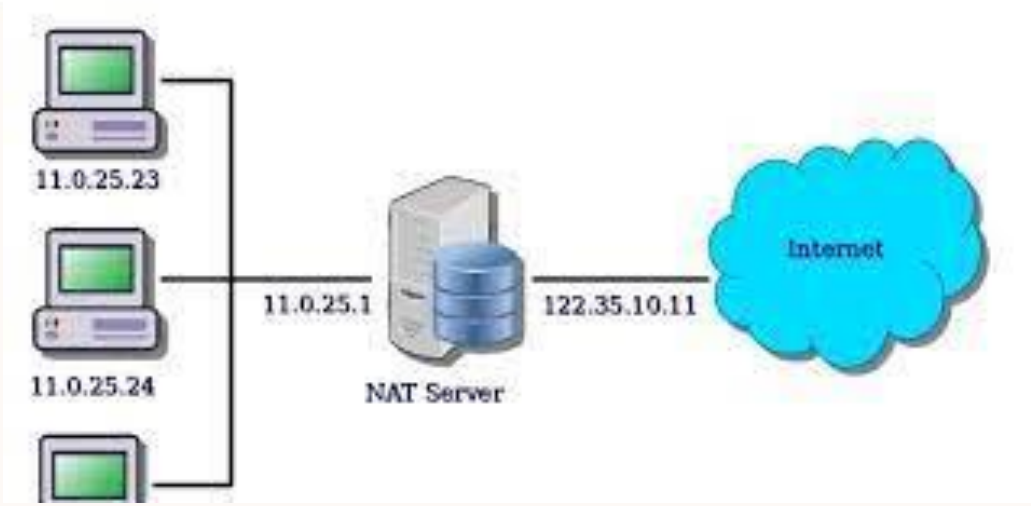
- **USO DE ABONADOS TELEFÓNICOS PREPAGOS**
  - La venta de líneas "prepagas" y la facilidad de activar las mismas con datos falsos permiten el anonimato de los estafadores.
  - La gran mayoría de las estafas virtuales comienzan con llamadas o mensajes de líneas con datos de titularidad ficticios.

DIFICULTADES EN LA INVESTIGACIÓN

- **ISP SIN REGISTRO DE IP'S – NATEO (1)**
  - La mayoría de los ISP (Proveedores de Internet) chicos utilizan NATEO, un sistema por el cual no entregan a sus clientes direcciones IP públicas (visibles desde internet), sino que utilizan direcciones IP privadas (no visibles desde internet)
  - Además, no dejan registro histórico sobre el uso de estas direcciones IP por cliente (listado de direcciones IP usadas por cada cliente)
  - Estas dos situaciones hacen que no sea factible determinar que cliente de este ISP usó una determinada IP un día y hora en particular.

DIFICULTADES EN LA INVESTIGACIÓN

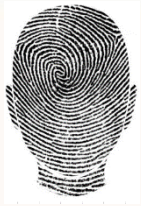
- **ISP SIN REGISTRO DE IP'S - NATEO (2)**



- **Observación:** Esto mismo sucede con algunos proveedores de internet móvil (planes de datos de una línea celular)

MEDIDAS DE PREVENCIÓN NECESARIAS

- **TELEFONÍA**

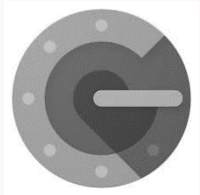


- Los proveedores de telefonía móvil deben aplicar ***procesos mas exhaustivos para corroborar identidad de los clientes*** (evitar SIM SWAPING)
- Se debe legislar para obligar a los proveedores de telefonía móvil a ***endurecer mecanismos de activación de líneas***, además de restringir lugares de ventas (minimizar líneas "prepagas" con datos ficticios)

MEDIDAS DE PREVENCIÓN NECESARIAS

- **ENTIDADES BANCARIAS (1)**

- Realizar una ***verificación fehaciente de la identidad*** del usuario de manera ***previa al otorgamientos de créditos*** pre-aprobados, y ***demorar su acreditación*** 48 hrs.. (Aplicar circular nro. del Banco Central https://www.bcra.gob.ar/Noticias/responsabilidad-bancos-creditos-canales-electronicos.asp)



- No utilizar los SMS como canal de verificación ante cambio de contraseñas para los portales de homebanking (permitir aplicaciones como Google Authenticator)

MEDIDAS DE PREVENCIÓN NECESARIAS

- **ENTIDADES BANCARIAS (2)**

- Requerir contar con la tarjeta de debito e ir al cajero automático para el otorgamiento de token (***no permitir sacar el token de manera totalmente online***)
- El Token reemplaza a la vieja tarjeta coordenas para realizar transferencias de dinero.
- En aquellos bancos donde se flexibilizó la activación del token de manera 100% virtual, se incrementaron exponencialmente las estafas con dichas entidades.

MEDIDAS DE PREVENCIÓN NECESARIAS

- **ESTABLECIMIENTOS DE EJECUCIÓN PENAL**

- Es necesario controlar y fiscalizar el uso de celulares desde los establecimientos de ejecución penal.
- Un gran porcentaje de las estafas virtuales, son cometidas por bandas organizadas que operan dentro de las cárceles.
- Se debe definir áreas de comunicación donde se permita el uso de ceulares a las personas privadas de la libertad comunicarse con sus familiares, pero restringiendo su uso fuera de estas áreas (usar inhibidores de señales)

CONSULTAS

GRACIAS

Ing. David Andrés Baffoni

dbaffoni@jusrionegro.gov.ar

Director de la Oficina de Investigación en Telecomunicaciones – O.I.Tel.-

Coordinador de Políticas Informáticas del Ministerio Público

Ministerio Público de Río Negro